*** Please note that this document ***

- only has a draft status (do not communicate with the European Commission about the content)

- is confidential (only share selected paragraphs of the text and not the whole document)

Fight against crime and Terrorism

Contents

Forensics

1 – Forensics topic 1: Intensive data usage in Forensics

Specific challenge:

Easy availability of petabytes of on-line and off-line information, both public and owned by the Law Enforcement Agencies (LEA), besides being a valuable resource represents a challenge. Access to huge amounts of data, structured (data-bases), unstructured (text), semi-structured (HTML, XML, etc.), available locally or over the Internet, may easily turn-out into a hardly manageable overload of information and represent a problem instead of a useful asset. Research under this topic should aim at providing solutions at and beyond the state-of-the-art in the area of intelligent use and management of complex and large amount of data for the discovery of correlated evidences to support forensic investigation. Data and content analytics, including visualisation and multilingual data, the use of data driven intelligence and knowledge discovery are the core technologies to be leveraged. Interdisciplinary approaches based on the definition and use of common ontologies and the exploitation of automated reasoning, information retrieval, and filtering tools should be broadly considered. Although not excluded, the integration and management of non-textual data is not part of the core focus of this topic.

Scope:

Proposals should address the problem of extracting useful information and integrating the results in formats easily intelligible by the LEA, to better and more efficiently allow the collection of facts and evidences to support forensic investigations. The problem of heterogeneous data schemata as well as that of exploiting unstructured data (Natural Language Text) has to be solved by means of the most up-to-date and beyond the SOA technologies in the areas of Big Data, Data Analytics, Intelligent User's Interfaces, Information Retrieval, Ontologies and Knowledge Representation. Human and organization factors like multilingualism/multiculturalism as well as other trans-border issues (different terminologies, legislations, procedures) have to be properly adressed.

Expected impact:

Improved capabilities for the LEA to conduct investigations. Higher efficiency in accessing relevant data sources and retrieving information significant for forensic investigation. Improved capabilities for trans-border LEA data-exchange and collaboration.

Form of funding:
Collaborative Project 100% funding (Capability project)

2 – Forensic topic 2: Advanced easy to use in-situ forensic tools at the scene of crime

Specific challenge:

Organised crime and criminals do not limit themselves to regional or national borders. Their crimes are thus leaving traces in multiple countries. Cross border access to evidence has become an absolute necessity for Law Enforcement Agencies (LEA) and judicial authorities.

Evidence gathering, collection and exchange at EU level should be usable from the field to the judge, independently of where the crimes have taken place. Rapid developments in technologies and communications in various fields go hand in hand with new opportunities for forensic science in order to keep the standards of forensic science in Europe at a high level.

Proposals for this topic should take into account the existing EU and national projects in this field.

Scope:

Proposals for this topic should focus on the development of EU-wide standards for the exchange of forensic data supporting evidence.

A platform integrating different techniques should be proposed in order to achieve better results for gathering evidence in the field of forensic research. Relying on knowledge-based fields such as artificial intelligence, machine learning, different procedures, tools and algorithm should be developed within this platform, based on the standard outlined above.

Specific areas of research could be:

- Ballistic data, including gunshot residue.
- The establishment of a EU-wide database new synthetic drugs and precursors (detection protocols and analysis methodologies).
- Other types of pan-EU databases - like for instance soils etc.

In addition due to the variability and the wide range of crime types, procedures or methodologies should be developed or adapted to the specific crime features. Moreover, horizontal strategies could be proposed for profiling crimes or offenders and matching and predicting different type of crimes. This should lead to the establishment of a catalogue of these procedures or methodologies.

The involvement of existing EU wide forensics networks should be beneficial for the development of this proposal.

Expected impact:

The usage of the most advanced information technologies should allow improving and upgrading the current forensic systems in the European police institutions. The scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase. Moreover, it should contribute to a considerable improvement in the field of public security and improve trust of the citizen in the work of police forces in the EU.

Form of funding:
Collaborative Project 70% funding (Integration project)

3 – Forensics topic 3: Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRN materials

Specific challenge:

In the event of an accident or a terrorist attack involving CBRN materials, the examination of a crime scene by man is hardly possible. Therefore, there is a need for the development of mobile, remotely-controlled technologies to enable an improved identification / detection of CBRN materials and collection of forensic material / evidence in a variety of situations and conditions.

Scope:

The objective of this project is to develop mobile, remotely controlled technologies to identify / detect (including visual recognition) CBRN materials in the case of accidents and terrorist attacks. Technologies should enable to verify the presence of CBRN materials and to identify which kind of substance is present. They should also permit the collection of forensic material / evidence and be operational in a variety of weather and terrain conditions. Proposals should link with existing projects.

Expected impact:

An improved identification / detection and collection of forensic evidence in case of accidents or terrorist attacks involving CBRN materials will be of direct support to first responders, civil protection and public health services. In addition, dual-use applications will be considered with possible synergies being established with the European Defence Agency.

Form of funding:
Collaborative Project 100% funding (Capability project)

4 – Forensics topic 4: Internet Forensics to combat organized crime.

Specific challenge:

The Internet is nowadays at the core of any business activity. Every big and distributed organization does necessarily rely on the Internet for the exchange of data, information, knowledge, both internally and externally, so as to organize and run its activities. Organized crime does not make an exception. Internet became for the criminal organizations an important tool for organizing their illegal activities. Research under this topic should refer to Internet Forensics as to the set of investigation techniques concerned with Internet as a media used by organized crime in general -also when not concerned with cyber-crime- mainly to communicate and exchange data and information. A further and specific challenge is represented by the camouflage of the real nature of the concerned data and information. Due to the borderless nature of the Internet, specific trans-border aspects should be considered when dealing with Internet Forensic. Therefore, aside the involved technological aspects, legal and organizational issues like the co-ordination of different Law Enforcement Authorities (LEA) and the harmonization of the different legal frameworks have to be addressed.

Scope:

Proposals should focus on how to extract, compare, correlate, filter and/or interpret suspect information, data, communications stored and/or transferred on the Internet, so to discover facts and evidences to support forensic investigations. Software and, if necessary, hardware tools, methods and guidelines should be proposed. They should tackle all the layers of analysis, from the data-packet level to the data mining, to language interpretation, semantic analysis, and information retrieval, including the multi-languages aspects. Investigation technique on any kind of crime using the Internet to some extents (to communicate, transfer data, etc.) should be concerned, including, but not limited to, cyber-crime. The proposed solutions should allow to speed-up the search in the huge amount of data-transfer that occurs on the Internet, and to discover and make clear (interpret) out of it the actually relevant data and information. At the same time, limited, or at least controlled, pervasiveness of the proposed solutions must be guaranteed, in order to mitigate the impact on the privacy of all the internet users. Ethical issues have to be clearly addressed and appropriate solutions to fulfil the legitimate request of privacy by the citizens should be embedded in the very core of the proposed results.

Expected impact:

Improved capabilities for the LEA to conduct investigations by using all information travelling and stored on the Internet. To enable an increase of the number of experts able to perform such kind of investigations. Increased crime prevention capabilities.

Form of funding:
Collaborative Project 70% funding (Capability project)

Law enforcement capabilities

5 – Law enforcement capabilities topic 1: Tools and software for the exchange, fusion and analysis of heterogeneous data for law enforcement agencies

Specific challenge:

Within Law Enforcement there is a demand for scalable systems capable to receive, manage, store, combine and present heterogeneous data like ANPR, Video, Audio and GPS, coming from the myriad of sensors that are nowadays used or otherwise accessible by the Law Enforcement Authorities (LEA). Current fragmentation of system architectures and diversity of data formats makes it difficult if not impossible to add intelligence (biometrics, behaviour analysis and scenario's) for operational and situational awareness.

Current challenges (e.g. big data, secure connections, data flow and vendor locking) is leading to procurement of ad hoc solutions and (re) building on old IT systems.

Scope:

Research is needed for open solutions that will bring a sustainable system in which heterogeneous data, vector handling and the unforeseen emerging needs are incorporated. Integrating intelligence has to happen at the system level instead of the sensor level. Vendor locking has to be excluded.

Relaying on previous research projects at EU and national level, proposal should focus on how to develop the base line for current and future end user requirements, based on the latest research and expertise in sensing, and scope a future demonstration to incorporate in a new intelligence system dedicated to law enforcement agencies. The proposal should take into account existing FP7 projects.

Expected impact:

At the end user level, it should lead to European cooperation of LEA. At research level, it should lead to more interoperable standards for sensors. The architecture of the demonstrated system shall be useful for police forces, border security agencies and others. On a research level the impact will be new solutions for large scale ICT systems for the management of heterogeneous sensor data.

Form of funding:
Collaborative Project 70% funding (Integration project)

6 – Law enforcement capabilities topic 2: Cyber-security and cyber-intelligence cloud system

Specific challenge:

In the last few years, many diverse tools and techniques have been developed in the area of cyber security in order to face the increasingly emerging threats. Traditionally, those cyber security services have been provided in a direct and local way, especially when SMEs are involved, since they do not count on an international provision of services or the required commercial structure for that purpose. However, the targeted end users in sectors such as the banking one, have become global, spreading their activity worldwide and incorporating amounts of data which increase exponentially. Besides, the information is highly distributed amongst corporate servers and multiple devices.

In this context, the competitiveness of many of the European cyber security companies are in danger unless those services are moved into a cloud framework, which will also be the model mostly adopted by their customers in the close future.

Meanwhile, organised crime is regrouping themselves in a global and cloud-like cross-border structure, provoking new threatening cyber scenarios.

Scope:

The proposed research shall analyse the cyber threats related to the use of cloud system (i.e. repository and computation).

The scope is:

First, to develop a proof of concept platform of global cyber security and cyber intelligence services which can cover the emerging security needs in areas with large amount of data and distributed assets to be protected. This platform will incorporate innovative tools for analysis, detection, prevention and handle of cyber risks, moving into the cloud services which are currently provided in a more local way. The platform may also provide secure storage of the information, as well as a reliable user management. An efficient and cost-effective processing of information will also be required for big data operation. The standards for tools to be included in the platform will be defined.

Second, to perform the testing, validation and demonstration of the appropriateness and performance of the solution in a real environment. The banking sector has traditionally been one of the greatest consumers of cyber security and anti-fraud solutions and is identified as a key sector by the Commission. Their needs in terms of large data processing are increasing as their environment becomes more global, with distributed assets all along the world.

Additionally, it is necessary to establish the framework in which the platform will operate, as well as its relation in supporting CERTs / CSIRTs and other public institutions such as EC3. Thus the identification of relevant legal framework of this new paradigm and to establish the consequent guidelines is one of expected outcomes.

For the demonstration part, the operational use case will be the banking sector, although the benefits may be extended to other sectors which work with large quantity of data and require security services (e.g. Public Service Organizations, LEAs, etc.).

Expected impact:

The proposal should aim to improve the competitiveness of the cyber-security industry, by allowing a more real global market within Europe and worldwide, giving access to new markets and enhancing collaboration amongst large security companies and SMEs. The higher available resources could then be devoted to the creation of more innovative tools.

At a policy level, the project should help to standardize the work of cloud security platforms, and how those private driven can help public bodies (such as EC3) ensuring a secure cyberspace within which economic and social activity can flourish, and the fulfillment of the cyber-security strategy.

The participation of SMEs is encouraged, since the cloud platform can give them the opportunity to provide specific and innovative global services by collaborating with larger companies. This will help the private sector to keep its leading role and strengthen EU-level cooperation.

The security of European citizens' as well as the European banking system should also benefit from the project, allowing access to a wider variety of cyber-security services and fighting the increasingly sophisticated banking crime. Thus, it has to be aligned with the third objective of the EU internal security strategy. In addition of improving the trust and confidence of the finance sector, it would help to fight against cyber risks of cross-border dimension and achieving cyber resilience.

Form of funding:

Collaborative Project 70% funding (Capability project)

7 – Law enforcement capabilities topic 3: Develop novel monitoring systems and miniaturised sensors that improve Law Enforcement Agencies' evidence- gathering abilities

Specific challenge:

Investigations on the activities of criminal organizations (related with drugs or human trafficking, terrorism, or any other forms of organized crime) usually require Law Enforcement Agencies (LEAs) to use electronic equipment for legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way, while keeping for both the sensors part and the monitoring station all the legal, integrity and chain-of-custody requirements that will enable the presentation of evidences obtained this way at the Courts of Justice.

Requirements for this equipment are very different from those offered by available commercial devices. Depending on the operation, the periods of time that these electronic devices have to work can range from days to months or in real time. Access to the device could be limited or impossible. Secure remote operation over radio channel (or other type of communication channel) should be possible. Other requirement may apply like small size for easy concealment, low power consumption for extended time life, robustness and self- protection in addition to strong authentication mechanisms for operators and protection of the communication channels.

Scope:

The task is to develop a new type of sensors, monitoring station and their associated communication channel for LEA operation on the field according to their specification and subject to their validation at the end of the project taking into account the societal acceptance of the proposed solutions. Participation of LEAs in the definition of requirements and validation of results is essential, as only end-users are familiar with the challenges they frequently have to face in real operations within criminal investigations.

Expected impact:

This action is directed to the substantial improvement of existing technologies and the development of new ones, and their direct and practical application to day-to-day needs that Law Enforcement Agencies are not able to realize efficiently with available commercial products including testing, validation and demonstration as justified.

Form of funding:
Collaborative Project 100% funding (Capability project)

8 – Law Enforcement capability 4: Detection and analysis of terrorist-generated content on the Internet

Specific challenge:

Due to the ease of publishing information on the Internet (Web site, blogs, social networks, newsgroups, etc.), terrorists increasingly exploit the Internet as a communication, intelligence, training, and propaganda tool where they can safely communicate with their affiliates, coordinate action plans, raise funds, and introduce new supporters into their networks. In order to cope with the dangers involved in the use of Internet by global terrorist organizations and grassroots terrorist cells, more efficient and effective automated techniques are required. Despite the often explicit or at least not disguised content of these web-sites, especially when used for propaganda, the huge amount of somehow related, yet not illegal, sites, represents a major obstacle to the reliable and fast analysis of their contents. Research should therefore develop and apply new and/or improved data and text mining methods to detect, categorize, analyse, and summarize terrorist-generated content. Aside this, modes of attacking, finding sources of threats, capturing and preserving data for forensic analysis, should be investigated.

Scope:

Research should focus on the accurate identification of terrorist online communities (even hiding their real identity), accurate and fast categorization of malicious content published by terrorists and their supporters in multiple languages, large-scale temporal analysis of terrorism trends, and real-time summarization of multilingual information published by terrorists. The developed methodologies should be able to handle massive amounts of multilingual web content in minimal time.

Expected impact:

More effective prevention of terrorist activities planned and organized via the Internet through automated analysis of terrorist-generated content. Faster detection of grassroots terrorist cells from their online activitieş. Faster and more accurate detection and analysis of malicious content published by terrorists. Faster detection and analysis of terrorism trends. Reduction of the "information overload" on web intelligence experts due to automated summarization of the relevant content.

The usage of the most advanced information technologies will allow improving and upgrading the current mining systems in the European police/ intelligence agencies (the scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase). Moreover, it will contribute to a considerable improvement in the field of public security.

Form of funding:
Collaborative Project 70% funding (Capability project)

9 Law enforcement capabilities topic 5: Securing the vehicle supply chain from production to destruction

Specific challenge:

In 21st century there is no need to get physically a car to receive the registration document, the number plate and to insure a high value vehicle. With this virtual registered and insured car, organized crime members can declare it as stolen. The direct benefits are the insurance payment of the car value and zero risk. International vehicle trafficking draws a yearly criminal benefit of approximately 5 billion Euro in Europe, increasing the risk of EU citizens to drive a stolen or defect car and impacting the legitimate vehicle business and the economy at large. International vehicle trafficking is one of the basics for organized crime groups to finance (illegal) operations worldwide.

Scope:

The main objectives are :

- To stop the criminal supply chain related to vehicles in Europe by enabling a comprehensive integration of information currently managed independently by all major stakeholders.
- To increase investigative capacities for police and custom authorities by significantly reducing the needed time to search for and assess essential information electronically.
- To strengthen public-private approach against vehicle crime in Europe and beyond through strong and structured cooperation between major stakeholders along the (criminal) supply chain.
- To enable strategic analyses for the purpose of targeted in concerned countries leading to crime prevention and crime detection.

The task is to create an e-platform where information could be exchanged between major stakeholders, with the following information available online to detect crime, avoid registration of stolen vehicles, avoid use of wrecks, ease police investigation:

- Manufactured Veicule Identification Number (VIN) and country of export;
- VIN registered in each country;
- VIN insured and VIN declared ‘wreck’;
- VIN stolen.

The proposal should take into account existing European and national projects and includes representatives/stakeholders from all value chain (manufacturers, insurance companies, law enforcement agencies and international./European law enforcement organization, registration authorities, car dealers, etc.).

Expected impact:

An effective and innovative tool in fighting crime and improving security should be developed. By stepping into state-of-the-art information management between public and private entities active in the fight against vehicle crime impacting EU citizen as well as EU business and law enforcement, the project is expected to bolster the prevention and detection of vehicle crimes.

Form of funding

Collaborative project 70% funding (Capability project)

10 Law enforcement capabilities topic 6: Trans-national cooperation among public security research stakeholders

Specific challenge:

The aim of the topic is to improve coordination at European level of various national or regional networks in different security research domains. Activities can concentrate on a specific core area or cover several areas. The focus of this challenge should be on the identification of the relevant technologies for law enforcement technologies.

Scope:

The action should further aim to: a) exchange information on security issues in their countries and define core areas of common interest in order to prevent duplication and identify synergies, b) exchange information about research needs and latest technological developments, c) develop common strategies and mechanisms in the specific area(s), and d) explore and demonstrate coordinated and/or joint activities.

Expected impact:

It is expected to improve networking and coordination of various Member State activities relevant to Security research at European level.

Form of funding

Coordination and Support Action 100% funding (Coordinating action)

Urban security

11 – Urban security topic 1: Innovative solutions to counter security challenges connected with large urban environment

Specific Challenge:

The current wave of urban growth, the largest in the world's history, is bringing various challenges and threats to urban security, especially in large urban environments. These challenges have also a strong impact on the security perception of the citizens and, by this, they can impact on the economic development and the quality of life.

Consequently, there is a growing need to go beyond the idea that only the law enforcement and criminal justice systems are tasked to tackle urban security challenges. On the contrary, new approaches and innovative solutions, including sustainable, affordable and transferrable security technologies, are needed to solicit citizens' engagement and direct participation in the improvement of the urban security conditions.

In this framework, and upon due consideration for the concerned ethical issues, recent technological advances and appropriate sensing mechanisms can help to make a city more transparent and readable as well as to empower the citizens in smart cities by ensuring that the main urban dynamics are unveiled and available to the public.

To this end, a bottom-up approach is sought to ensure that the above-mentioned approaches and solutions are satisfactorily responding to the needs of the end-users and of the citizens' community at large.

Scope:

The proposed research should focus on the development of technologies for urban security and resilience that, at the same time, intend to reduce the fear of crime and enhance the perception of security of the inhabitants of large urban environments.

Specific attention should be paid to technologically enhanced platforms that allow citizens both to share information and experiences in real-time streaming and to receive alerts and messages from security command and control centres.

The proposed action should take into account sustainable and low impact solutions and, possibly, rely on already set standards and tools. Modularity and security by design should also be in the backbone.

The proposed research should take into consideration past and on-going EU research in this field. The testing and validation of the results from the proposed research should be carried out in several European cities.

Expected impact:

The output of this research should provide concrete suggestions for policy making to address security challenges in large urban environments.

The research results are also expected to contribute to increase the perception of security of citizens by empowering them, fostering their sense of belonging to a greater community and facilitating their engagement to improve the security conditions of smart cities.

Moreover, the research would provide new market opportunities, especially for SMEs and entrepreneurs, to develop and produce innovative technologies for urban security.

Finally, the consideration for a possible wider integration of new and existing digital technologies into sustainable and innovative security solutions is strongly welcome.

Form of funding:
Collaborative Project 100% (Capability project)

12 – Urban security topic 2: Cyber-security and privacy

Specific challenge:

Smart cities are a new reality which is posing serious challenges in terms of cyber-physical security and citizens' privacy and personal data protection. So far the RTD focus on smart cities has been placed in developing solutions for the data sharing cross-sector applications –e.g. transport, energy, etc.-. Limited attention has been placed in security and privacy, and these limited efforts have only been applied on an isolated, sector-by-sector basis.

Scope:

The proposed research shall imperatively address the cyber security and privacy challenges of the complex multi-operator, multi-application, multi-infrastructure, open data ecosystem brought up by the smart cities. It is an environment where sensitive data and mission-critical systems coexist with generic services massively used by society at large.

The proposed research shall provide:

•Research on ICT solutions to the challenges posed by the massive deployment of reliable cyber security and privacy-protecting technologies.

•Development of a methodology and the associated ICT tools to support to both cities wanting to get 'smarter' and those which are already considered as smart cities is secure and respectful with the privacy of their citizens.

•Carrying out of large scale demonstrations of novel solutions involving several application domains of a smart city –including at least mobility and energy-.

The end users of this topic may be:

•City council authorities and operators of municipal services, who should be able to provide more secure and privacy regarding services in a more cost-effective manner.

•Citizens, as very end beneficiaries of a more secure and privacy environment.

Expected impact:

•Smart cities are a global business. Cyber security and privacy protection in this context should be then a worldwide concern. Thus the proposed research should contribute to increase the competitiveness and visibility of European technologies at a global scale.

•SMEs as providers of services and products should be in the corner stone of innovative solutions. Furthermore the proposal shall demonstrate the applicability of the research by set up a proof of concept of the outcome of the project.

Form of funding:
Collaborative Project 70% funding (Capability project)

13 – Urban security topic 3: Countering the terrorist use of an explosive threat

Specific challenge:

Many studies and research projects have been launched until now in order to enhance technology support to counter the terrorist use of explosive at a specific period during the preparation/execution of a terrorist explosive plot. These methods/technologies are from the starting point in a time line the use of intelligence methods to spot individuals/groups projecting to plot such an event, the inhibition of well-known precursors, the detection of specific chemicals and/or bomb factories, the transportation of the bomb or of the element of the bomb or at the latest stage the disruption of the bomb itself.

But up to now, no comprehensive research was undertaken to assess the effectiveness, the efficiency and the cost of all the developed methods/techniques. The main focus of the proposals should be to address this issue.

Scope:

Proposals should address the full time line of a terrorist explosive plot. At each period of the time line, the project should assess the effectiveness of the supporting method/technology used to counter the threat at that period using credible scenarios based on real cases.

Expected impact:

The research should help Law Enforcement Agencies (mainly anti-terrorist units and bomb disposal units) to make proper choices taking into account the specificities of their countries with regards to this particular threat.

Form of funding:
Collaborative Project 100% funding (Capability project)

Ethical/Societal Dimension

14 – Ethical/Societal Dimension Topic 1: Factors affecting (in-) security - Phase 1 Demo Project

Specific challenge:

Security has been defined as a subjective phenomenon that changes within society. Information on people's understanding of security issues, their perception of security as well as the relevant facts about the risks and dangers they face, may vary according to the level of assessment, be it public or personal (individual). Furthermore, people's feelings of insecurity and their perception of the importance of security can be different in diverse demographic groups. Persons who are amongst best protected and most secure in the society are likely to have expectations of security much higher than poorer, less protected persons.

Scope:

Research should be based on real life examples and address factors affecting public and personal assessment of (in-) security. Furthermore, taking into account past and on-going EU research, this action should aim at collecting analysing studies and data demonstrating this division. Tools necessary to reduce public and personal perception of insecurity should be examined. Proposers are also encouraged to focus on different demographic groups in order to verify how aspects such as: gender, age, income, occupation, education or kind of a lifestyle, affects the feeling of (in-) security. Furthermore, the anthropological dimension should also be considered.

Expected impact:

Better understanding of factors defining public and personal assessment of (in)security. Research should lead at explaining how demographic background influence the feeling of (in)security. Both research outcomes should help improve the strategic security planning.

The project should aim at identifying research priorities for a major real-life phase 2 project (2016).

Form of funding:
Coordination and Support Actions 100% funding

15 – Ethical/Societal Dimension Topic 2: Enhancing cooperation between law enforcement agencies and citizens - Community policing

Specific challenge:

Community policing is a value system followed by a police department, in which the primary organizational goal is working cooperatively with individual citizens, groups of citizens, and both public and private organizations in order to identify and resolve issues which potentially affect the liveability (quality of life) of specific neighbourhoods, areas, or the city as a whole. Police departments which are 'community-based' acknowledge the fact that the police cannot effectively work alone and must partner with others who share a mutual responsibility for resolving problems. Community policing aims at stressing prevention, early identification, timely intervention, as well as better crime reporting, identification of risks, unreported and undiscovered crime. Individual police inspectors are encouraged to spend considerable time and effort in developing and maintaining personal relationships with citizens and different community organizations.

Scope:

Research in this area should focus on indicating best practices for co-operation between police and citizens (communities at different level). Moreover, the proposed actions, taking into account past and on-going EU research, are expected to analyse "community policing" as an opportunity to use a community to observe their environment identify risk and exchange information.

Expected impact:

The output of this research topic should help determine effective and efficient tools, procedures and approaches to strengthen community policing principles. This concept based on collaboration and coordinated activities should be analysed as a system aimed at facilitating information sharing and trust building. Proposers are encouraged to focus on trainings, awareness raising and information sharing activities both, for police and citizens involved. One of the most relevant impacts of the proposed research should be developing a technology (e.g. application of smart phones) which will facilitate, strengthen and accelerate the communication between two groups by making it possible for community representatives to identify the risk and immediately report it to the police forces.

Form of funding:
Collaborative Project 100% (Capability Project)

16 – Ethical/Societal Dimension Topic 3: The role of new social media networks in national security

Specific challenge:

The internet has become a central part of modem life. Omnipresent social media, especially media sharing platforms, chat sites, web forums, blogs radically change the way current societies operate. That is why these instruments attract more and more often attention from national security planners.

Scope:

This topic shall look at the role and purpose of social media and the relationship between the new social networks and national security. Research may focus on analysing the following issues:

- To what extent are social media likely to influence national security planning?
- Shall the adoption of social media across the national security community be treated as a threat or a tool for national security purposes?
- Shall the potential of social networking tools be explored by national security agencies for example in order to predict future trends or identify possible threats?

Expected impact:

Stakeholders should get a better understanding of the impact of social media for national security purposes. Proposers are encouraged to assess the positive and negative aspects, challenges and opportunities of engaging social media as well as how these tools could be used by national security planners.

Form of funding:

Coordination and Support Action 100% funding

17 – Ethical/Societal Dimension Topic 4 - Understanding the underlying social and economic aspects of the genesis, methods and motivation of organized crime (including cyber related offenses)

Specific challenge:

There is a need for a deeper understanding of processes that lead to organised crime, including cyber related offenses. This needs to be examined from a social science and economic perspective.

Scope:

Research should into the role of friendships, kinships, milieus and peer groups of (social) networks and social media in the progression of individuals who had unremarkable and ordinary lives. Research should also look into communication processes within and between networks as well as into processes that leads from a violent/extreme organization or individual into terrorist cells.

Proposers need to develop solutions in compliance with European societal values, including privacy issues and fundamental rights. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be taken into account in a comprehensive and thorough manner.

Expected impact:

Research should lead to insights into the origins and development of violent and terrorist networks as well as enhance the capability to identify them in an early stage.

Form of funding:

Coordination and Support Action 100% funding

Disaster resilient societies

Contents

Crisis management

1. Crisis management topic 1: Demonstration activity on potential of current measures and technologies to respond to extreme weather and climate events

Specific challenge:

Extreme weather and climate events, interacting with exposed and vulnerable human and natural systems, can lead to disasters. According to the Intergovernmental Panel on Climate Change (IPCC), some types of extreme events (e.g. flash floods, storm surges) have increased in frequency or magnitude, and in the meantime populations and assets at risk have also increased, leading to enhanced disaster risks. Besides the need for better forecasting, prevention and preparedness, improved measures and technologies are needed to better manage the immediate consequences of weather- and climate-related disasters, in particular regarding emergency responses.

Scope:

Research and demonstration should focus on the potential of current measures and technologies to respond to extreme weather and climate events (including local measures) affecting the security of people and assets. Research should focus on emergency management operations and cover the whole crisis management, linking early warning to effective responses and coordination with first responders, including the use of adapted cyber technologies to gain time and improve coordination in emergency situations.

Expected impact:

The demo should help improving emergency responses to extreme weather and climate events, in particular gaining time and efficiency regarding coordination of emergency reactions in the field.

Form of funding:

Collaborative Project 70% funding (Integration Project)

2 Crisis management topic 2: Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRNE contamination with dual-use applications

Specific challenge:

A fast detection of CBRNE substances using traceable tools is essential to gain time in the triage of victims in case of accidents or terrorist attack. Research on traceability and monitoring of a large number of people in case of a massive CBRNE contamination is therefore needed in order to differentiate between contaminated or not contaminated persons on-site or in hospital zones.

Scope:

The objective of this topic is to integrate existing tools and procedures along with the development of novel solutions in order to rapidly determine, in case of accidents or terrorist attack, if victims are contaminated or not (by a CBRNE contaminant) as well as the level of contamination / exposure (including making use of point of care diagnostic tests), establish a decontamination / treatment / medical follow up based on the level of contamination / exposure, ensure the tools and procedures fit in overarching search & rescue systems, establish guidelines for hospitalisation and admission to intensive care units (or other specific units) based on the contamination evaluation. The Ethical implications and social acceptance of the proposed solution needs to be studied.

Expected impact:

Breakthrough on detection and monitoring capabilities to the benefit of first responders, civil protection and public health services. In addition, a new integrated, interoperable and centralised system approach involving all stakeholders in case of a mass contamination. Dual-use applications will be considered with possible synergies being established with the European Defence Agency.

Form of funding:

Collaborative Project 70% funding (Integration Project)

3 Crisis management topic 3: Demonstration activity on large scale disasters' governance and resilience of EU external assets against major identified threats or causes of crisis

Specific Challenge:

Governance regimes tend to lack integration when facing large-scale disaster events. State-civil society relationships, economic organization, and societal transitions have implications for disaster governance. Various measures can be employed to assess governance and resilience of major natural and man-made disasters against identified threats or causes of crisis. However, more research is needed in this nascent field of study on factors that contribute to effective governance of major crisis, including risk analysis and cost modelling. In particular, demonstration is needed to develop the concept of on-field management of international and humanitarian crises operations, including civil protection assistances, deployment (before and after a crisis) of EU teams, materials and services, possibly repatriation of EU citizens, as well as their protection and the protection of EU assets.

Scope:

The demo would aim at demonstrating the EU capability to develop, test and validate crisis management systems which could be applied in real situations outside the EU. The research should take into account the consequences of poor and/or late situational awareness reducing the ability to comprehend the scale of a crisis, it should also consider the whole management chain from the detection of a crisis event to the delivery of information to the remote centre from here to the responders on site, moving through the mobilization of responders and support of field users, the planning of actions and the prioritization of efforts within emergency scenarios, combining dynamic data (from sensors, aerial networks etc.) with static information (maps, infrastructure, assessment templates) enabling a better risk assessment and improved decision-making. Interoperability and dual-use applications should be considered as well as health, environmental, legal and ethical aspects.

Expected impact:

The demo would aim at demonstrating the EU capability to develop, test and validate crisis systems which could be applied in real situations outside the EU. This should impact on the rapidity of assessment and feedback of data to coordination centres, effective communication and coordination of response actions and sharing information with the public. This would certainly contribute to boost the competitiveness and visibility of EU crisis services and product suppliers.

Form of funding:
Collaborative Project 70% funding (Demonstration Project)

[TO BE DEVELOPED FURTHER]

4 Crisis management topic 4: Feasibility study for strengthening capacity-building for health and security protection in case of large-scale pandemics – Phase I Demo

Specific Challenge:

Emerging diseases and their pandemic potential pose a great security threat at national and EU level, particularly in the era of globalization when disease can spread more rapidly than in previous eras. Thirty four percent of all deaths worldwide are now attributable to infectious disease, while war only accounts for 0.64 percent of those deaths. Improving capacity-building is key to fight epidemics and the European Union must increase its efforts to improve domestic and global risk assessment, surveillance, communication capability and governance. Additionally, reducing disease transmission through public education and related measures is also crucial to minimizing pandemic impacts, i.e. for health security and protection in case of large-scale pandemics, further capacity-building is essential.

Scope:

Based on the consolidation and exploitation of results, tools and systems from previous R&D efforts and building on existing projects, the overall aim is to develop innovative concepts. Approaches should integrate relevant research as well as aspects related to risk assessment, communication and governance. Concepts should be developed with a view to cross-border approaches. The project should aim at identifying gaps and research and priorities to be addressed in a second phase focusing on demonstration.

Expected impact:

Identification of research gaps and priorities for improving capacity-building at transnational level with a view to prepare for a demonstration project including all relevant actors, including SMEs.

Form of funding:
Coordination and Support Action 100% funding

5 Crisis management topic 5: Situation awareness of Civil Protection decision-making solutions – preparing the ground for a PCP

Specific challenge:
The Lisbon Treaty contains specific and important changes regarding Civil Protection that provide competence to the EU to: a) carry out actions to support, coordinate or supplement the actions of Member States at national, regional and local level in risk prevention and preparation; b) promote swift effective cooperative action within the EU between national civil protection services; c) promote consistency in international activities, including transnational crisis management. A comprehensive European approach on security issues based on the capitalization of knowledge existing at EU and national will considerably help the development and implementation of harmonized Civil Protection decision-making solutions.

Scope:
The study should carry out a survey leading to a mapping of new and promising Civil Protection decision-making solutions developed in the 7th Framework and national programmes in transnational crisis management situations, including in fast developing and changing crisis situations.

This should prepare the ground for a future PCP for civil protection solutions, including public-private cooperation at local, national and EU level, with a view to test technological solutions and protection, deployment and intervention equipments (e.g. tents, relief equipments, basis needs supply, Remotely Piloted Air System (RPAS)) and tools (e.g. situation awareness) in order to make them more cost effective and interoperable.

This coordination action should thus:

- exchange experiences between (public) stakeholders on civil protection and create a network of potential procurers;
- initiate a concrete debate on the mid-to-long term public needs that would require the development of new civil protection technology solutions with a potential role for pre-commercial procurement strategies; and
- create a roadmap for a future PCP topic to be included for an upcoming Horizon 2020 secure societies research call.

Expected impact:
Preparing the ground for a PCP, improvement of emergency responses with better knowledge of existing technological solutions, perspectives for large testing of CP solution with the view to improve decision-making solutions at national and European levels.

Proposed instrument:
Coordination and Support Action 100% funding

Additional condition:
At least 3 Member States relevant public authorities

6 Crisis management topic 6: Addressing standardisation opportunities in support of increasing disaster resilience in Europe

Specific challenge:

Increasing Europe's resilience to crises and disasters requires an orchestrated set of actions across the value chain, including standardisation. While dedicated research projects and new topics look into different aspects of resilience to be investigated and further developed, at the same time related opportunities and needs for European standardisation to support disaster resilience have to be addressed. Such standardisation activities could e.g. significantly improve the technical, operational and semantic interoperability of command, control and communication systems for crisis and disaster management, or the interoperability of detection equipment and tools in the areas of CBRNE. Research should support the identification and further elaboration of potential standardisation opportunities and needs in those technological areas where a significant contribution to improve the disaster resilience in Europe through standardisation can be expected.

Scope:

Proposals could address the areas of crisis management / civil protection and/or CBRNE, including sub-sets of both areas. Proposals need to assess the feasibility and the expected impact of the proposed standardisation activity, the appropriate standardisation deliverable(s) and the expected time frame to finish the proposed activity. Relevant legislation on EU and Member State level need to be taken into account appropriately, including potential ethical, societal and privacy issues of the proposed activities. Proposals need to show how duplication of efforts with relevant past or on-going EU research projects, and standardisation activities on European (e.g. CEN/TC 391) and international level (e.g. ISO/TC 223) will be avoided, how a cross-fertilisation of work between the proposal and these relevant activities will be achieved and how the proposal consortium intends to involve itself in relevant CEN and/or ISO TC's.

Expected impact:

Improved disaster resilience of EU population, crisis management / civil protection and/or CBRNE systems, tools and services, and reduced fragmentation of the respective EU market(s).

Proposed instrument:

Coordination and Support Action 100% funding

7 – Crisis management topic 7: Accelerated Open topic for Small and Medium Enterprises: “Combating lethal pathogens”

Specific challenge:

The accidental or intentional release of pathogenic viruses or bacteria in densely populated areas could have catastrophic consequences. Biothreat agents can be dispersed in air, water or food and are extremely difficult to detect, identify and remove. In the event of a biological attack of other contamination incident, fast and reliable detection and decontamination tools have to be made available to laboratory technicians. SMEs are at the front edge of the development of detection devices for lethal pathogens and of decontamination tools for personnel and/or facilities in the event of accidents or terrorist attacks threatening security. Proof of concept of existing prototypes developed by SMEs is needed to demonstrate their applicability with a view to boost their near-term commercial impacts.

Scope:

The objective is to carry out small-scale demonstration of detection and decontamination tools for lethal pathogens with a focus on prototypes developed by SMEs. In this respect, at least 70% of the EC contribution should go to eligible SMEs. Small size projects are encouraged with possibility of one-year duration.

Expected impact:

Projects should enable to accelerate innovation and reduce time to market. It is expected that solutions with potential for significant near-term commercial impact will be developed. Potentials for spin-off applications in non-security sectors will be considered as positive.

Form of funding:

Collaborative Project 70% funding (Capability Project

8 – Crisis management topic 8: Crises and disaster resilience – operationalizing resilience concepts

Specific challenge:

To increase Europe's resilience to crises and disasters is a topic of highest political concern in the EU[1] and its Member States. While the term 'resilience' can be described as "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions." (UNISDR, 2009), it is necessary to break down and practically apply this definition to the different security sectors. Resilience concepts namely need to be developed for critical infrastructures (supply of basic services like water, food, energy, transport, housing/ shelter, communications, finance, health), but also for the wider public to integrate and address human and social dynamics in crises and disaster situations, including the role of the media. Moreover, as resilience management and vulnerability reduction are closely related, it is necessary to link the on-going efforts to harmonise and share EU-wide risk assessment and mapping approaches[2] with relevant resilience management approaches, to ensure that risk assessment is followed by the development of resilience concepts in the various security sectors, based on the results of the risk assessments.

Scope:

Research should first survey worldwide approaches how to define, develop, implement and evaluate resilience concepts. In a second step, promising implementation approaches should be identified for one or more of the security sectors mentioned, and/or the public, and assessed regarding their potential to serve as a basis for a general guideline on resilience assessment and implementation. In a third step, such a general resilience management guideline should be developed, linked with the EU Risk Assessment Guidelines, and operationalized in one or more of the security sectors, and/or the public. The successful pilot implementation of the developed guideline need to be demonstrated and tested in an operational environment. Findings from relevant FP7 projects like e.g. PEP (Public Empowerment Policies for Crisis Management), or ENSURE (Enhancing Resilience of Communities and Territories facing natural and Na-tech hazards) need to be taken into account, and integrated into the research where possible. Furthermore, a close collaboration with the major EU demonstration project on aftermath crisis management (SEC-2013.4.1-1, expected to start in 2014) should be sought, in order to avoid duplication of efforts and to facilitate cross-project contributions.

Expected impact:

The proposed research should for the first time develop a European Resilience Management Guideline, which through its pilot implementation should facilitate the uptake of risk assessments through Member States and Critical Infrastructure Providers to increase their crises and disaster resilience, in a more coherent way.

Form of funding:

Collaborative project 100% funding (Capability project)

[1] COM(2010) 673 final, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe

[2] SEC(2010) 1626 final, Risk Assessment and Mapping Guidelines for Disaster Management

9 – Crisis management topic 9: Trans-national co-operation among NCPs Security

As a complement to the cross-cutting NCP networks focussing on quality standards, benchmarking and legal/financial training, the Security NCP network should focus on sharing good practices related to security specific issues.

The Security NCP network should also organise trans-national brokerage events on a regular basis and on the demand of the Commission.

The aim is to make the existing NCP network more efficient and effective.

Form of funding:

Coordination and Support Action 100% funding

Critical Infrastructure Protection

10 Critical Infrastructure Protection topic 1: Critical Infrastructure “smart grid” protection and resilience under “smart meters” threats

Specific Challenge:

Critical Infrastructure functions are technologically and operationally interconnected, of which their exact possibilities and potential risks need to be better understood. For example: in the case of energy distribution networks, especially "Smart grid", the proliferation of "Smart Meters" by its nature introduces new threats.

Scope:

The objective is to analyse potential new threats generated by “smart meters” on the smart grid system and propose concrete solutions in order to mitigate the risks, improve resilient and reduce vulnerability of critical infrastructure “smart grid”, due for example to cyber-attacks, the interconnectivity with renewable energy grids, etc.

The new technologies, processes, methods and dedicated capabilities shall help protect smart grid infrastructures and shall also take into account the urban areas implications (i.e. the general public subscribing to this service). The research shall provide concrete solutions for securing public and private critical networked infrastructures and services against the above mentioned threats.

It is expected that consortia under this research topic will select the most representative sample of “smart meters” used in Europe’s smart grid as starting point of the research and analyse their potential weakness/threats.

Moreover the proposal shall study and provide solutions in order mitigate the impact of “smart meters” on the current critical infrastructure security and resilience to new threats.

Expected impact:

It is expected that the research output will lead to a systematic approach to resilience enhancements of smart grid critical infrastructures when new components are added. Furthermore a small scale proof of concept of system should be create in order to demonstrate the “resilience” of the proposed “solutions”.

Finally the research should be carried out in the context of policy initiatives at EU level on the Smart Meters and Smart Grids, such as the 2011 CEN/CENELEC/ETSI Mandate 490 on smart grids (including the security and data privacy issues on the roll-out of smart metering systems), and the 2009 CEN/CENELEC/ETSI Mandate 441 on smart meters, as well as the guidance on software in smart meters, provided by WELMEC.

Form of funding:
Collaborative Project 100% funding (Capability project)

11. Critical Infrastructure Protection topic 2: Demonstration activity on tools for adapting building standards and infrastructure in vulnerable locations in the case of natural catastrophes

Specific challenge:

The expected increase of frequency and severity of climate-related natural catastrophes and the current risks of disasters of geological origin pose a serious threat to buildings located in vulnerable locations, including critical infrastructures (i.e. public buildings, such as governmental offices, transport stations, terminals and historical buildings and monuments) along their life cycle. One of the responses to be better prepared to crises related to natural hazards is to adapt building standards and infrastructure in order to limit the risks of demolition, protect critical infrastructure and save human lives in the case of a major event. Complementing current research in this area, and based on the knowledge of risks in vulnerable areas in Europe, building standards should be developed and tested, applying a number of technological means and design procedures. A comprehensive approach should be developed that take into account the security issue from the conceptual design of any building to its operation (in the case of a critical infrastructure) or use (in the case of households). The comparison of different solutions tested should include cost and cost/benefit analyses, and societal implications.

Scope:

The research proposal shall develop methods and tools for adapting building standards in vulnerable locations. Furthermore the research proposal shall demonstrate its finding, taking into account the occurrence of different types of natural (climate or geological) hazards, and including comparative cost and cost/benefit analyses.

Expected impact:

The development of building standards for infrastructures and households located in vulnerable areas will have a clear impact on security of citizens and assets).

Moreover one of the paths to be assesed could be the development of an innovative high performance composite system to protect critical concrete infrastructure against extreme shocks providing high levels of performance in terms of shock absorption, load distribution, concrete confinement, and overall structural capacity.

Other methods could be an appropriate blast simulation, modelling tools and risk assessment methodologies to priorities actions taken in design and operation should be developed and validated to assess the vulnerability of critical infrastructure subject to blast and other threats. Understanding the behaviour of structures to highly dynamic loadings, to the modelling and analysis of shock and impact effects on structures. Design guidelines could be also drafted to disseminate the developed approach.

The topic will complement FP7 research focusing on impacts of extreme weather on critical infrastructure.

Form of funding:

Collaborative Project 100% funding (Capability project)

12. Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator - analysis and development of methods for assessing resilience

Specific challenge:

A better understanding of critical infrastructure architecture is necessary for defining measures to achieve a better resilience against threats (due to human errors or terrorist/criminal attacks).
Moreover a global approach of the resilience on the critical infrastructure should be taken into account, for example: (human factors (i.e. radicalization), security issues, geo-political issues, socio economic issues, etc.).

Scope:

Critical Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The analysis of resilience should therefore not only focus on potential threats caused by attacks or accidents (human error or terrorist/criminal attacks), but also on the expected developments in these areas and the impacts and potential challenges of new technologies.

Therefore the effectiveness of a resilient critical infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event (human error or terrorist/criminal attacks). The proposed research shall demonstrate that a set indicator could be applied to critical infrastructures in order to assess its level of “resilience”, moreover a scale approach of “resilience” level should be proposed across critical infrastructures (power grid, water, etc.).

Expected impact:

Therefore the proposed research should analyze different areas of critical infrastructures (energy grid, water supply, transport, communication, etc.) and propose a comprehensive methodology that uses uniform and consistent data from known Critical Infrastructure Protection threats to develop a resilience level based on summations of various "indicators" (technical and non-technical, i.e. human factors).

Furthermore the proposal research outcome should select at least two types of critical infrastructure as test case and apply the above methodology in order to demonstrate its applicability.

Form of funding:

Collaborative Project 100% funding (Capability project)

13. Critical Infrastructure Protection topic 4: Protecting potentially hazardous and sensitive sites/areas considering multi-sectorial dependencies

Specific challenge:

There is a need to better understand how society as a whole might be affected by risks of accidents from potentially hazardous substances to enable effective protection measures to be developed. In this respect, the breadth of impacts from Seveso sites/areas has to be investigated, considering multi-sectoral dependencies. This implies developing knowledge on multiple types of sectors and socio-economic conditions around Seveso sites/areas that might be affected by accidents, taking into account the type of sites/areas, CBRNE substances of concern, the vulnerability of various sectors and their dependencies/interactions and of the population, and scenarios mimicking different levels of severity of impacts.

Scope:

Research should focus on the development and testing of qualitative methods that involve identifying links between sectors (multi-sectoral dependencies) and evaluating how impacts from a Seveso type accident might affect them. Quantitative impact assessment tools should also be developed to evaluate socio-economic impacts of such accident. Research outputs should enable to improve or design protection measures for a better preparedness to Seveso site/area related accident. Small-scale demonstration activities focusing on SMEs should be considered.

Expected impact:

The research and demonstration should enable to help policy-makers and other stakeholders to understand how multiple sectors, community, region or nation could be affected in total by an accident from a Seveso site/area, and what the total impact might be. This can be useful to understand the potential severity of a CBRNE accident and develop adequate protection measures in the light of established policy goals. In addition, risk assessment studies should enable to evaluate different sectors, regions or populations compare them in terms of relative vulnerability to help set priorities that can guide the allocation of protecting measures financing appropriately.

Form of funding:

Collaborative Project 70% funding (Capability project)

14. Critical Infrastructure Protection topic 5: Cybercrime on Industrial Control Systems protection - Advanced Persistent Threats (APTs)

Specific challenge:

Industrial and Automation Control Systems (IACS) constitute the foundations of key strategic and critical sectors according to the Council Directive 2008/114/EC and the EU Internal Security Strategy, such as Energy, Oil and Gas, along with Water and Chemical. Those sectors provide a critical service to citizens and countries and the threat of sabotage through a specific and lead driven attack may represent a major drawback to an individual or to the Economy. Electricity service, for instance, is crucial because involves more than a country.

Scope:

IACS are no longer isolated siloes, they are fully integrated with corporate ICT infrastructures there is therefore a connection between both infrastructures, at the same time there is a lack of awareness regarding ICT risks that can affect IACS. An attack to ICT assets can spread, to IACS jumping to SCADAs and Control Centers. Specific attacks like Stuxnet have demonstrated existing and unmanaged vulnerabilities and today there is a new kind of risk called Advanced Persistent Threats (Stuxnet as an example), where hackers know exactly where to hit, with unlimited resources at hand.

In order to increase European Critical Infrastructures resiliency and availability, a new approach to those APTs is needed. IACS and SCADAs design does not address cyber-attacks and IT risks by conception, their vulnerabilities are therefore easily exploitedable.

Currently the Information Security Market is not providing technology solutions to mitigate APTs for IACS.

The topic aims to design and develop ICT security technologies to be integrated into SCADAs and IACS Control Centers, mainly software and hardware updates. It would allow extending existing published standards and methodologies to address the new APTs for IACS modus operandi scenario.

European Critical Infrastructures, operating locally or internationally, should be the end users, especially those named European Critical Infrastructures by the Council Directive above.

Expected impact:

European industry will benefit from cyber security improvements due to present and future cyber-attacks protection, increasing availability and resiliency, showing a stronger state to dissuade penetration attempts.

Economy will avoid panic situations after cyber-attacks against key economy actors

SMEs will provide specific and very focused security services such as fine tuning, security assessments, APT digital surveillance and many more are essential to ensure a successful and innovative solution. Liaison should be done with previous security research.

Form of funding:
Collaborative Project 100% funding (Capability project)

15. Critical Infrastructure Protection topic 6: Improving the aviation security chain

Specific challenge:

Security in aviation is particularly provided by the security chain implemented on airports (checkpoint, hold baggage, cargo, etc.). Compliancy of airport security operators with EU and national regulations is mandatory, and generally addresses equipment and procedures. However, the balance of benefits (e.g. perception of security) and the actual security provided (deterrence, detection, response), and costs of implementing security in the widest sense is under constant debate. While guidance and compliance is currently at low integration levels (e.g. equipment), security provided at the level of the airport as a whole should be the driving factor for development, regulations, and implementation. Regulation compliance of security at system level instead of at equipment and procedures level is promising in terms of foreseen benefits for the operator, the equipment manufacturer and the regulator. Risk-based security is an approach where acceptable (or improved) levels of overall security can be achieved, while differentiating security measures applied on the basis of risk levels. This may allow a reduction in the cost of security through reduction in numbers (of people, bags, etc.) to be screened and screening delays. It requires risk levels to be assessed and applied to categories of people, flights, destinations, airlines, and so on, where application to individual or groups of people raises concerns with regard to ethics and fundamental rights. It also requires a thorough understanding of the relation between risk levels assessed and security levels provided, and flexibility in implementation of security systems. Such fundamentals need to be better understood, including related global initiatives (e.g. trusted traveller programs).

Scope:

Future aviation security chain approaches leading to higher benefits including higher level of security and their impact should thus be developed and tested at airports. Realistic cost-benefit analyses of proposed solutions should be undertaken to help to identify promising and reasonable approaches. The R&D work should include an analysis how information from one part of the security chain can be used in other parts of the chain, particularly when including border control and customs, whereas the process of dynamically assessing risk levels of passengers and cargo could benefit from multiple implemented processes; to develop and test ‘smarter’ combinations of security subsystems, namely of detection equipment, such as fusion or non-thresholded detectors and risk level approaches which provide better true positive/ false positive response rates; and how to maximize deterrence as an valuable part of the effectiveness of security measures, where unpredictability is key, without reducing security by detection. Finally, effective implementation of risk-based security approaches should be proven through trials with a strong ethical fundament. Findings from relevant, ongoing FP7 projects need to be taken into account.

Expected impact:

Approaches for future aviation security chain should lead to higher benefits including higher level of security and impact, by being systematically investigated, prioritized, developed and tested.

Form of funding:

Collaborative project 100% funding (Capability Project)

Communication technologies and interoperability

16. Communication technologies and interoperability topic 1: Information management, systems and infrastructure for civilian CSDP missions

Specific challenge:

Considering the range of civilian CSDP missions in complex environments, the ability to efficiently manage information and resources is a key factor in all the phases of crisis management, from early warning up to “the-lessons-learned’ phase, and the discontinuing process throughout. There is a need to research C2 processes, information management, systems and infrastructure within the context of CSDP with a view to developing coherent and interoperable processes, tools, technologies and capabilities to improve the planning and conduct of crisis management operations.

The development of a Situational Awareness and Operation Control Platform (SAOCP) will improve cooperation among different EU actors and with Member States, with the possibility to involve also other international organisations, and in particular EU partners in crisis management, notably UN, NGOs, etc.. The needs of end-users will be a focal point of the proposed coordination action.

Scope:

Proposals should address the development of a specific and dedicated research agenda, including the technical specifications which will serve as basis for the future development of a Situational Awareness and Operation Control Platform (SAOCP). This platform should allow end-users to enhance their common understanding of crisis management in EU civil CSDP missions. It should also improve the management of the EU resources' allocated to combatting crisis and help federating the Community of Interest (CoI) amongst CSDP entities.

Based on a stocktaking of the existing system, the research is expected to focus on the definition of services, interfaces, formats and protocols for sharing selected objects of relevance consumed or produced by the CSDP entities. The research is also expected to focus on interoperable, secure, resilient communication services to be deployed and shared by the involved CDSP entities.

Expected impact:

The research should lead to the creation of a strong community of interest. Additionally, the selected proposal should pave the way of a demonstrator, which should be entirely focussed on the needs of the end-users.

Form of funding:

Coordination and Support Action 100% funding

17. Communication technologies and interoperability topic 2: interoperable next generation of radio communication system for security use - PCP

Specific challenge:

Until now each EU Member State has adopted its own radio-communication system for the use of its security forces (Police, first responders, etc.) based on similar standards. Unfortunately, most of these systems are not EU interoperable at the technical level. The EU has already funded a number of research projects to help to overcome this issue. The main challenge is now to make a step further and to push the research done to the institutional market, leading to the introduction of innovative, interoperable PPDR communication systems, while preserving the investment done on the currently deployed systems.

The proposed project should take into account the extensive works done so far by other research projects in the field, both in terms of user requirements and of technological solutions proposed.

Scope:

The proposed project must be structured around six different phases, some of which may run in parallel.

1) Technology review and specifications definition

In its initial phase the project will assess the technology developed by various EU-wide or national projects in this area. Special consideration should be given to software defined radio technology. On this basis, the specifications for the next generation of an EU interoperable radio communication system and a set of standard to be used in the following steps, will be agreed upon. All components of the system should be defined, including both the network (base stations, management of the network) and the handsets.

2) Definition of the call for tender

In this phase, the project will develop the core text of the specifications to be used as a toolkit to build national call for tender taking into account the EU common requirement for interoperable PPDR communication systems.

3) The execution phase

In this phase, the solution providers will do their implementation work according to the provisions of the call for tender, working under the supervision of the concerned participating public authorities.

4) Definition of the Validation Centre

In this phase, the project will prepare the specifications for a common EU Validation Centre to validate the radio-communication technology developed during the procurement phase for the replacement radio communication system.

5) Establishment of the Validation Centre

In this phase the project will contribute, to establish the Validation Centre according to the specifications laid out in the previous phase. Sustainability of the Validation Centre beyond the lifetime of the project should be addressed, both with respect to its legal status and its funding sources.

6) Testing and validation

In the last phase the project will launch a number of interoperability tests for voluntary countries. These should involve multiple first responder and police agencies from at least three Member States in a cross-border operational setup.

Expected impact:

To create an EU interoperable radio communication system for security forces over the next 15 years.

Form of funding:

Pre Commercial Procurement (100%)

The conditions related to this topic are provided along with the general conditions for this call in Annex.

[THIS TOPIC NEEDS TO BE FURTHER DEVELOPED]

Ethical/Societal Dimension

18. Ethical/Societal Dimension topic 1: Improving protection of Critical infrastructures from insider threats

Specific Challenge:

Critical Infrastructures are crucial assets for the functioning of a society and an economy. Consequently, they can be the target of several threats, in particular terrorist threats.

In this framework, the risk of an insider threat coming from personnel and third party individuals, who have inside knowledge about the infrastructure security practices and/or have access rights to certain key components, data and computer, is particularly high for Critical Infrastructures.

A particular type of insider threat is the one brought along by personnel who have undergone a violent radicalisation process and, as a consequence of that, intend to affect the normal functioning of the infrastructure or, even, to sabotage it.

In order to prevent the latter, it is important to deepen the current knowledge about the main constituents of the violent radicalisation processes to timely detect them and to prevent resulting insider threats to materialize.

Scope:

Research in this area should focus on determining and analysing the main constituent factors of a violent radicalisation process (including family and social environment, psychological factors, religion and ideology, the internet and social media, socio-economic and political factors) as well as on the conditions that can lead a person from ideas to violent action. The proposed actions should take into consideration past and on-going EU research in this field and include, to the extent possible, real life examples of individuals that underwent a violent radicalisation process.

Expected impact:

The output of this research should be directly applicable to support national and local security practitioners to strengthen the protection of national and European Critical Infrastructures from insider threats brought by violent radicals.

In particular, the research results are expected to contribute to shade light on the violent radicalisation processes and paths and to raise the awareness of the security practitioners about the possible early indicators that can allow a timely detection of insider threats brought by violent radicalised individuals.

The development and application of new equipment and systems to support the security practitioners should also be considered by the proposed research.

The research and the usable results should consider fundamental rights protection, comparative studies of international laws, ethical and societal impacts, with particular consideration for EU anti-terrorism and Critical Infrastructure Protection (CIP) policies.

Form of funding:
Coordination and Support Action 100% funding

19. Ethical/Societal Dimension topic 2: Better understanding the links between culture and disasters

Specific challenge:

Culture is the characteristics of a particular group of people, defined by everything from a set of values, history, language, religion to cuisine, social habits or music and arts. Preparedness, response to disasters and after-crisis recovery is always influenced by cultural background of individuals and the society they live in.

To this end, cultural factors play also an important role in determining the way people respond to stress and accept disaster relief in an emergency situation. At the same time lack of cultural understanding, sensitivity and competencies can hamper and even harm the professional response to disaster as it is crucial to understand the cultural background of disaster victims.

Considering the significance of cultural influences during a disaster especially in urban areas which become more and more diversified, will help increase the effectiveness of all who respond to disasters, will be of value for policy makers and health professionals working in the areas of disaster management or crisis intervention and consequently will help build a more resilient society by ensuring that cities are better prepared for and able to recover from emergencies.

Scope:

Research in this field may focus on the following issues:

- Which cultural factors, important insights, specific communication styles for a given cultural group should be taken into consideration during disaster situations in urban areas?
- How to anticipate and identify solutions to cultural problems that may arise in the event of an emergency?

Proposers are encouraged to analyse how emotional, psychological and social needs, as well as communal strengths and coping skills that arise in disasters can affect the way certain urban communities prepare, respond and recover from disaster.

Expected impact:

This support action will help in better understanding the links between disaster and culture in urban areas. The research and its results will serve as input to build necessary strategies meeting the needs of various cultures in order to provide disaster relief.

Last but not least, taking into account past and on-going EU research, this project will provide a framework for improving disasters' policies and practices by taking into consideration every disaster victim's cultural and personal uniqueness with a view to contribute to building a more resilient society.

Form of funding:
Coordination and Support Action 100% funding

20. Ethical/Societal Dimension topic 3: Impact of climate change in third countries on Europe's security

Specific challenge:

Climate change in Third Countries is a real threat to security of the European Union. Extreme weather events which devastate lives, infrastructure, but also institutions and budgets can have disastrous consequences on European security, as climate-driven crises occurring outside the EU can have detrimental effects and direct or indirect security implications on the Union (e.g. climate-driven migration forcing large number of people to move from their homelands to another country – EU Member State).

Therefore, adequate political, strategic and institutional responses should be found in order to enhance international and European cooperation on the detection and monitoring of the security threats in Europe related to climate change in other regions of the world. European policy makers and analysts as well as national governments should tackle climate change as today's non-traditional security hazard.

The research and consecutive execution of the project has as its aim facilitating the adoption of a comprehensive approach, which will provide a way to consider risks and vulnerabilities in order to take necessary steps to give more attention to the impact of climate change on security and at the same time will help minimise negative consequences of climate-driven crises.

Scope:

Research in this field may focus on the following issues:

- What kind of instruments, tools, and actions can be used alongside mitigation and adaptation policies to address the climate change security risks? Proposers shall analyse the impact of environmentally induced migration (temporary or permanent), new type of refugees concept; climate refugees from Third Countries territories that could provoke tensions or civil disorder affecting security in the EU.

- Which could be the most efficient ways of developing contingency plans for the EU's response to the effects of climate-driven crises occurring outside the Union that have direct or indirect security implications on the Union?

Proposers are encouraged to analyse how early warning and early preventive action depend on adequate human resources and methodology as well as to study common criteria for analysis, risk assessment and possibilities of setting up of a joint alert system.

Expected impact:

This action will help to better understand consequences of climate change events in Third Countries on security implications in the EU.

Taking into account past and on-going EU research, this topic should thoroughly examine the impact of climate-driven crises on European security in order to provide a framework for improving situation analysis and policy planning at the EU level.

Form of funding:
Coordination and Support Action 100% funding

Border security

Contents

Maritime Border Security

1. Maritime Border Security topic 1: Deployable high frequency (HF) long range radar systems for coastal and pre-frontier areas, and in support of search and rescue operations

Specific challenge:

The challenge refers to early and long distance border surveillance. Research is needed in the development of high frequency (HF) surface wave and sky wave Over the Horizon (OTH) radars of improved performance, reduced cost, lower power requirements, deployable (for possible combined use for a more complete and flexible border surveillance system). These technologies are expected to be appropriate to support Search-and-Rescue (SAR) operations in the Mediterranean Sea.

Scope:

Pre-competitive research is expected to involve the various stages of development, from sensor design, to the analysis and design of system configuration (taking into account the spatial and time performance variability caused by ionosphere behaviour), the integration and validation by (public) authorities for target detection, identification and recognition. A validation workpackage should therefore be foreseen in a realistic SAR operational scenario.

Expected impact:

This topic would contribute directly to the development of the European Border Surveillance System (EUROSUR). HF technology provides extended coverage over the coastal marine band radars, potentially reaching pre frontier detection, thus proving appropriate for the three main missions of EUROSUR, particularly the third which refers to the reduction of the current death toll at high seas through the extension of SAR capability in a flexible way.

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding: Collaborative Project 70% funding (Capability Project)

2. Maritime Border Security topic 2: Low cost and "green" technologies for EU coastal border surveillance

Specific challenge:

The use of low cost and "green" technologies is expected to become mandatory for future border control systems in environmentally sensitive areas. Systems of passive (or low emission) radar technologies provide promising results for the detection of targets in areas that cannot be covered by active systems. Passive radars offer different advantages, such as lower detectability and cost and the possibility of use practically anywhere.

R&D is needed to better apply this technology to the environment of maritime surveillance, also in combination with IR and EO cameras and acoustic systems, and using the signals coming from existing coastal systems.

Scope:

The areas of research and development are expected to include, among others:

1. further development of the passive devices based on different active sources
2. development of specific tracking algorithms based on passive sensors
3. development of specific fusion algorithms for combined passive and active sensor systems
4. use of passive sensors for maritime targets and environment
5. use of passive sensors on mobile platforms
6. operation in network configurations together with other IR/EO and/or acoustic systems exploiting the data fusion potentiality for improving surveillance performances.

Expected impact:

This topic would contribute directly to the development of the European Border Surveillance System (EUROSUR).

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding:

Collaborative Project 100% funding (Capability Project)

3. Maritime Border Security topic 3: Light optionally piloted vehicles for maritime surveillance

Specific challenge:

Beyond coastal waters, surveillance tools such as Off-shore Patrol Vessels (OPV) and Maritime Patrol Aircrafts (MPA) are oriented to image and position the acquisition of targets by mobile assets. Occasionally, medium size helicopters are used to survey the area (typically situated between 20 to 100 NM off coastal line). However, their performance is limited if these are not equipped with maritime surveillance radars. However, MPAs and helicopters have very high operational costs, and this undermines their cost effectiveness to continued surveillance.

Unmanned Aerial Vehicles are also foreseen to have a major impact on the surveillance of remote areas, but their high cost and lack of regulations to fly outside a segregated air space impose some difficulties and limitations to their utilization.

Therefore, this R&D is targeted to extend the portfolio of light surveillance platforms with a reduced operational cost, for increased capability in surveillance in high seas (to be tested in the context of a real operational scenario, such a Frontex led joint operation), e.g. by developing appropriate low weight/high performance radars with Marine Moving Target Indication (MMTI)/SAR and data fusion/correlation capabilities.

Scope:

Research on required technologies and systems may include:

1. Maritime radar technologies for detection and early identification of targets.
2. Electro-optical technologies, allowing identification and tracking of targets.
3. Affordable aerial platforms compliant with current regulations.
4. Collaborative system to perform joint operations.
5. Mission control system integrating the information acquired by all sensors, allowing its control and managing ground station communication.
6. Reliable and long range communication channels.
7. Improvement of Ground Control Station communications, reducing costs and providing the possibility to be mobile.
8. Integration of ground control station with legacy maritime surveillance system.
9. Improved sensors for detection, identification and tracking.

Expected impact:

This topic would contribute directly to the development of development of the Common Information Sharing Environment (CISE) at sea initiative, as included in the final steps of the European Border Surveillance System (EUROSUR).

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding: Collaborative Project 100% funding (Capability Project)

4. Maritime Border Security topic 4: Detection of low flying aircraft at near shore air space

Specific challenge:

The deployment of maritime surveillance system for border control has exerted pressure on smugglers in the last years. Drug smugglers reacted by changing their modus operandi using low flying aircrafts to cross borders undetected. As an example, this situation has been identified as a major gap to combat drug smuggling entering through the south coast of Spain.

In this case the typical scenario (in line with the concepts of operations being defined by the Frontex agency) is a small low flying aircraft loaded with drugs coming from the North Mediterranean coast of Africa and entering southern European coasts. This kind of aircrafts land in small airports or runways. Landing areas are well known by security forces. Nevertheless, the early detection of these aircrafts is crucial to determine the landing area.

Scope:

Required technologies and systems to be investigated and developed may include:

1. Mobile units which can be quickly deployable in remote areas with communication links with command and control centres.
2. Multi-mode radar technologies for the early detection and tracking of low flying aircrafts.
3. Integration of radar data and correlation with repositories of information to predict most probable landing areas.

The scope and outcomes of this line of research may be applied also to land border security.

Solutions should be validated in a realistic operational context.

Expected impact:

This topic would contribute directly to the development of the European Border Surveillance

System (EUROSUR)

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime such trafficking in human beings and the smuggling of weapons and drugs.

Form of funding:
Collaborative Project 100% funding (Capability Project)

5. Maritime Border Security topic 5: Development of extended capabilities for Automatic Identification System information (AIS)

Specific challenge:

Current efforts aimed to enhance the information contained in the recognised sea picture have shown that AIS inputs constitute a basic element to improve maritime awareness. AIS is also an important tool to contribute to EUROSUR missions and to Search and Rescue (SAR) operations. However, AIS capabilities are limited by the nature of the standard itself, which, in its most extended version, is based in a VHF link.

To implement their concept of "see without being seen", Law Enforcing Institutions operating at sea have shown interest in the development of secure/encrypted AIS, with a view to increase trustworthiness and guarantee reliability. To extend the range and improve capabilities, R&D is also needed in the development of novel surveillance platforms to provide optimal airborne or on board AIS.

Scope:
Developments at the technologies and systems level should be foreseen in the:

1. design and deployment of more effective terminals in the area of satellite AIS;
2. development of processing algorithms/approaches optimizing real time transmission of data/imagery between airborne and surface patrolling assets and optimizing also the satellite reception windows (if appropriate);
3. bandwidth and communication management between command and control centres and mobile platforms participating in operations; and
4. putting in place technical countermeasures against fakers.

Expected impact:

This topic would contribute directly to the development of development of the Common Information Sharing Environment (CISE) at sea initiative, as included in the final steps of the European Border Surveillance System (EUROSUR). CISE is currently being developed jointly by the European Commission and EU/EEA member states in the context of the EU integrated maritime policy.

The aim of EUROSUR is to reinforce the control of the Schengen external borders. EUROSUR will establish a mechanism for Member States' authorities carrying out border surveillance activities to share operational information with a view to reduce the loss of lives at sea and the number of irregular immigrants entering the EU undetected, and increase internal security by preventing cross-border crime.

Form of funding: Collaborative Project (70%) – (Capability Project)

Border crossing points

6. Border crossing points topic 1: Novel mobility concepts for land border security

Specific challenge:

Border authorities are facing new challenges to secure land borders of the EU/Schengen areas, while the recent trends show a significant increase of travellers' flows. In the meantime, travellers are requiring fast and convenient border crossing, therefore pushing authorities to implement novel approaches in order to maintain and even improve the throughput at the crossing points.

Infrastructure for land border checks is not very flexible. As a consequence, improved solutions are required. They could rely on the development of mobility concepts along with traveller programmes that are extensively being developed in order to facilitate border crossing. Moreover, the current wide-spread use of mobile devices such as smartphones or tablets provide potentially exploitable means and distributed Computer Processing Units (CPU) power that could (or could not) be combined with border authorities dedicated mobile equipment to perform identity checking for border security.

Scope:

Research should lead to novel mobility concepts for land border security enabling authorities to achieve higher throughput at the crossing points whilst guaranteeing high security level, enabling fast processing of passengers within vehicles or pedestrians and improving the efficiency of passengers flow management. In particular, the use of passengers' personal mobile devices is expected to enable efficient and reliable identity checks through the application of biometric technology. The ability to automatically detect document forgeries is also expected for further improvements. Projects should therefore aim at proposing novel concepts relying on the use of traveller's personal mobile devices and/or border authorities' specific mobile equipment for high security level passengers' identity control. What is needed is to perform biometric identification of travellers inside vehicles (cars, bus trains) as well as pedestrians. R&D could propose novel technological solutions as well as procedures to manage relevant associated workflows (to be validated by border guards in a realistic operational scenario). An appropriate portable (and, if seemed necessary, fixed) ABC gate for land borders could be developed (if portable, this gate should be movable so that it could be used at lanes outside the terminal). In this research legal, ethical or social implications must be taken into account appropriately.

Expected impact:

All studied scenarios show that in the long term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities will remain a critical capability, given the expected rising cross-border flows of people (and goods).Border control is likely to face increasing demands for efficiency, which implies a need for technical systems that are user friendly and reliable in operational conditions. A general challenge is to make the technical equipment affordable enough to be widely employed. The approach to use technology from adjacent markets such as mobile telecommunications where the volumes of production are very high could help the costs of processing down to a minimum. Harmonization of requirements across Member States (and standardization) is expected to also automatically greatly improve affordability.

Form of funding:

Collaborative Project 100% funding (Capability Project)

7. Border crossing points topic 2: Exploring new modalities in biometric-based border checks

Specific challenge:

The ever-growing number of travellers crossing the EU borders poses a serious challenge to the border control authorities in terms of a reduced amount of time for carrying out border checks. Consequently, efforts have already been undertaken to facilitate the travel of bona-fide and genuine passengers and simultaneously to safeguard high level of security. In particular, in the field of person and document authentication and/or verification deployment of biometric-based approaches led to significant advances as regards making the border control processes more efficient. Further explorations going beyond state-of-the-art biometric-based person identification detection techniques are expected to contribute to making the daily work of border control authorities more efficient and to significantly facilitating non-EU citizens in crossing EU external borders.

Scope:

Research is needed in order to explore whether it is possible to use other biometric data (potentially already used in another context and in another domain) than fingerprint, iris or picture to store in the e-Passport chip, which would guarantee the same or higher level of security, but would be more accurate and can be retrieved in a more efficient manner than in the case of the conventionally used biometric data types. For instance, the feasibility of storing DNA-string in the e-Passport chip and capturing the DNA on a glass plate or a capturing filter could be explored. While the introduction of new biometric-based modalities in the process of person identification might lead to making this process more accurate and efficient, an integral part of the research should also embrace related ethical, societal and data protection aspects.

Expected impact:

Non-EU residents contributed €271 billion to the economy of Member States when travelling to the EU in 2011. Business travellers, workers, researchers and students, third country nationals with family ties to EU citizens or living in regions bordering the EU are all likely to cross the borders several times a year. Making it as easy as possible for them to come to the EU would ensure that Europe remains an attractive destination and helps boosting economic activity and job creation.

Form of funding:
Collaborative Project 100% funding (Capability Project)

8. Border crossing points topic 3: Improving border checks at railway Border Crossing Points

Specific challenge:

Border Control authorities are facing various new challenges resulting from an ever-growing number of travellers crossing the EU borders. In particular, it has been acknowledged that carrying out border checks at railway Border Crossing Points (BCP) poses problems in terms of very limited time for processing and retrieving information related to a person being checked and the specific conditions in which checks are carried out (movement of the train over long distance) which impacts the performance. Although mobile document readers are already on the market and are being successfully deployed on trains, the entire border check process at railway BCP and on trains might and often does require retrieving information from numerous information systems, not necessarily available at hand, and whose obtaining is time critical.

Scope:

Research is needed in order to explore new technical solutions that could allow carrying out border checks at railway BCPs and on the trains in a more efficient manner, while preserving a high level of security. In particular, elaboration of a concept, development and testing of ”all-in-one” mobile terminal that could reduce the information processing and retrieval time should be undertaken. The potential solution should be highly flexible, namely, it should not only take into account all related existing and emerging national and EU-level information systems (e.g., EES), but also integration/linking to future systems. Similar-in-nature scenarios to railway BCPs could be considered too.

Expected impact:

Non-EU residents contributed €271 billion to the economy of the Member States when travelling to the EU in 2011. Business travellers, workers, researchers and students, third country nationals with family ties to EU citizens or living in regions bordering the EU are all likely to cross the borders several times a year. Making it as easy as possible for them to come to the EU would ensure that Europe remains an attractive destination and help boosting economic activity and job creation.

Form of funding: Collaborative Project (100%) - (Capability Project)

9. Border crossing points topic 4: Optimization of border control processes and planning

Specific challenge:

Apart from the known problem of a continuous increase of travellers crossing EU external borders border control authorities are confronted with a wide range of other problems, including: (a) less staff and financial means in the nearby future, (b) emergence of new technologies that are supposed to support border control authorities in carrying out border control and surveillance tasks, and (c) an ever-growing amount of information available to them coming from various sources (e.g., national or international information systems, sensors, open sources, etc.). Having “less people”, but “new tools and machines” and “more information available” requires establishment of mechanisms to improve decision making processes in the context of planning resources allocation and information workflows.

Scope:

Research is needed in order to conceptualize and develop tools that would facilitate: (a) planning cost- and performance-efficient allocation of assets and human resources to border control tasks, (b) exploration of how to best combine humans with new technologies (e.g., through simulations, virtual environments), and (c) designing optimal information workflows for particular border control scenarios, i.e., which information to utilize and fuse with other, and which to discard, etc. The underlying data to support the decision making and/or planning in the context of such tool could come from the information gathered over longer period of time from the past.

Expected impact:

All studied scenarios show that in the long term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities will remain a critical capability, given the expected rising cross border flow of people and goods. Border controls thus face increasing demand for efficiency, which implies the need for technical systems that are user friendly and reliable in operational conditions. A general challenge is to make the equipment and procedures appropriate for wide employment. A further general challenge that applies to all scenarios is interoperability (operational as well as technical).

Form of funding:
Coordination and Support Action 100% funding

Supply Chain Security

10. Supply Chain Security topic 1: Development of an enhanced non-intrusive (stand-off) human scanner

Specific challenge:

Smugglers ingest or conceal packages of drugs, using their body to evade controls at the border. Likewise people can easily threat items under clothing, such as explosives, money, narcotics, weapons and ampules containing Chemical and Biological threats, which can remain undetected by conventional technologies. There is a need to develop a body-scan technology able to discern between material identified as risky by customs from benign materials carried in the body and beneath clothing. The device/system should have the capability to automatically identify the chemical composition of packages. A technology which could automatically identify, the main commodities, heroin and cocaine, while hidden or inside the body, would make the inspection of suspected individuals more efficient, while acting as a deterrent to other potential smugglers.

Scope:

To develop a body-scanner capable of specifically identifying and alerting an operator to specific threats such as narcotics, or explosives concealed inside the body, or hidden beneath clothing.

The capability required is to be able to discern those materials from harmless items and alert the operator of this. Important technical challenges are to be faced. A human can conceal up to 5 kilograms of drug on the body, which may be moulded to their shape and/or compensate by them wearing larger clothing. Packages may be compressed powder or even liquid. Drugs are by nature organic, so it is difficult to distinguish them from other organic or food waste in the digestive system of the human body. Organic objects on the body for a significant time can become opaque to the technology if they are close to the body temperature. Low-dose x-ray are useful tools, but these are imaging technologies which require interpretation. There is a potential for error and packages could be missed. Millimetre wave offers some potential for detection, however these are only anomaly detectors and cannot distinguish between threat and benign. Ideally novel solutions should be able to deal with more than one person in their field of view, or at least the other people in the frame should not interfere with the performance on the primary target. Technology is expected to work in real time, not to disrupt passenger flow, or movement of crowd. Performance will have to be validated in a realistic operational scenario.

The technology should pose no health threats to particular groups or with health issues (children, pregnant women, pacemakers). If ionising radiation were to be used, it would have to comply with law and limits of dose. Privacy of individuals should be honoured by not showing body contours.

Expected impact:

The technology to be developed would replace current conventional technology (including existing millimetre wave body-scans without material discrimination) being used by the Customs administrations of some Member States. If the appropriate capability were developed, it is expected to significantly improve security at the border, and would constitute an effective tool in the fight against organized crime.

Form of funding:

Collaborative Project 100% funding (Capability Project)

11. Supply Chain Security topic 2: Technologies for inspections of large volume freight

Specific challenge:

Approximately 70% of all cargo is transported in intermodal shipping containers representing approximately 240 million container moves in any given year. As a major trans-shipment hub, the EU handles around a third of the container moves throughout the world. Container security associated with terrorist threats, illegal immigration, theft and smuggling is therefore an important factor in the overall EU border security.

Customs currently employ a limited amount of technology to assist in working on its largest problem: how to counter hiding/smuggling in large volume freight. Thus far the technology of choice is X-ray interrogation (supported by risk-selection). Ideally, upon effective risk selection, the most effective (array of) technology out of a number of availabilities should be selected to screen the freight. The best results (relative low false-positive, relative low false negative) is expected to be achieved in a situation in which (at least) two independent technologies are employed in conjunction

Scope:

The research should explore options for parallel development of at least two different technologies for container scanning:

1) Atomic property based interrogation (e.g. X-ray, muon, neutron), particularly to detect threat materials shielded in dense cargos, interrogation technology being directed towards the detection of organic products of relevance to Customs;

2) Evaporation based interrogation (e.g. mass spectrometry, biological detection, ion mobility spectrometry), with targeted selectivity at approximately femtogram/ litre level, to be directed towards a wider scope.

These combined approaches should be validated in an operational scenario, to come up with practical, wide scope, detection tool to be used on large volume freight (e.g. containers and large pallets).

Expected impact:

The research is expected to provide a substantial contribution in the prevention of the unlawful transport of dangerous and illicit materials, also protecting critical elements of the supply chain from attacks and disruptions. The greatest volume (and risk) of illegal/illicit/mis-declared goods into the EU, as of interest to Customs, include, but are not limited to: illicit narcotics (heroin, cocaine, etc.) explosives, tobacco products, chemicals. Intelligence together with scanning is useful in narrowing suspicious consignments, but ultimately a physical examination of the load is required. This is resource intensive and adds cost and delay to importers, should the anomaly be found to be benign. A technology which could scan a load with high probability of detection of particular key commodities would increase efficiency and throughput and reduce cost and delays to innocent shippers. Solutions are therefore to be developed to allow for an increased assurance level in particular for dense containerised cargo, avoiding the need to unnecessarily resorting to physical inspection. It is difficult to predict a priori which technology will yield the most practical solution. This will have to be validated in a realistic scenario. As the research should facilitate and expedite the smooth flow of legitimate international trade through improved security controls, it would the work of WCO for high risk cargo.

Form of funding:

Collaborative Project 100% funding (Integrated project)

Ethical Societal Dimension

12. Ethical Societal Dimension topic 1: Human factors in border control

Specific challenge:

Border management relies on a number of presumed abilities in those performing it. These include the ability to:

- stay alert from the beginning of a shift to the end;
- distinguish truth from falsity;
- detect malicious intent;
- detect invalid or falsified documents;
- detect hidden goods or humans in vehicles;
- detect types of persons engaged in, or methods used to undertake, illicit activity.

Recent psychological research has demonstrated conclusively that, inter alia, humans are very bad at assessing veracity of other humans (only slightly better than random), that performance drops off rapidly with length of time spent on a monotonous task, and that risk profiles based on experience may bear little relation to empirical fact. Border guards and customs officials are moreover not tested at recruitment nor throughout their career to determine whether they effectively possess one or more of these abilities or not.

Scope: The project should list and carefully analyze the psychological factors which may affect the performance of key border guard tasks and also include a review of the psychological literature relevant to such task. It should suggest remedies and a strategy for improving performance at them (whether improving human performance of substituting it via machine) , in this way making a major contribution to the effectiveness of EU border control.

Expected impact:

All studied scenarios show that in the long term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities will remain a critical capability, given the expected rising cross-border flows. Border control is likely to face increasing demands for efficiency, which implies a need for technical systems that are user friendly and reliable in operational conditions. This research would contribute to the implementation of the Smart borders initiative (and future regulation) , reinforcing checks while speeding up border crossing for regular travellers, optimizing procedures and enhancing the security at the moment of the crossing of the EU external borders.

Form of funding: Collaborative Project (100%) – Single stage (to be implemented in 2015)

13. Ethical Societal Dimension topic 2: Study on Public Private Partnership and Privatization opportunities in Integrated Border Management

Specific Challenge:

Every year more than 700 million EU citizens and non-EU nationals are crossing the EU's external borders. Enabling smooth and fast border crossing for travellers, while ensuring an adequate level of security, is a challenge for many Member States.

In many countries the border crossing experience remains largely the same as it has been for decades despite the advent of new technological solutions - such as X-ray equipment, cargo tracking systems, information technology could ease trade while boosting regulatory compliance. While at border crossing points a steady increase in the flow of passengers and goods is expected, the number of border guards is not likely to increase, particularly in a scenario of scarce public budgets. Well-designed border posts, related infrastructure, and effective operating modalities can support reform across various border crossing points and, at the same time, promote facilitation and security objectives. Novel modi operandi will have to be identified to match this scarcity of human resources.

Scope:

Good practice models could guide a meaningful reform of border management. One such model could imply more shifting of responsibilities for migration control (and implementation of procedures) to private companies as well as could pave the way towards improved management of risk. This is already the case in the airport borders, where private sector companies such as airlines are becoming more involved in surveillance and migration control functions and thereby in security governance.

Inevitably as more border control work is being contracted out to private companies, the line between state and social control would be blurred complicating questions of oversight and accountability.

The action should analyse what private sector services can be contracted to underpin the government’s activities, augmenting its resources and capabilities. Areas addressed could include suggestions for developing a new legislation, modalities and areas for outsourcing.

Furthermore, it should be examined how private companies and organisations could be co-opted into the control of the movements of people. Legal and ethical issues should be carefully analysed.

Expected impact:

It should explore advantages and disadvantages, identifying key issues for reformers, delivering a cost-benefit analysis demonstrating that border management reform would represent a sound business investment and not merely a cost, and suggesting a strategy to cope with the challenges of the future, highlighting the specificities of specific issues in controls at the border.

Form of funding:
Coordination and Support Action 100%funding

Other actions

Contents

Activity 1 – Galileo Public Regulated Services (PRS)

Financing the development of the security module for the **Galileo Public Regulated Service (PRS) will be addressed.** It should be noted that this development is about cryptology, secured design, etc. and is related to dual-use technology development; hence this corresponds largely to classified development. The proposed activities to be funded from the Horizon 2020 Security theme are only a part of the overall development, and that complementary tasks are expected to be carried out in the Space theme of Horizon 2020, as well as by some Member States.

Two specific public procurement actions are to be funded from the Security budget with 15 million for the first action and 5 for the second action. The procurement will be opened early in 2014, and the contracts are expected to be awarded by mid-2014, and will run for 30 months.

PRS topic 1: Use of Galileo PRS in Professional Mobile Networks receiver, provision of an Early Service

The aim of the Galileo programme is to establish the first global satellite navigation and positioning infrastructure specifically designed for civilian purposes. The system established under the Galileo programme is completely independent of other existing or potential systems. The services offered through Galileo contribute, in particular, to the development of trans-European networks in the areas of critical infrastructure such as transport, telecommunications and energy infrastructures. The Public Regulated Service (PRS) is one specific objectives of the Galileo programme. This European GNSS service is restricted to government-authorised users, for sensitive applications which require a high level of service continuity.

From 2014 onwards, the exploitation phase of Galileo is set to begin with the deployment of Early Services. One of the biggest potential user communities for secure positioning, navigation and tracking is the one using Professional Mobile Radio (PMR) for Public Safety and Security (PSS). Indeed, missions of PSS are increasingly dependent on GNSS. At the same time, threats loom over GNSS and the critical applications using it.

The Public Regulated Service uses strong encrypted signals. However, the benefit of additional security comes with additional security constraints that may hamper critical applications from using the PRS. Previous studies have shown that those constraints can be made transparent to users by providing appropriate access control service based on use of an access control server and interconnectivity between the server and the terminals.

Further to those studies and demonstration activities, a full scale service shall be developed, deployed, accredited, and made available to Early Service demonstrations. A prototype of a receiver shall be developed. The objective is to use the all demonstrator it in 2016.

The research shall focus on the following points:

- Critical review of previous studies and demonstrations done by the Commission and the European GNSS Agency (GSA);

- Develop and deploy a demonstrator at full scale server;
- Develop a PMR receiver combined with PRS (following PRS4PMR demonstrator);
- Security certification and accreditation; and
- Provide logistic support to the operation of the service and its use for early services.

Expected impact:

Action under this topic shall provide significant improvement in the use of the Galileo PRS service by public safety and security user communities., in particular in critical infrastructure. The respect of the high level of security of PRS has to be demonstrated. By making this service available via networks, the cost to integrate PRS in PMR terminals will be minimized. This assumption has to be validated and demonstrated.

PRS Topic 2: Remote PRS processing server.

This task is devoted to the setup of a server able to process PRS samples and to provide position velocity and time (PVT) as an output to the users. The idea behind this project is the concept of a "PRS Access Server": a service provision based on a client-server architecture in which the client takes a snapshot of the Signal in Space (SIS) and provides it to the server that computes the PVT solution before sending it back to the client.

Given the challenges associated with development of fully-fledged security modules, the PRS Access Server may be the easiest way to deploy an early PRS service for some civilian users.

Starting from the activities already carried out by the GSA in this domain, this project should focus on:

- Consolidation of technical specifications;
- Definition of the system functional and physical architecture;
- Detailed design of the system;
- Detailed definition of internal and external interfaces;
- Development, assembly and integration of the different elements;
- Qualification testing and associated verification activities; and
- Acceptance testing.

Expected impact:

Action under this topic shall provide significant improvement in the use of the Galileo PRS service by public safety and security user communities.

Activity 2 – Supporting the implementation of the Security Industrial Policy and Action Plan through the European Reference Network for Critical Infrastructure Protection (ERNCIP)

With the publication of the Security Industrial Policy and Action Plan - COM(2012) 417 -, the European Commission has underlined the need and its ambition to foster the global competitiveness of the EU security industry, e.g. by promoting EU-wide standards of security technologies, tests and evaluations of security equipment, and respective certifications. ERNCIP, set up in the context of the European Programme for Critical Infrastructure Protection (EPCIP), is a direct response to the lack of harmonised EU-wide testing or certification for products and services (in the area of critical infrastructure protection), which is a barrier to future development and market acceptance of security solutions. This action should focus on linking the relevant work of ERNCIP with the implementation of the Security Industrial Policy and Action Plan, by supporting the uptake and promotion of identified activities. Relevant legislation on European and Member State level need to be taken into account appropriately, including potential ethical, societal and privacy issues of the proposed activities.

Expected impact:

Accelerated implementation of the Security Industrial Policy and Action Plan, leading to improved efficiency of security technologies, improved interoperability of stakeholders, including cross-border cooperation, reduced fragmentation of the EU market in this sector.

Form of funding:
Predefined beneficiary: Joint Research Centre

Activity 3: Support to workshops, conferences, expert groups, communications activities or studies

a) Organisation of an annual Security Research event.

Indicative Budget: up to EUR 1 000 000.

Funding scheme: Support Action – framework contract

b) Support to workshops, expert groups, communications activities or studies

Workshops are planned to be organised on various topics to involve end-users, to support an expert group on societal issues, to prepare information and communication material etc.

Indicative Budget: up to EUR 900 000.

Form of Funding:

Coordination and Support Action

Activity 4: Ex post evaluation of the FP7 Security Theme

The FP7 legal basis foresees the execution of an ex post evaluation: DECISION No 1982/2006/EC Article *"7 3. Monitoring, evaluation and review* - *Two years following the completion of this Framework Programme, the Commission shall carry out an external evaluation by independent experts of its rationale, implementation and achievements."*

On this basis, the evaluation should address notably the following questions:

How far has FP7 achieved its general objectives, including those of the specific programmes?

Does FP7 play an adequate role in positioning Europe on the global map of science and technology?

How can the impact and added value of collaborative research that cuts across scientific disciplines, industrial sectors and policy fields be further enhanced with a view to better address large societal challenges?

To what extent have simplification measures been effective?

What progress has been made under FP7 concerning the major issues which were highlighted in the FP6 evaluation report as needing further analysis, notably the participation, role and achievements of industry (including SMEs) in the Framework Programme?

Indicative Budget: 500.000