WORK PROGRAMME 2011

COOPERATION

THEME 10

SECURITY

(European Commission C(2010)4900 of 19 July 2010)

Table of content

Objective:

The objective of the Security theme is to develop the technologies and knowledge for building capabilities needed to:

- ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental rights including the protection of personal data
- ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security,
- stimulate the cooperation of providers and users for civil security solutions,
- improve the competitiveness of the European security industry
- and deliver mission-oriented research results to reduce security gaps.

I CONTEXT

A secure Europe is the basis for planning our lives, for economic investments, for prosperity and freedom. The Security theme contributes to the implementation of EU external policies[1], to the creation of an EU-wide area of freedom, justice and security[2], in the context of the "Stockholm Programme", and to policy areas such as transport[3], health[4], civil protection[5], energy[6] development[7] and environment[8].

Through this, the Security theme also contributes to the Europe 2020 strategy[9] and its Innovation Union flagship initiative, by promoting growth and employment in general, stimulating innovation (including in SMEs) and enhancing the competitiveness of European industry.

The respect of privacy and civil liberties is a guiding principle throughout the theme. All individual projects must meet the requirements of fundamental rights, including the protection of personal data, and comply with EU law in that regard.

The Security theme has an exclusively civil application focus.

The Security theme facilitates the various national and international actors to co-operate and coordinate in order to avoid unnecessary duplication and to explore synergies wherever possible. Furthermore, the Commission will ensure full complementarity with other EU initiatives and avoid duplication, e.g. with the 'Framework Programme on Security and Safeguarding Liberties' (SSL), which focuses on actions related to policy and operational work in the area of law enforcement and combating and preventing crime/terrorism, while the Security theme supports R&D actions oriented towards new methodologies and technologies.

[1] http://ec.europa.eu/external_relations/cfsp/ ;
[2] http://ec.europa.eu/justice_home/fsj/ ;
[3] http://ec.europa.eu/dgs/energy_transport/security/index_en.htm;
[4] http://ec.europa.eu/health/ph_threats/com/preparedness/preparedness_en.htm;
[5] http://ec.europa.eu/environment/civil/index.htm;
[6] http://ec.europa.eu/dgs/energy_transport/security/index_en.htm;
[7] http://europa.eu/pol/dev/
[8] http://ec.europa.eu/dgs/environment/index_en.htm;
[9] COM(2010) 2020

On 11 September 2007, the European Security Research and Innovation Forum (**ESRIF**) was established with 64 high level members, including two representatives of the European Commission, and over 600 experts. The objective of ESRIF was the development of a mid and long term Joint Security Research Agenda that will link security research with security policy making and its implementation. The ESRIF Final Report[10] was published on 1 December 2009. In its communication[11] COM(2009)691, the Commission welcomed it and acknowledged its importance in the context of the FP7 Security theme.

Following the recommendations of the Commission's *European Security Research Advisory Board (**ESRAB**)*[12] in September 2006, the Security theme addresses four security **missions** of high political relevance which relate to specific security **threats**. It contributes to building up the necessary **capabilities** for safeguarding security in these mission areas by funding the research that will deliver the required **technologies and knowledge** to build up these capabilities.

It is clear however, that the use of security related technologies must always be embedded in political action. To support this and also to improve the effectiveness and efficiency of the technology related research, three domains of **cross-cutting** interest are selected as well.

The overall structure of the Security theme, including the seven main mission areas, is summarised in the following table:

Security missions:

1. Security of citizens
2. Security of infrastructures and utilities
3. Intelligent surveillance and border security
4. Restoring security and safety in case of crisis

Cross-cutting missions:

5. Security systems integration, interconnectivity and interoperability
6. Security and society
7. Security Research coordination and structuring

The Security theme aims at **meeting its main objectives – improved security for the citizens,** and **enhanced competitiveness for industry.** Successful demonstration of the appropriateness and performance of novel solutions is a key factor for the take-up of the output of the research work and its implementation by security policies and measures. The Security theme should also support the (re)structuring of the European security sector.

Research in the Security theme consists of several building blocks, representing three – in some cases parallel, in others subsequent - routes that contribute to the overall objectives (see figure 1):

[10] See www.esrif.eu
[11] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0691:FIN:EN:PDF
[12] *ESRAB Report: Meeting the Challenge: the European Security Research Agenda - A report from the European Security Research Advisory Board, September 2006. ISBN 92-79-01709-8.*

- On the lowest level of the building block structure, '**capability projects'** aim at building up and/or strengthening security capabilities required in the four security missions. This will be done through *adaptation of available technology* as well as the development of *security specific technology and knowledge aiming at tangible results*. In many cases these will also have cross-mission relevance.
  Typical duration: 2-4 years
  Funding scheme: Collaborative Projects

- On the medium level of the building block structure, '**integration projects'** aim at mission specific combination of individual capabilities providing a security *system* and demonstrating its performance.
  Typical duration: 3-4 years
  Funding scheme: Collaborative Projects

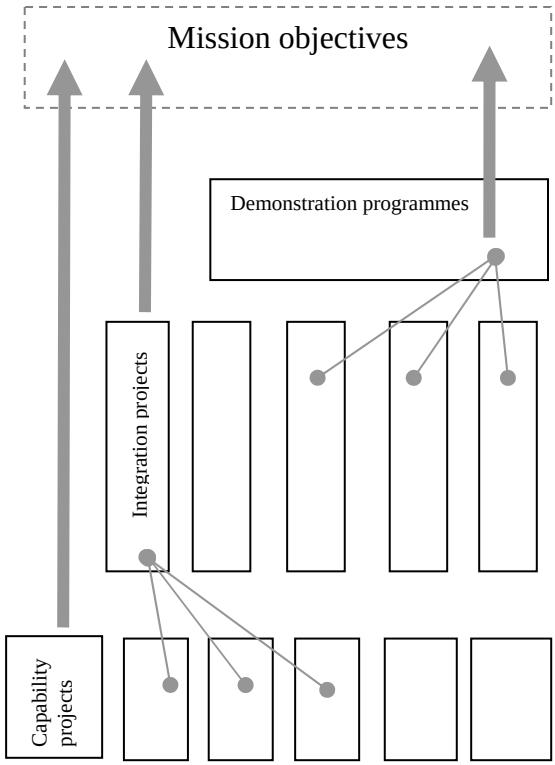


Figure 1: Research routes to meet the Security theme objectives

- On the top level of the building block structure, '**demonstration programmes'** will carry out research aiming at large scale integration, validation and demonstration of new security systems of systems going significantly beyond the state of art. They depend upon the compatible, complementary and interoperable development of requisite system and technology building blocks of the integration projects and capability projects. They intend to promote the application of an innovative security solution, which implies a strong involvement of end users, taking into account the relevant legal and society related issues, and strong links to new standardisation. Demonstration programmes will be implemented in two phases:

  Phase I projects (either one or several projects in each of the demonstration programmes) will define the strategic roadmaps and trigger Europe wide awareness, both elements involving strategic public and private end users as well as industry and research. The strategic roadmaps will take into account relevant completed, ongoing and planned work and indicate further research needs for Security theme integration projects and capability projects, but also for other themes of the Seventh Framework Programme or for the national level.
  Typical duration: 1 year
  Funding scheme: Coordination and Support Actions

  Phase II projects (either one or several projects in each of the demonstration programmes) will then technically implement the system of systems demonstration, taking already into account steps which have to follow the research, like certification and/or standardisation (if and as appropriate), development of marketable products and pre-procurement. This will mobilise a significant volume of resources.

Typical duration: 3- 4 years
Funding scheme: Collaborative Projects

ESRAB identified 5 topics for Demonstration programmes: Aftermath crisis management, Border control, Logistic and supply chain security, Security of mass transportation and CBRNE. Phase 1 projects for Border and Transport were selected after the 1st call (FP7-SEC-2007-1). Topics for the two corresponding phase II were open in the call 3[13] (FP7-SEC-2010-1). Phase 1 demo for CBRNE, Supply chain logistics and Crisis management were open in the call 3. Proposals for CBRNE and Supply chain were selected and should start early 2010. It is expected that they will be completed in time for opening topics for these two phase II in the call 5 (FP7-SEC-2012-1). No proposal was selected for the demo I Crisis Management. This topic was re-introduced in the call 3. It is expected that the phase II could be open in the call 6 (FP7-SEC-2013-1).

For the **cross-cutting domains** of the Security theme, actions can be both self standing or linked to the missions in activities 1 to 4. Society relevant research issues will also be, as far as possible, integrated in technology projects.

The following funding schemes are envisaged:

- **Collaborative Projects** in this work programme are divided into a) small or medium-scale focused research project (CP-FP), and b) large scale integrating project (CP-IP).
Integration projects described above will be implemented using the funding scheme Collaborative Project (large scale integrating project) with EU requested funding of over EUR 3 500 000.
Capability project will be implemented using the funding scheme Collaborative Project (small or medium-scale focused research project) with requested funding of EUR 3 500 000 and below.
It is important to note that the above mentioned funding thresholds will be applied as eligibility criteria and that the proposals not fulfilling these thresholds are considered as ineligible.

- The **Networks of Excellence** scheme aims at research organisations, end users and other stakeholders that wish to combine and integrate in a durable way a large part of their activities and capacities in a given field, in a 'Joint Programme of Activities', possibly with a view of creating in this field a European 'virtual centre of research'.

For activity 5 and 6, collaborative projects and coordination and support actions are possible as funding schemes (as appropriate). For activity 7, *Security Research coordination and structuring*, the funding schemes will be collaborative projects, networks of excellence and coordination and support actions (as appropriate). For the latter, core activities will be studies, networking, exchanges of personnel, exchange and dissemination of good practices, the definition and organisation of joint or common initiatives, meetings, conferences and events etc. and the management of the action.

In the Security theme, the EU funding for research activities may reach a **maximum of 75%** in cases with very **limited market size** and **a risk of 'market failure'**, and for **accelerated**

[13] Evaluation of proposals submitted under call 4 is planned on the first half of 2011.

equipment development in response to new threats.[14] To claim this higher funding level, proposers need to demonstrate in their proposal that the required conditions apply. Please note that demonstration activities are excluded from these provisions.

The forms of the grant to be used for the funding schemes for the Security theme are given in Annex 3.

- **SME relevant research**

All actions are open to the participation of all security stakeholders: industry including SMEs (small and medium enterprises), research organisations, universities, as well as public authorities, non-governmental organisations and public and private organisations in the security domain. Considering the Security theme's objective of increasing the competitiveness of industry, the broad **involvement of SMEs** in consortia is highly encouraged.

- **International Cooperation**

All actions of the Security theme are open to **international co-operation** to industrialised countries as well as to ICPC[15] countries. At this stage, it is not foreseen to have any 'specific international co-operation actions' in the Security theme. These might be implemented at a later stage, in case participation of international partners through normal actions were deemed insufficient.

- **Dissemination actions**

In general, particular networks of security research stakeholders (including both the supply and the demand side) are seen as instrumental in promoting the **dissemination** of security research to its end users, national public authorities and citizens alike. Attention is drawn to the exploitation strategy requirements which is part of the evaluation criteria 3, Impact. Suitable and dedicated coordination and support actions to achieve this could also receive funding. It is important to strengthen these activities in all projects.

- **Theme specific information**

In order to ensure that the outcome of the research carried out under the Security theme does in particular contribute to meeting the theme's main objective - the improvement of the security of the citizens - co-operation between the user side (authorities and organisations responsible for the security of the citizens) and the supply side of security technologies and solutions must be promoted. Thus the active **involvement of end users** in the projects is considered of utmost importance. Whenever possible, this should translate into a direct participation of user organisations to the consortia implementing research actions (though other forms of indirect participation might also be followed, as appropriate).

Security theme actions should generally be **multidisciplinary** and **mission-oriented**. A multi-purpose nature of technologies is encouraged to maximise the scope for their application, and

[14] *Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013) Art 33.1*

[15] *ICPC: International Co-operation Partner Countries - see Annex 1.*

to foster cross-fertilisation and the actual take-up of **critical technologies** for the civil security sector.

The **testing**, **validation** and **demonstration** of the security solutions developed in the projects, involving as much as possible the end users, is considered at the core of the Security theme. These activities should be present in every type of project (as appropriate): *demonstration programmes* but as well *integration projects* or *capability projects*. **Concrete achievements** and milestones are strongly encouraged.

Standards are considered crucial for interoperability and take up of research results. Preparation and promotion of standards within the projects is encouraged. Self-standing actions related to **interoperability, standardisation** or **pre-normative research** are open in the Security call 4.

Security research can also cover areas of **dual use** technology relevant to both civilian and defence applications. Appropriate coordination mechanisms are in place with the *European Defence Agency* (EDA), who will consult its Member States about national programmes, thus ensuring complementarity.

Actions within the Security theme build not only on technology gain from the capability projects, but also on research outcomes of other origins. Issues of **European added value** and large scale integration are covered in the theme, and complementarity is ensured with all other EU actions. Complementarity with research carried out in FP7 Associated Countries will be ensured via the members of the Security Programme Committee configuration.

Due to the sensitivity of the Security theme, the *Rules for participation*[16] foresee the possibility of restrictions to the dissemination of the outcome of the actions on a case by case basis. In particular, special provisions for *classified information* will be taken in the grant agreement, as necessary and appropriate.

For the Security Research Call 4, **proposals must not contain any classified information**. This would lead to declaring them ineligible immediately. However, it is possible that the output of an action ('Foreground') needs to be classified, or that classified inputs ('Background') are required. In such cases proposers have to ensure and provide evidence of the adequate clearance of all relevant facilities. Consortia have to clarify issues such as e.g. access to classified information or export or transfer control with the national authorities of their Member States / Associated Countries prior to submitting the proposal. Proposals need to provide a draft *security classification guide*[17], indicating the expected levels of classification. Appropriate arrangements will have to be included in the consortium agreement.

---

[16] *Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013) Article 22*

[17] 'Security Aspects Letter (SAL)': a set of special contractual conditions, issued by the contracting authority, which forms an integral part of a classified contract involving access to or generation of EU classified information, and that identifies the security requirements or those elements of the classified contract requiring security protection.

'Security Classification Guide (SCG)': a document which describes the elements of a programme, contract or grant agreement which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme, contract or grant agreement, and the elements of information may be re-classified or downgraded. The SCG must be part of the SAL.

See Commission Decision 2001/844/EC, ECSC, Euratom on security, amended by Decisions 2006/548/EC, Euratom and 2005/94/CE, Euratom.

Positively evaluated proposals involving sensitive or classified information, those involving international co-operation as well as those collaborative projects where 75% funding for all participants is foreseen, will be flagged to the members of the Security **Programme Committee** configuration and dealt with according to its Rules for Procedure.

Gender aspects in planning, decisions, and funding must always be taken into account, both as integrated research activities and as diversity in workforce. The pursuit of scientific knowledge and its technical application towards society requires the talent, perspectives and insight that can only be assured by increasing diversity in the research workforce. Furthermore sometimes security needs to be balanced against the accessibility needs of persons with disabilities. Therefore, a balanced representation of diverse branches of knowledge and of women and men as well as person with disabilities where relevant at all levels in research projects is encouraged, including in evaluation groups etc.

The integration in projects of the notion of ***privacy by design*** is strongly encouraged. Attention should also be given to the impact of the proposed technologies on the society, the organisational processes and the respect of legal requirements, such as respect for fundamental rights which must be embedded in each proposal and foreseen in the proposals' work plans.

Security issues could also be regarded as intrinsic elements of other themes in the Co-operation programme. The scope of the calls has been carefully defined throughout the themes, in order to avoid gaps or duplication during the entire Seventh Framework Programme. Thus in case of doubt, whether a proposal is fully in scope with the topics presented under this theme, it is recommended to consult as well the Work Programmes of the other Co-operation themes.

The theme will also support **ERA-NET** activities (see more information in Annex 4), which are meant to develop the cooperation and coordination of research programmes carried out at national or regional level in the Member or Associated States through the networking of research programmes, towards their mutual opening and the development and implementation of joint activities. See topic SEC-2011.7.1-1 page 46 and specific eligibility criteria page 57.

Research Executive Agency

Call for proposals under this work programme part (Security) will be implemented by the Research Executive Agency[18] (REA). The management of all projects to be funded as a result of this call for proposals will be implemented by REA, with the exception of:

- Classified grant agreements and contracts and
- Policy related actions (indicated in section II of this work programme).

[18] See Commission decision C/2008/3980 of 31 July 2008 "delegating powers to the Research Executive Agency with a view to performance of tasks linked to implementation of specific EU programmes People, Capacities and Cooperation in the field of research comprising, in particular, implementation appropriations entered in the EU budget"

II SECURITY RESEARCH CALL 4 (FP7-SEC-2011-1)

The primary ambition of the Security theme is to develop innovative security solutions and to facilitate their rapid take-up for the implementation of security policies and programmes.

All seven activities, the four mission-oriented and the three cross-cutting areas have topics in the Security call 4. Topics address one (or more) of the following four **ambitions**:

- important **capability gaps** (urgent needs that can easily be fulfilled with new solutions based on innovative technologies),
- **validation** of solutions resulting from research and development (experimentation involving their appropriation by the end-users),
- core **critical capabilities** needed by Europe (where technologies are not yet mature),
- **high risk / high pay-off** projects (with a view at long-term development of groundbreaking new technologies).

The topics that are open to the submission of proposals under the Security Research Call 4 are described in the following seven sections corresponding to the seven activities. For each activity, the description is taken from the FP7 Cooperation Specific Programme. Then, topics are presented within areas[19].

Activity: 10.1 Increasing the Security of the Citizens

Actions in this activity will concentrate on threat aspects of potential incidents of a trans-national importance, such as offenders, equipment and resources used by them or as mechanisms of attack. A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases 'identify', 'prevent' and 'prepare' and 'respond'. The ambition is both to avoid an incident and to mitigate its potential consequences. To build up the required capabilities with the aim of providing civil protection, including bio-security and protection against risks arising from crime and terrorist attacks, emphasis will be on issues such as: threat (e.g. Chemical, Biological, Radiological and Nuclear, CBRN) awareness (e.g. intelligence gathering, collection, exploitation, sharing; alerting), detection (e.g. hazardous substances, explosives, agents B or C, individuals or groups, suspect behaviour), identification and authentification (e.g. of persons, type and amount of substances), prevention (e.g. control of access and movements, with respect to financial resources, control of financial structures), preparedness (e.g. risk assessment; CBRN protection, control of intentionally released biological and chemical agents; assessment of levels for strategic reserves such as manpower, skills, equipment, consumables; with respect to large scale events, etc.), neutralisation (e.g. missiles, communications, vehicles, non-destructive systems) and containment of effects of terrorist attacks and crime, law enforcement data processing.[20]

Regarding the "Respond" phase, an important aspect is to give enough legally ascertained information to allow prosecution of alleged offenders in an EU (even international) context.

[19] See the conclusions of the 8th meeting of the FP7 Security Advisory Group http://ec.europa.eu/research/fp7/index_en.cfm?pg=eag

[20] The definitions of the Activities presented in the "boxes" are directly referring to the Specific Programme for the FP7 security Theme, see page 135: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:400:0086:0242:EN:PDF

Part of the topics presented here deal with "forensic activities" in various technological areas. These topics must be dealt with in liaison with the "forensics" topics from the previous Work Programme.

This activity is divided among five areas: **Organised crime; Intelligence against terrorism; Explosives; Ordinary crime and Forensic; and CBRN Protection**. It should be noted that the intelligence against terrorist activities is mainstreamed across many other areas.

Area: 10.1.1 Organised crime

Topic SEC-2011.1.1-1 Digital forensic - Capability Project

Description of the topic:
Most of the large scale incidents perpetrated using computers and telecommunication networks have shown the difficulties to gather sufficient information and in such a way that may lead to the prosecution of the alleged offenders. In this particular context, the main objective is to define the best practices which should be used within the appropriate legal context in order to help to solve this type of cases, not only taking into account their international dimension but also solving the technical difficulties coming from the very nature of cyberspace, including the growing use of cloud computing, that makes more difficult the identification of the location of relevant information for forensic analysis. The early involvement of industry/providers, investigation police forces, prosecutors, judges and legal experts is a necessary condition for the success of this action. Necessary tools to support the defined best practices and testing methods for their evaluation should be developed taking into account other EU research in this area, with the aim to preserve under all circumstances the chain of custody of evidence to the final trial.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: to raise the awareness of policy- makers and help developing the proper legal framework (if needed) while fully respecting the legal requirements as to the admissibility of criminal evidence as well as fundamental rights, such as the rights to fair trial and the protection of personal data; to demonstrate to the law enforcement agencies the added value of cooperation supported by common tools in the EU (international) operation; to demonstrate to the citizens that action/progress in this area is possible without building an "a priori endangering privacy" set of laws.

Area: 10.1.2 Intelligence against terrorism

Topic SEC-2011.1.2-1 Strategies for countering a terrorist attack in an urban environment – Capability Project

Description of the topic:
Terrorist attacks take extremely varying forms (e.g. "9/11", Madrid bombings in 2004 or Mumbai attacks in November 2008). Terrorists have often demonstrated their aptitude for creativity, innovation or adaptability. Security forces and counter-terrorism units need to continuously anticipate and adapt their ways of working. The objective of the project is to improve the effectiveness of security forces in preventing and dealing with an urban attack,

while taking fully into account legal requirements and democratic and ethical principles. The scenario addressed by the project is the situation where there is a known specific threat, or an actual terrorist attack, in an urban environment. Given that scenario, the project should identify, research and develop tools, technologies and methods that would best facilitate all or some of the following aspects:

- the short-term anticipation of a concrete attack, based on behaviour analysis of possible terrorist groups (e.g.: their patterns of movement, financing or communications), and characteristics of the possible urban-based targets;
- the response to such attacks, including scenario awareness and rapid alerting of relevant authorities and responders.

The project will include the identification of new technologies, methods, and capabilities supporting the above objectives. A strong participation of the end users community, i.e. security authorities, is essential. Due to the potentially high sensitivity of the information exchanged or produced, a suitable framework has to be proposed including the ability of partners to deal with classified information if relevant.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact: Prevent terrorist threats identified through intelligence sources, or limit to the minimum the consequences of a terrorist attack in an urban environment, by improving the preparedness of security forces, the capabilities at their disposal, and facilitating the emergence of a cross-European common approach.

Area: 10.1.3 Explosives

Topic SEC-2011.1.3-1 Improvised Explosive Device (IED) neutralisation in urban / civil environment - Capability Project

Description of the topic:
The main objective is to re-visit the actual practices of forces dealing both with human borne and static explosive devices just discovered and to propose new and innovative methods in order to improve the actual practices for their neutralisation before being triggered, or to drastically limit the consequences of their explosion. Scenarios of the last years terrorist attacks in EU that involved explosives should be taken into account.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: To help police forces agencies to react more efficiently to explosive devices, to facilitate the emergence of a common European approach.

Topic SEC-2011.1.3-2 Forensic analysis of an explosion or an unexploded IED- Capability Project

Description of the topic:
The main objective is to complement other EU research activities in the forensic area with highly specialised tools and best practices. This action should address the development of forensic capabilities for detection, selection (screening), analysis and evaluation of evidence

at a post-blast crime scene following an explosion or the analysis of a non-exploded Improvised Explosive Device (IED). Aiming at on-site technology with quick results, to be supported by tools for information management and 3D crime scene registration to be developed as plug-in to be inserted in a global EU forensic open framework (this last item should not be developed in the proposal). All these tools should preserve the chain of custody/evidence from the filed to the trial. The developed forensic capabilities should be compatible with first responder procedures and protocols.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: To help law enforcement agencies in their analysis and to deal with explosive events in a common European approach.

Topic SEC-2011.1.3-3 Comprehensive toolbox for humanitarian clearing of large civil areas from anti-personal landmines and cluster munitions - Integration Project

Description of the topic:
The European Commission and the EU member states together represented in 2008 the biggest donor in humanitarian demining efforts. Anti-personnel landmines and cluster munitions remaining from armed conflicts represent an obstacle to the livelihood of populations, transition of states from crises towards post-conflict survival as well as towards sustainable development and sustained stability. They perpetuate humanitarian crises, threaten peace processes, fuel crime and terrorism, put national and regional security at risk, undermine conflict prevention programmes, and adversely affect social and economic rehabilitation, post-conflict reconstruction and sustainable development for many societies worldwide.
The action aims at developing and integrating innovative solutions, i.e. technologies and methods, for the – mapping, localisation (long distance) – detection (short distance) - neutralisation of landmines and/or cluster munitions in a civil environment, by non-military organisations. This toolbox should include protective equipment for personnel and training solutions. It should foresee an initial assessment on state of the art and related on going actions.
In order to assure coherence and to avoid unnecessary duplications of measures and initiatives, an active involvement of relevant stakeholders, e.g. NGOs, local public authorities, other organisations involved in the humanitarian demining, the United Nations Mine Action Services (UNMAS), is essential. Existing promising technologies, e.g. used by military demining teams, should be taken into account while keeping in mind the constraints of civilian use (e.g. costs, presence of population, local cultures...). Cost effectiveness, deployability, maintenance constraints, ability to be used by normal civil operators, contention of potential damages to properties are key elements to take into account to guarantee the effectiveness of the solution to be developed.
The action should include a demonstration / table-top exercise, mine risk education and dissemination activities.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact: To reduce the lingering threat of landmines and cluster munitions for the population and to increase humanitarian security, while, at the same time, recreating an environment in which people can live safely, ensuring peace and stability, promoting a

sustainable social and economic development and alleviating human suffering of affected victims and communities.

Area: 10.1.4 Ordinary Crime and Forensic

Topic SEC-2011.1.4-1 Understanding of unintended consequences of global illicit-drug control measures – Capability Project

Description of the topic:

Major policy initiatives in the past decades have attempted to curb the global illicit drugs market. However, the potential unintended consequences of drug control efforts undermine a global coordinated response in tackling the illicit drug phenomenon. Sometimes different policy measures unintendedly may even result in an array of social, health and security risks for the production and transit countries and regions concerned, and also for the EU as major destination market of the drug trade. For example, analysis suggests that law enforcement interdictions may affect drug production or trafficking networks, but often also result in geographical displacement of production and routes. At the same time, evidence suggests that these networks are not necessarily dismantled but that they adapt to the new market situation (and risk of interdiction) by extending their drugs trade to production and 'trafficking' hubs around the globe.

This research project has the task to further analyse the relation between EU/global drug control policies and their interaction with and impact on the production, trade and trafficking of illicit drugs, with a particular emphasis on unintended consequences of these policies and practices.

The research needs to take into account – inter alia – the following issues:

a) to assess (1) whether unintended consequences may be the result of the drug control policies implemented by EU Member States and/ or the international community, (2) whether these unintended consequences were the result of trends and developments that caused important changes in the global illicit drugs market (e.g. global political, economic or security changes, etc);

b) to analyse the impact of these unintended consequences on achieving the objectives of drug control on the one hand, as well as the impact on the social, economic, health and security situation in the affected production and transition countries.

c) to provide recommendations and methodologies with which potential unintended consequences of drug control policies can be better predicted and assessed prior to their implementation.

The research activities should include qualitative and quantitative analysis of unintended consequences. Efforts should utilise existing research as well as generate new data and methodologies for thinking about the consequences of drug control (both intended and unintended). These efforts may include fieldwork in production and trafficking countries and should cover a wide range of stakeholders and affected populations.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: This action will contribute to the development of an effective and efficient EU response to the global drugs phenomenon, in particular to an ex-ante analysis of policy efforts targeting drug production and trafficking in third countries which are undertaken on the basis of the EU Drugs Strategy and EU Drugs Action Plans.

Topic SEC-2011.1.4-2 Innovative techniques for safe external control of non cooperative vehicles – Capability Project

Description of the topic:
Organised crime is always using new means to perpetrate its unlawful activities. One example is the use of high speed car to smuggle unlawful merchandise from one country to another.
The action should investigate innovative means for the police/security/border guard forces to control, slow and stop, non-cooperative vehicles (e.g. motorcycles, cars, trucks, boats) at distance. Safety and security of people, other vehicles and environment in nearby public or private areas should be taken into account as well as of the people inside the vehicle to be controlled. Secured and controlled usage of this new means should be included by design. Legal implication of the use of such new means should be studied. Support and collaboration of vehicle manufacturers could be sought.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: to raise the awareness of policy- makers and help developing the proper legal framework (if needed); to demonstrate to the law enforcement agencies the added value of new technologies in specific areas in relation with their daily operations; and to demonstrate to the citizens that the use of new technologies by security forces in their daily mission could increase their security without endangering their safety.

Topic SEC-2011.1.4-3 Advanced forensic framework - Coordination and Support Action

Description of topic:
The task is to further develop a EU framework and methodology for forensic science with the aim to include past and new technological developments in this field, in order to make measurements and their comparison more objective, automated, and robust to forensic conditions. The forensic methodology needs in fact needs to be strengthened to increase the objectivity of evidence evaluation, and allow for consolidating and combining evidence from multiple sources. These important aspects form the common core of the very diverse forensic disciplines: an approach that is balanced, logical, transparent, and robust. This action should lead to a better understanding of the evidential value of forensic analysis and make it more objective by removing potential biases. It should also liaise with all other projects awarded in the context of the FP7 Security theme in the forensic area, with the aim of steering their activities in the direction aimed to by this action, and of proposing to evaluate their results against the framework being developed ensuring a cross-validation of the respective products.

Funding schemes: Coordination and Support Action

Expected impact: To increase the quality and robustness of decisions based upon forensic analysis conducted in accordance to common practises and methodologies, and therefore increase public confidence in the judicial system.
To offer a solid basis to be developed in new academic curricula and forensic protocols and to be fed in standardization activities.

Area: 10.1.5 CBRN Protection

Topic SEC-2011.1.5-1 Development of detection capabilities of difficult to detect radioactive sources and nuclear materials - Capability Project

Description of the topic:
As underlined in the EU CBRN action plan, efficient and reliable (i.e. with low innocent and false alarm rate) detection of difficult-to-detect radioactive sources and nuclear materials, incl. masked and shielded sources, is still a challenge. The research project should look specially into solutions for the improvement of detection and enhancing the portability and mobility of detection solutions, which could among other be used also by emergency responders in the field (incl. neutralisation and detection equipment for bomb squads) or for the detection and location of a radiation source in large crowds. The solutions proposed should facilitate reliable and correct assessment of the detected signal for subsequent launching of appropriate response.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: This project will make available new or improved technology able to detect low or difficult to be detected radioactive sources and nuclear materials. It will therefore contribute to minimise the risk of use or disseminating of such substances in the population.

Topic SEC-2011.1.5-2 Identification and Development of low-risk alternatives to high-risk chemicals – Capability Project or Support Action

Description of the topic:
As underlined in the EU CBRN action plan, high-risk chemicals can be used by malevolent individuals or organisations and are a security threat for civilian population. The research should look into the chemical or physical-chemical properties of high-risk chemicals, their ways of production, processing, transport and storage, and explore alternatives for lower risk chemicals. As a first step an inventory of substances in question is required.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: The scientific knowledge basis developed during the project should contribute to the reduction of production and use of high risk chemicals at mid or long term.

Topic SEC-2011.1.5-3 Development of improved forensic tools applied to radiological contaminations – Capability Project

Description of the topic:
Radioactive and nuclear (waste) materials can be used by terrorists to assemble a radiological dispersal device (RDD). The main objective of this project is to improve the forensic chain from the field to the court in case of such an act. This project should complement other EU research activities in the forensic domain.
The project should focus on the following topics; (a) the stability of traditional forensic evidence (e.g. DNA, fingerprints) under conditions of radiological contamination, (b) the securing of traditional forensic evidence under conditions of radiological contamination, (c) the cooperation between police forces, forensic laboratories and highly specialised laboratories without breaking the chain-of-evidence, (d) the forensic profiling of radioactive materials in order to interrelate seized batches of materials from different origins and (e) the development and validation of techniques and protocols for the securing and evaluation of such radioactive (contaminated) evidence.
Specific tools and best practices should be investigated and could be developed as plug-ins that could be inserted in a global EU forensic open framework (this last item should not be developed in the proposal). The results of this project will be of key importance for prosecution of criminal or terrorist acts involving nuclear or other radioactive material.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: To help law enforcement agencies to deal with radiological events in a more standardised way around EU.

Activity: 10.2 Increasing the Security of infrastructures and utilities

Actions in this activity will concentrate on targets of an incident or disaster of transnational importance, examples for infrastructures include large scale event sites, significant sites of political (e.g. parliament buildings) or symbolic (e.g. particular monuments) value and utilities being those for energy (including oil, electricity, gas), water, transport (including air, sea, land), communication (including broadcasting), financial, administrative, public health, etc. A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases ‘protect’ but also ‘prepare’. The ambition is both to avoid an incident and to mitigate its potential consequences. To build up the required capabilities, emphasis will be on issues such as: analysing, modelling and assessing vulnerabilities of physical infrastructure and its operations; securing existing and future public and private critical networked infrastructures, systems and services with respect to their physical, logical and functional side; control and alert systems to allow for quick response in case of an incident; protection against cascading effects of an incident, defining and designing criteria to build new secure infrastructures and utilities.

This activity is divided among five areas: **Design, planning of buildings and urban areas; Energy, Transport, communication grids; Surveillance; Supply chain; and Cyber crime.** The focus in the Cyber Crime area lies on the sets of tools, instruments, rules, etc. used for the prevention, detection, counteracting or investigation of, criminal (including terrorist) activities

targeted to the cyber environment, or to any subject's material or immaterial assets or infrastructures, and delivered through the cyber environment.

Area: 10.2.1 Design, planning of buildings and urban areas

No specific topic for this area has been planned for this call.

Area: 10.2.2 Energy, Transport, communication grids

Topic SEC-2011.2.2-1 Airport checkpoints - Integration Project

Passenger checkpoints are locations where people and objects pass through, while they are inspected for (visually hidden) prohibited articles, including liquids and gels, under both ordinary or exceptional security measures (for example during a red level alert due to an imminent terrorist attack). The primary function of a checkpoint is implementing security in the flow of objects or people, but a high throughput of passengers is also required. Examples of checkpoints are passengers and cabin baggage checkpoints, staff checkpoints, hold baggage screening locations. The present topic will focus on the checkpoints used by passengers and crew staff, including their cabin baggage, before boarding airplanes.

The goal is to design a better, smarter, more reliable and flexible checkpoint that delivers efficient and cost-effective security and ensures a positive passenger experience at European airports. For this:

The research should develop a design process and a shared evaluation platform for European airport checkpoints (either centralized or distributed). The design process and evaluation platform should deliver operationally acceptable, modular, qualitatively and quantitatively adjustable security, where technology solutions as well as requirements are integrated and interoperable into a much higher degree than nowadays.

The research should seek to align operational and security processes for improving passenger facilitation. The research should ensure that results are measurable at each checkpoint and should identify the most appropriate technologies and how they can be deployed to ensure an effective outcome. The research should anticipate on future needs to cope with the broadening of threat scenarios (e.g. liquid and solid explosives including homemade explosives. The research should also identify which of these criteria would be applicable to security checkpoints in other transport modes, particularly mass transportation.

The checkpoint design and evaluation process would address all the necessary modules to meet all criteria (security, operational, facilitation, ethics/human rights/privacy requirements human factors and ergonomics), but it should be adaptable to include other modules later. The design process should also allow for the assessment of the impact of new technologies and methods on security levels and operation, potentially expandable to assessing the ethical aspects and costs.

Funding Scheme: Collaborative project (large scale integrating project)

Expected impact: The research is intended for its use in aviation security to comply with regulatory requirements while optimizing operational efficiency, security and cost effectiveness. It should have an influence on the overall checkpoint security performance

criteria of governments and authorities responsible for security regulation, and to bring manufacturers to develop truly innovative technologies and solutions. Stakeholders must be directly involved in the research. The following impacts are expected in particular:

- Whole checkpoint design and performance: measurable security performance criteria on checkpoint scale instead of single equipment scale, and for all technologies currently or proposed for use at airport checkpoints
- Demonstrable difference between state of the art and the checkpoint of the future; improved detection capability and increased automation
- Privacy by design: procedures and equipment in the future scenario should not raise concerns as to the compliance with legal requirements, such as fundamental rights and protection of personal data in particular.
- Human factors: a design that supports operational staff in their work and the passenger experience. The design should be measurable by both these stakeholders.
- Integrates operational and security needs with enhanced security and improved passenger facilitation
- Unpredictability; how it is incorporated and its impact on passengers and staff
- Identification of those design criteria that may be applicable in other transport or civil security systems.
- Technology development needs: The research should indicate a roadmap for technology where further development is needed to better meet the objective.

Topic SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic Attacks - Capability Project

Description of the topic:
Future civilian critical infrastructures could be exposed to deliberate attempts at disruption/destruction by non-nuclear EMP (electromagnetic pulse) or HPM (high power microwave) means. This not only means conventional and novel hardening, but also systemic resilience features as well as methodologies and instruments for detection and verification of attacks capabilities. With the danger being perceived as abstract at best, a thorough risk assessment and database on the costs of such attacks should be created, as this would strongly underpin the necessary legislative incentives and enforcement of such hardening measures. Therefore, a regulatory and organisational framework should be implemented that would also provide methodologies and procedures, designate responsibilities and offer help to affected parties. Particularly security and emergency services should use hardened equipment wherever possible. All of these capabilities represent gaps today and in the near future. There are neither regulations nor organisations in place, and detection means are non-existent. No assessment or evaluation methodologies are readily available, and threat awareness is mostly missing.

Objectives:

- Threat analysis and risk assessment of the occurrence of such events and their most likely modalities.
- Investigations of high power microwaves (HPM) pulses influence on various civil objects: buildings, energy units, transport, banks, communication systems, computer networks, computers and electronic units.
- Investigate to what extent the current protection is efficient.

- Prepare HPM detection, diagnostic system and risk management, mitigation, reference HPM pulse power sensors and standards.
- The project should provide recommendations tools, of the shell materials and redundancy architectures, for protecting civil objects against microwave radiation.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: Provide a clear view for the policy makers on the possible threats of an electromagnetic attack, i.e. assessing the vulnerability of Critical Infrastructures and indicate tools and materials to improve the resiliency against EMP/HPM attacks

Area: 10.2.3 Surveillance

No specific topic for this area has been planned for this call.

Area: 10.2.4 Supply chain

Topic SEC-2011.2.4-1 International postal supply chains - Integration Project

Description of the topic:
Postal services are or might be used for smuggling, drug trafficking, money-laundering and (low-cost) terrorism. Thus the aim is to create a system for screening and identifying suspicious items following a risk-based approach. It may use existing systems and be built upon a common architecture for exchanging information between postal operators and customs authorities.
National and international legislative context, especially on privacy and postal secrecy, and standardisation issues should be taken into account. Collateral benefits for postal operators are an important factor for ensuring a broad acceptance of the system. Localisation and tracking systems could be also considered.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact: The system should allow for an efficient and effective recognition of suspicious items, while fully safeguarding the information chain and privacy (postal secrecy). Furthermore, it should contribute to a common European approach for standards and procedures.

Area: 10.2.5 Cyber crime

Topic SEC-2011.2.5-1 Cyber attacks against critical infrastructures - Capability Project

Description of the topic:
The objective of this topic is to successfully prevent cyber attacks issued by criminal organisations against telecommunication networks and SCADA (Supervisory Control And

Data Acquisition) systems supporting critical infrastructures. To reach this objective it is necessary to develop efficient and real-time monitoring, detection, diagnosis and reaction approaches to increase critical infrastructures reliability, resiliency and security. ICT (information and communication technologies) systems supporting critical infrastructure (e.g. energy plants, water plants, financial entities, public administrations, transport networks, etc) are no longer separated and isolated entities. The interconnection with other public and open networks causes security problems, and successful attacks may have significant effects, such as, for example, energy blackouts. Moreover, the crucial information from monitoring systems may be delayed or even lost, preventing early warning systems from proper and on-time reaction.
The targeted tools would also aim at analyze, test and benchmark the performance capabilities of ICT infrastructures supporting critical infrastructure (example: Firewalls, IPS/IDS, anomaly detection systems, threat forecasting systems, network access points, anti spam, antivirus system). This could include the exposure of shortages in actual systems in their respective interconnections.
Thus, there is a need for novel solutions and systems assuring protection of ICT/SCADA systems supporting critical infrastructure, with particular focus on cyber defence.
Related existing activities funded notably under the FP7 Security and ICT themes have to be taken into account. The consequences of the various national and international legal contexts, such as respect for fundamental rights and in particular the protection of personal data as well as related policy initiatives are important and should be taken into account as well.
The action should be an opportunity for networking and exchange between the stakeholders to facilitate the emergence of common European solutions. The active participation of end users (e.g. public authorities, relevant EU agencies) is essential.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact: This work should enhance reliability and resilience of ICT systems supporting critical infrastructures.

Activity: 10.3 Intelligent surveillance and enhancing border security

Actions in this activity will deal with issues relevant to all the consecutive tiers of European border security strategy, starting with visa application procedures in embassies and consular posts (1st level), cross-border cooperation (2nd level), measures at the border crossing points at land borders, harbours and airports as well as between the border crossing points at green and blue borders (3rd level) and finally activities inside the European external borders (4th level) such as exchange of information, compensatory measures, Schengen Information System (SIS), Judicial and Police, Customs and Border Guard cooperation (PCB). A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases ‘identify’, ‘prevent’ and ‘protect’. The ambition is both to avoid an incident and to mitigate its potential consequences.
To build up the required capabilities, emphasis will be on issues such as: enhancing the effectiveness and efficiency of all security relevant systems, equipment, tools and processes used at border crossing points (e.g. identification of accessing people, non-invasive detection of people and goods, tracking of substances, sampling, spatial recognition including data capture and analysis, etc.); improving the security of Europe’s land and sea borders (e.g. through non invasive and underwater detection of vehicles, tracking of vehicles, spatial

recognition including data capture and analysis, surveillance, remote operations, etc.); maritime security; assessment and management of (illegal) migration flows. A suitable framework will be established to coordinate with the activities of the European Agency for the Management of Operational Cooperation at the External Borders[21].

This activity is divided among five areas: **Sea borders; Land borders; Air borders; Border checks; Border intelligent surveillance.**

Area: 10.3.1 Sea borders

No specific topic for this area has been planned for this call.

Area: 10.3.2 Land borders

No specific topic for this area has been planned for this call.

Area: 10.3.3 Air borders

No specific topic for this area has been planned for this call.

Area: 10.3.4 Border checks

Topic SEC-2011.3.4-1 Security of biometric data and travel documents – Integration Project

Description of the topic:
Citizens expect high levels of security from digital systems. This topic addresses research aimed at enhancing the accuracy of biometric and other identification inspection devices (when used at border controls) by developing stronger authentication processes and technologies, for better secure real-time authentication of individuals, while at the same time protecting individual privacy. From the start, a 'privacy by design' data protection approach should be embedded in the architecture separating data of different streams, combining privacy management systems, with effective 'anonymisation' of personal data.

The increasing global use of *ePassports* has led to the availability of biometric information on passports that can be used for automatic processing. However, the potential advantages that this new technology brings in terms of speed/ease of use have to be assessed against potential vulnerabilities, and is limited by lack of reliable, easily- accessible and rapidly updatable systems for the exchange of certificates by issuing states/agencies attesting the authenticity of such documents.

There are ongoing efforts to establish a rapidly updatable system for the exchange of certificates attesting the authenticity of *ePassports*. However, questions have been raised about the possibility of impersonation or attacks against the technology currently used. New

[21] FRONTEX

ideas on possible technologies to ensure the authenticity of certificates and documents are needed. The project would propose at least one different technology for the issuance and checking of *ePassports* and for the production, exchange and reading of certificates authenticating them.

Border checks processes (with the introduction of VIS) gather a large amount of information which could be used better, while ensuring proper data protection. Checks against national, SIS, VIS and Eurodac databases as well as PNR and API data (and, in some MS, national E/E records), for example, are currently generally performed, and held, separately. Relevant information from consulates issuing Schengen biometric visas and inland biometric checks are also performed and the information they produce held separately.

The action would i) look at what information is needed to perform necessary checks and how privacy rights can be ensured, ii) look at ways of combining available information from relevant databases as per the relevant legal requirements to provide a one-stop shop for users such as border guards at MS level, iii) suggest what data could be combined and what type of analysis could be provided at EU level from such databases and target audiences, iv) develop protocols to interchange information to allow travel documents to properly identify border control authorities, in order to grant them access to biometric or confidential data contained in the document.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact: To significantly improve the security and usability of *ePassports*. Practitioners would have quicker, easier-to-use and more complete information available to them at point of use and their organisations (as well as EU and other relevant agencies) would have better analysis both of migration flows and of criminal movements across borders at EU level thus helping to improve policymaking in a wide range of areas.

Topic SEC-2011.3.4-2 "Artificial sniffer"- Capability Project

Description of the topic:
This topic refers to the integration in a one stop shop of different technologies for the detection of illegal substances and hidden persons, border control being closely linked to customs control of goods (this category comprises, inter alia, weapons, drugs, CBRNE, legal goods subject to duty, goods subject to import or export restrictions and those that fail to meet health and safety standards). At the moment, several disconnected devices are used ad-hoc. Dogs are essentially trained (and capable) to detect the presence of one specific substance.
The challenge requires mainly technological capabilities for achieving better parallel identification of the elemental, molecular, or biological composition (in order of increasing complexity) features of the material sought after.
If possible, solutions should incorporate a stand-off capability, flexible, fit to be automated, upgradeable, mobile, user-friendly and affordable. The 'mechanized dog' should be able to detect in parallel a variety of possible illicit elements, with reliability, high speed of detection and identification, allowing fast threat assessment. The research should focus on exploring the overall process (how to collect odours and store them, what is the best protocol to compare, how to evaluate the performance...). A metric to assess performance should be presented to be validated under operation conditions. This assessment should take place already at the

midterm of the project in order to define the best way forward. Existing related research activities have to be properly taken into account.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact:

- Today many of the sensitive controls are carried at border checks by trained dogs, which cannot be replaced, nor expected to operate on a 24/7 mode.
- The technology should be seen as a complement to them.

Topic SEC-2011.3.4-3 Border crossing points of the future - Capability Project

Description of the topic:
A common challenge for customs and border control authorities is to improve the processes related to the increasing flow of cargo and people crossing borders, without undue delay and with minimal intrusion, whilst employing affordable technical and human resources. Each type of Border Crossing Point (BCP) presents particular challenges (for example, airports have constraints of available time and space, sea ports of available time and perimeter security, land BPCs of infrastructure/space availability and connection with land BCP/road network of neighbouring countries) which affect the workflows for performing checks. Moreover, the ability of border guards to perform checks will be constrained by the environment in which they work (human factors).

Research is needed to improve the design of land and maritime checkpoint infrastructure, technologies and processes at border crossings so that checks may be carried out in a more reliable, convenient and efficient manner. The action will identify and analyse relevant constraints affecting security and efficiency of land and maritime checks (ID and detection) for each type of BCP and propose an innovative model solution for each. The research will consider the combination of existing and new technologies and redesigned processes in order to solve several unsolved problems and new paradigms related to the detection of illicit material and to the introduction of new electronic travel documents and visas for third country nationals entering the Schengen space. The study will include a human factors analysis of the ergonomics of equipment used and their effect on efficiency at each type of BCP (whether checks are performed on trains/buses/ships, influence of quality of images from CCTV/scanning equipment on threat recognition). Special attention needs to be paid to the use of mobile systems at land border crossing points. Emphasis will be given to the overall flexibility of implementation of the proposed processes.

Identify key infrastructure and ergonomic constraints at each type of BCP and suggest one ideal solution per BCP type to aid planning and efficient, speedy performance of border checks.
The compliances of the proposed processes with the legal requirements such as respect for fundamental rights, in particular the protection of personal data and with the ethical principals are important elements that need to be addressed by the action.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact:

- Identification of key infrastructure and ergonomic constraints;

- Streamlining of passenger traffic;
- Higher detection rates of illicit goods at higher speed with lower false alarm rate;
- Increasing security by reducing so called “human errors”;
- Ensure the ‘privacy by design’ of the new systems (i.e. more secure, less invasive, less legally and ethically questionable).

Area: 10.3.5 Border intelligent surveillance

No specific topic for this area has been planned for this call.

Activity: 10.4 Restoring security and safety in case of crisis

Actions in this activity will focus on technologies providing an overview of, and support for diverse emergency management operations, such as in civil protection (including natural disasters and industrial accidents), humanitarian aid and rescue tasks. A series of capabilities are required to cope with this mission area, many of which primarily relate to the phases ‘prepare’, ‘respond’ and ‘recover’. The ambition is to mitigate the consequences of the incident. To build up the required capabilities, emphasis will be on issues such as: general organisational and operational preparedness to cope with security incidents (e.g. inter-organisational coordination and emergency communication, assessment of strategic reserves, strategic inventories, etc.), crisis management (e.g. integrated means of alert and management, assessment of the incident and priority requirements, integration of heterogeneous actors and resources, evacuation and isolation, neutralisation and containment of effects of terrorist attacks and crime, etc.), intervention in hostile environment, emergency humanitarian aid and the management of the consequences and cascading effects of a security incident (e.g. the functioning of the public health care system, business continuity, confidence building measures, restoring the disrupted or destroyed functioning of society, etc.).

This activity is divided among four areas: **Preparedness, prevention, mitigation and planning; Response; Recovery; CBRN Response.**

Area: 10.4.1 Preparedness, prevention, mitigation and planning

Topic SEC-2011.4.1-1 Crisis management modelling tool - Integration Project

In the area of crisis management, several tools for foreseeing the evolution of incidents already exist. These tools are specific to each hazard, like: propagation of forest fires, raising of the river water level, dispersal of toxic fumes, land movement intensity following an earthquake. The nature of a crisis requires a tool that can provide a multi-sectorial foresight of possible consequences of the incident (For example – estimated numbers for deaths and injured, losses of property, environmental conditions, situation of overload of the roads damage in communications infrastructures). It should also provide decision makers with the capability to simulate possible outcomes resulting from possible actions. Crisis management capabilities (including personal and equipment) need to be carefully planned in order to have an effective use of the limited available resources. This action should aim at the development of a tool for the modelling of capabilities, concepts, operational activities and realistic crisis scenario for both:

- the assessment of existing / available capabilities and the definition of vulnerabilities / capability gaps, and
- the planning, monitoring and assessment of a real life operation.

This simulation based decision making systems should be implemented into a collaborative, modular and open environment, taking into account the many available 'capability bricks' already existing.

Focusing on one or more category of crisis, e.g. (large) natural disasters, humanitarian crisis, conflict prevention, security sector reform operations, the action will preferably include the development of realistic models and the integration of modules such as progress/achievement indicators and setting up of new/updated priorities. The future operational development of additional bricks (equipment, scenario, modules) has to be integrated and adapted to non specialist developers.
The active participation of potential future users is essential.

Funding schemes: Collaborative Project (large scale integrating project)

Expected Impact: Facilitate on the one hand the planning of operations (make difficult choices and prioritisations) and their subsequent monitoring, and on the other hand, the identification of capability gaps. The developed tool should help crisis managers and decision makers to analyse and assess their capabilities in order to achieve an optimisation of resources dedicated to crisis response and to understand the evolvement of a crisis, the impact of their decisions and actions on this evolvement, thus preparing better plans of action, during the preparedness as well as the response phase.

Topic SEC-2011.4.1-2 Psycho social support of Crisis Management – Capability Project

Description of the topic:

Affected public and crisis responders have to deal with different forms of stress and other psycho-social strains and traumata; in order to reduce the short-, mid- and long-term consequences of the various forms of stress and psycho-social strains, psycho-social support should be provided in a timely and professional way. People will be confronted with injured, mutilated, traumatised persons and probably also fatalities. External circumstances such as the extent of the devastation, suddenness, force and brutality of the incident, or suspected contamination, may intensify impressions. However, the community in a larger sense and society itself may be affected and suffer from the event which might bear larger cultural, societal consequences and losses, for which support should also be provided.

Thus psycho-social support is not only relevant during the crisis itself, but also afterwards during the recovery phase, sometimes even for the long-term, and may have to extend well beyond the persons directly impacted, such as first responders and the victims and public on the scene, and those indirectly impacted such as family members and para-medical and medical personnel, to a larger audience who might be witness to the incident through media and internet reports. The immediate impact and effect over time of stress and traumatic stress on response forces and crisis management personnel and authorities should also be taken into account. All these elements may have an effect on the dimension, magnitude, duration and repercussions (including delayed repercussions) of a crisis.

Research should identify optimum deployment scenarios of medical and psycho-social intervention forces. Following an analysis of existing approaches and best practices, effective intervention strategies and related support should be developed.

Bottom-up strategies - built up on the capabilities and know-how present on the ground - and effective intervention techniques using adequately trained laypersons instead of professional personnel - who might be scarce - should also be developed.

Objective:

- To develop effective methods and tools for medical and psycho-social intervention for victims, intervention forces and volunteers as well as for the larger community during and after a crisis situation, including
    - Immediate/post-immediate psychological support (acute stress reactions),
    - Treatment of long-term consequences (trauma and PTSD - Post-Traumatic Stress Disorder);
- To improve psycho-medical preparedness for crisis situations (contingency planning for the early interventions, readiness of medical supplies and hospital facilities, determining training and intervention strategies to deal with stress during preparation, response and recovery phases,
- To develop tools able to assess the relationship between the level of stress of the Crisis Managers and the effectiveness of the whole Crisis Management System;
- To develop technologies and effective methods to provide social support to large numbers of people;
- To develop assessment tools for psychological fitness of crisis management personnel and authorities;
- To 'help the people help themselves', that is: to validate and support efforts at local level;
- To identify longer term psychological, societal and cultural impact of crises.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact: Improved psycho-social preparedness of the public and of first responders for crisis situations, effective interventions and appropriate treatment of people affected by psycho-traumatic problems resulting from disasters, societal recovery from, and cultural integration of, traumatic events.

Area: 10.4.2 Response

Topic SEC-2011.4.2-1 Post crisis lesson learned exercise – Capability Project or Coordination and Support Action

Europe has responded to a number of (natural) disasters over recent years, be it earthquakes like in L'Aquila (Italy 2009) and Izmir (Turkey 1999), Haiti (2010) or the series of massive forest fires in southern Greece. During those events the crisis response forces gathered crucial information through their work on the best/most adapted practices. In many cases, e.g. forest fires in southern Europe the responders are confronted with recurrent issues encountered previously during a similar situation by other responders. The existing knowledge of EU responders should therefore be gathered and evaluated through an exchange of information, thus creating a "lessons learned database". This would in turn serve for the better

preparedness and effective response to the future disasters and improve the capability to restore activity after a crisis situation.

Objective:

- As a first step the knowledge acquired by crisis management responders would be gathered, categorised and analysed through consultation with major international stakeholders. The methodology should aim for a holistic approach (i.e. including all phases of a crisis, improving the interoperability between first responders and their equipment, the decision making process, identification of victims/people, etc); it could be done through the organisation of workshop(s), conference(s) and/or table-top exercise(s).
- The results of this exercise should then be evaluated involving the main stakeholders on Crisis Management with a focus on the end users. The results should be presented in the form of a "living document" which would be revised on a regular basis.

Learning process itself, dissemination means (such as training) have to be investigated. The action should also lead to recommendations for further related research activities. A significant involvement of responders' organisations is essential.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected Impact: The action should increase the preparedness of the responders, crisis managers and decision makers and provide them with a set of guidelines on the best ways and means for different crisis situations.

Topic SEC-2011.4.2-2 Unmanned search and rescue solutions – Integration Project

Description of topic:

In particular large scale disasters like the earthquakes in Haiti 2010 and in L'Aquila, Italy 2009, but also local incidents like gas explosions destroying houses always require a range of search and rescue (SAR) measures and tools for the localisation and rescuing of victims in collapsed structures. A hazardous environment due to fire, danger of further collapses, contamination, etc. implies the use of unmanned SAR devices (either single or cooperative ones) and their seamless integration into C2/ C4I systems, sufficient communication links, adequate motion and navigation capabilities in hostile environments and appropriate human-system-interaction between first responders, victims and the unmanned SAR vehicles and ground vehicles and on-board devices.

In large scale incidents further challenges are frequently posed to multinational sets of first responders, with their SAR equipment and procedures operating on the spot, demanding improved technical and procedural interoperability. Those large scale scenarios furthermore demand suitable support for planning and managing of complex SAR operations (over land and sea), collecting all data required to compute probability areas and define search zones, planning the allocation and use of rescue assets, including vehicles and unmanned devices, monitoring and coordinating the operations. Other important characteristics of unmanned SAR systems are the easy deployment of appliances under limited transportation capacities and their self sustainability in environments with very limited logistics backup (e.g. lack of fuel, no electricity).

This capability/integrated projects should aim at

- Assessing the state-of-the-art in SAR devices, particularly unmanned solutions, and main technical and procedural challenges to be tackled,
- Liaising with relevant ongoing or past R&D projects,
- improving interoperability and equipment (sensors, detection, smart kit) for SAR operations of first responders in disasters, including ground vehicles,
- developing novel SAR solutions, including ground vehicles and cooperative unmanned devices, and assuring the seamless integration of these systems into C2 / C4I systems, sufficient communication links, adequate motion and navigation capabilities and human-system-interaction,
- delivering a suitable support system for the planning and managing of complex SAR operations (over land and sea) as outlined, including the use of cooperative unmanned SAR devices and multinational forces.
- Novel solutions for easy deployment of SAR vehicles and long term self sustainability of the devices in the field.

Funding schemes: Collaborative Project (large scale integrating project)

Expected Impact: This project should increase the effectiveness of rapid and coordinated response in SAR operations, in particular with regard to fast deployment needs, and the capabilities of first responders and crisis managers to use cooperative unmanned SAR devices in complex, multinational SAR operations.

Topic SEC-2011.4.2-3 Rapid deployment of shelters, facilities and medical care resources following a major disaster - Integration Project

Description of the topic:
Large scale disaster (mainly natural, but also some that are manmade, for example in case of large contamination of the environment) leave large amounts of population homeless, in urgent need for medical assistance and appropriate shelter, safe water and food supply.
These disasters (especially when the infrastructure is damaged or poor before the disaster stroke) and the response required pose an enormous logistical challenge. It requires the mobilisation of large quantities of goods, in some cases over large distances in poor and sometimes dangerous conditions.
The logistics are, sadly, in some cases the reason for delays in the humanitarian assistance to the people in need. Therefore there is an essential need to develop tools and methods that will speed up the deployment of urgent humanitarian assistance following a large scale disaster.
Novel solutions for rapid deployment of medical care facilities and supplies (e.g. medicines, blood, …), safe drinking water, food and appropriate shelter, to be provided to the people in need within the immediate first days following a large scale disaster. These solutions should focus on situations where logistical capacities and transportation capacities are scarce or badly affected by the disaster.

Funding schemes: Collaborative Project (large scale integrating project)

Expected impact: Novel tools and methods, new emergency response kits that will dramatically scale up the arrival time of emergency supplies to the people in need, in the time frame of hours, following a major disaster.

Topic SEC-2011.4.2-4 Enhancing crisis response abilities of the public – Coordination and Support Action

Description of topic:

While a lot of efforts are made in strengthening professional crisis response forces like first responders and crisis managers how to react in crisis situations like natural disasters or terrorist attacks, the knowledge of what individuals and the public as a whole who are affected by such an incident could actively contribute to contain and overcome the crisis still needs to be developed. Driven by the overarching key message of ESRIF (European Security Research and Innovation Forum) on *societal resilience*, i.e. that "[…] security research and innovation should focus on strengthening Europe's inherent resilience and ability to efficiently recover from crises […]", it is evident that Europe's ability to efficiently and quickly as possible recover is particularly determined by the reaction or non-reaction of everyman in case of an incident, especially in a large scale disaster.

In a long-term approach security research should analyse how the public as a "prime responder" could be best enabled to actively contribute to crisis containment and overcoming, and deliver appropriate measures (e.g. education and training) and tools to support this goal. As a first step, a study should be carried out thoroughly identifying and assessing potential key enablers enhancing individual and community based crisis response abilities.

This action should include:

- Surveying the state-of-the-art in integrating individuals, social groups, volunteers communities and the public as a whole into crisis preparedness and response, identification of worldwide centres of excellence and best practices,
- Assessing potential key enablers for human resilience and exploration of appropriate measures and tools for enhancing individual, family and community crisis response (e.g. self-help abilities, education of public how to behave in certain situations, involvement of public in large scale exercises, use of social network tools (twitter, facebook), dissemination of training material through Internet connected mobile devices, etc.),
- Technology Acceptance Models to assess the acceptance and ease-of-use of novel devices and means of communications for a wide variety of individuals and communities for the purposes of crisis management,
- Roadmapping of further R&D and other implementation needs towards the long-term goal of an "enabled European public", and/or
- Awareness raising among and dissemination of project results to relevant stakeholders, i.e. public authorities, first responders, emergency management practitioners, specialised education and training professionals, identified centres of excellence and the public itself.

Funding schemes: Coordination and Support Action

Expected impact: This study should prepare the ground for further research activities to reach the long-term goal of an "enabled European public" by achieving awareness about this concept and approach among relevant parties to be involved as described, and by describing and sequencing further R&D and other needs delivering a full concept.

Area: 10.4.3 Recovery

No specific topic for this area has been planned for this call.

Area: 10.4.4 CBRN Response

Topic SEC-2011.4.4-1 CBRN individual Protective Clothing - Capability Project

Description of the topic:

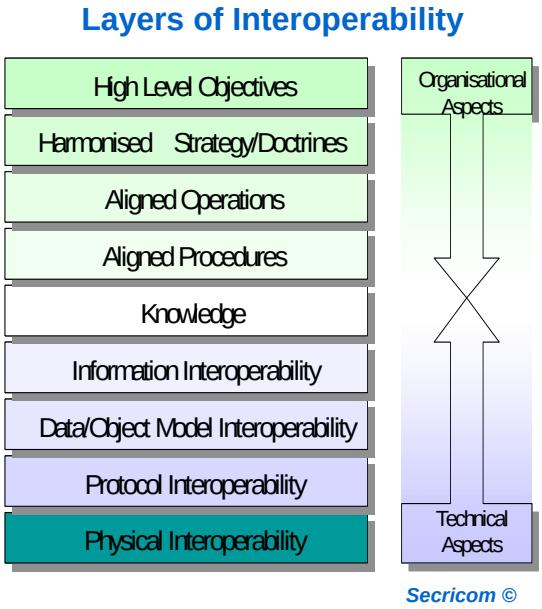
In case of a CBRN (Chemical, Biological, Radiological, Nuclear) crisis, individuals and particularly first responders need some protection. Various forms of protective clothing exist already but are e.g. difficult to use, of limited protection or too expensive.
Following a qualitative and quantitative evaluation of existing equipments the action is to develop innovative protective clothing for first responders and/or for the public in case of a CBRN crisis. It could focus on one or address several types of threats including pandemic crisis.
Concepts of use and distribution, including costs analysis, interoperability and standardisation of these equipments should be investigated. The participation of end users and / or public health authorities is encouraged.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected impact: Development of new and better protective equipments that enhance the security of first responders and individuals, helping them to work more efficiently within or to go through a CBRN crisis.

Activity: 10.5 Improving security systems integration, interconnectivity and interoperability

Actions in this activity related to intelligence, information gathering and civil security will enable and/or contribute to the performance of technology required for building up the above listed capabilities, thus focusing on cross-cutting issues such as: enhancing the interoperability and intercommunication of systems, equipment, services and processes, including law enforcement, fire fighting, civil defence and medical information infrastructures, while ensuring their reliability, protection of confidentiality and integrity of information, traceability of all transactions and their processing, etc. Activities will also address standardisation and training matters (including such with respect to cultural, human and organisational interoperability).



The capability of two or more organisations or discrete parts of the same organisation to exchange decision-critical information and to use the information that has been exchanged.

Clearly, interoperability ranges from organisational to technical aspects all of which must be 'harmonised' in order to achieve full interoperability.

This mission area seeks research that takes an outcome-oriented perspective, developing approaches (including methodologies that solve interoperability constraints) to achieve practical interoperability in both the short and longer term, while ensuring the reliability, protection of confidentiality and integrity of information. The focus is on the holistic aspects of interoperability, especially where solutions cut across the other Activity Areas. The relationship between end-user's processes and training with technological issues is expected to be an important element in this Activity. It is recognised that interoperability in the practical context of different organisations and nations is even more about processes than about technology. It is expected that actions in this area will involve research into the interaction between these technological and organisational factors.

Achieving interoperability between information and command functions is a high priority area, but achieving interoperability for other equipment that is deployed in security incidents is also within the scope.

This activity is divided in four areas: **Information Management; Secure Communications; Interoperability; and Standardisation.**

Area: 10.5.1 Information Management

Topic SEC-2011.5.1-1 Evaluation of identification technologies, including Biometrics

Description of the topic:
The main objective is to reinforce the reliability and interoperability of techniques used to identify / authenticate persons. A significant effort is expected on evaluating and perfecting metrics and criteria used for evaluating / validating / certifying identification technologies operationally (for instance by developing specific Protection Profiles using an approach similar to the one developed in the Common Criteria scheme ISO 14508), including biometric technologies often used in identity cards, visa applications and immigration services. This project should look both at the underlying supporting technologies and the identification processes themselves, paving the way to a 'European Identification Certification System' analogue to the Common Criteria scheme. In addition, mechanisms to identify vulnerabilities could be evaluated and integrated in the solution.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: to support the development of the proper legal framework (if needed) that fully complies with existing legal requirements, such as respect for fundamental rights, in particular the protection of personal data without endangering the EU legal privacy framework; to increase the industry's competitiveness by allowing them to compete using common standards, to demonstrate to the law enforcement agencies the added value of using common certified systems within the EU (international) operation; to demonstrate to the citizens that action/progress in this area is possible without building "a priori endangering privacy" systems.

Area: 10.5.2 Secure Communications

Topic SEC-2011.5.2-1 Technical solutions for interoperability between first responder communication systems – Capability Project

It is recognised that interoperability between communications systems used by different first responder organisations (e.g. TETRA and TETRAPOL systems) is a current issue in operations, especially those involving more than one nation, e.g. as in cross border operations. Many of the difficulties experienced are believed to be solvable through developing compatible security operating procedures, and/or procurement of suitable interface equipment. There are short term needs to address existing system investments, and longer term needs to develop new architectures for future communications systems.

The aim of this research action is to advance capability for the short term needs in proposing innovation solutions (technical, operational and legal) for gateways between existing networks.
Proposals must take full account of the available state of the art, industrial base and research already underway, e.g. physical and protocol interoperability was and is still subject of numerous projects funded under the FP7 theme 3: Information and Communications Technologies and in previous FP7 Security call projects.

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact Research results that offer a cost effective innovative solutions addressing the 'techno-organisational-legal' issues of effective, secure interoperability between first responders.

Area: 10.5.3 Interoperability

Topic SEC-2011.5.3-1 Establishment of a first responders Platform for interoperability[22]

Description of the topic:
The task is to establish an End Users Platform in order to stimulate the cooperation between providers and users (police, fire brigades, emergency services…) at each level of interoperability as presented in the figure above,

- for the use of public safety communication and information management systems to detect gaps and to ensure that the new technologies and tools to be developed fit their needs;
- for users requirements to be collected, assessed, compiled, updated, quantified and made available at EU level on a regular basis;
- to avoid shortfalls by analysing organisational issues, policies and behaviours issues which may lead to obstacles to interoperability.
- to allow for convergence towards some level of standardisation across Europe at the highest organisational levels operational processes and policies, as well as technology.

Funding schemes: Coordination and Support Action

Expected impact: To involve the end users (police, fire brigades, emergency services, etc.) in the security research projects in a more systematic manner ensuring that research results match their needs, thus improving the interoperability of public means for all types of safety and security missions (large scale and/or daily/ordinary missions as well as local or cross-border missions).
To create a global source of information and support forum for exchange of information and procedures for all user organisations allowing innovation from one organisation to benefit others.

[22] Policy related action: the management of the grant agreement will *not* be externalised to the REA.

To provide the industry with requirements and install a dialogue with all stakeholders for the EU research projects, to make economy of scale, to limit the duplication of users involvement and to strengthen the position of the European market.

Topic SEC-2011.5.3-2 Operational data exchange

Description of the topic:
The task is to explore the 'data/object model interoperability', the 'information interoperability' and the 'knowledge interoperability' as presented in the figure above, in order to help exchange of data about an incident between first responders within an organisation and between different organisations involved in an accident, by developing an ontology shared by all of the stakeholders. The tool should also take into account language/linguistic and cultural issues. Data model should also take into account location and time information. Real time interaction at operational level should be studied.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: Obtain the control of the different tools and methodologies of information management and make sense out of pervasive and ever-growing information. To understand the different options, cost and benefits to reduce the consequences of the functioning of data information systems in Service Oriented Architectures (SOA), ensuring that service consumers and providers exchange data in a flexible and consistent way that allows performance and scalability while taking into account language and cultural issues.

Topic SEC-2011.5.3-3 Developing interoperability frameworks for mission-oriented security systems

This topic is aimed at developing 'profiles' of standards and operating procedures that meet operationally defined interoperability needs, and detecting gaps where new technological solutions, guidelines, recommendations or standards are needed, at each level of the interoperability as foreseen in the figure above. The task is also to propose designing methodologies for specifying interoperability requirements and certifying compliance.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: Guidance on how to achieve practical interoperability, in order to address near term interoperability limitations and to link long term implementation of standards with certification methodologies.

Topic SEC-2011.5.3-4 Video archive search– Capability Project

Description of Topic:
Today many infrastructure operators (airports, railway, underground, etc.) are using video surveillance systems for security purposes. All these systems gather high volumes of data which are stored up for a specific period of time, usually legally defined. The exploitation of this huge amount of information, in a legal framework, is technically difficult for law

enforcement agencies, due to different compression formats, indexing systems, data storage formats, access systems and proprietary systems.
The aim of the action is to analyze the existing technical constraints and to look for appropriate search solutions. The action should make recommendations for interoperable standards, common practices and procedures taking properly into account the legal, ethical and democratic challenges of the use of video surveillance. Given the sensitivity of video surveillance, close links should be established with the projects to be selected after the topics in coordination with the FP7 theme SSH (Socio-economic Science and the Humanities)[23].

Funding schemes: Collaborative Project (small or medium-scale focused research project)

Expected Impact: Higher crime detection rates, better interoperability between video systems, ideas of video exchange and access standards, lower European dependency on non-EU-Systems, more secure and legally and ethically acceptable systems ('privacy by design' concept).

Area: 10.5.4 Standardisation

Topic SEC-2011.5.4-1 Towards standardisation of CBRN detection and identification[24]

Description of the topic:
The action should aim at the development of common and/or comparable methods, procedures and protocols for the detection, analysis and identification of CBRN (Chemical, Biological, Radiological and/or Nuclear) substances allowing a significant comparison of results from different laboratories and operators within Europe.

Large EU-wide round robin exercises should be included. These inter-laboratory trials will focus on substances that are most likely to be used by terrorists or being released incidentally in the environment. They could be qualitative for highly concentrated materials, but should be more quantitative with low levels of detection and quantifications for materials released in the environment in case of an incident (where possible, neutralised or non virulent compounds should be used). Different strategies and work plans have to be envisaged to take into account the important discrepancies between them in terms of existing protocols and standards.
The action(s) should take into account ongoing related activities (in or outside FP7). Definition of common standards should be open and transparent to the community of European stakeholders while taking fully into account the necessary precautions for the use of dangerous substances. If necessary, ability to deal with dangerous / restricted substances would have to be demonstrated in the proposal.

Funding schemes: Coordination and Support Action

Expected impact: This action will be the opportunity of in-depth networking of key EU CBRN laboratories and could serve as basis for the creation of a potential European network of reference laboratories or centres.

[23] See topic SEC-2011-6.1-5
[24] Policy related action: the management of the grant agreement will *not* be externalised to the REA.

Activity: 10.6 Security and society

Actions in this activity are of a cross-cutting nature and should be conducted by interacting between natural sciences, technology and other sciences, in particular political, social and human sciences. The focus will be on targeted cultural and socio-economic, as well as systemic risk analyses, scenario building and other research activities related to subjects such as: Security as an evolving concept (comprehensive analyses of security-related needs, in order to define the main functional requirements to address the fluctuating security landscape); interdependencies, vulnerabilities due to disasters and new threats (e.g. in the field of terrorism and organised crime); the attitude of citizens in crisis situations (e.g. perception of terrorism and crime, behaviour of crowds, public understanding of civil rights and socio-cultural forms of protection and acceptance of security (and safety) controls); preparedness and readiness of the citizen in case of terrorist attacks; issues related to communication between authorities and citizens in crisis situations; raising public awareness for threats; citizens' guidance on the internal security advisory and assistance systems in the Member States and at EU level; behavioural, psychological and other relevant analyses of terrorist offenders; ethical issues with respect to personal data protection and integrity of information. Research will also be directed into developing statistical indicators on crime to permit assessments of changes in criminality.

Security, whilst very important, is just one of the societal values in Europe which must be balanced against others. It is a tool in support of freedom and can only be achieved within the rule of law. The EU Member States have all signed up to the European Convention on Human Rights and the EU's Charter of Fundamental Rights has become legally binding. The EU and its Member States are bound to respect and to promote human dignity, freedom, democracy, equality, the rule of law and protection of fundamental rights (which include both the right to privacy and the right to security).
In this activity, the objective is to carry out research into all those political, social and human factors that influence European security solutions and related new technologies, and to specify how the proposed security solutions must be adaptable to diverse cultural and institutional settings.

Actions in this activity will provide improved insight and advice for security policy makers, security research programme makers and (mission oriented) security research performers (in some cases, acting as "Think Tanks"). They aim to obtain a broad and well-based understanding of the public administrative, cultural and societal frameworks in which security enhancing policy measures, including in particular security research, take place. In particular they effectuate in-depth understanding of the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. The outcome of the research together with appropriate dissemination strategies contribute to the effective and efficient planning and designing of future security research programmes and actions as well as to policies, programmes and initiatives which enhance the security of the European citizens.

As this activity takes a threat and incident related approach only, it is complementary to the more general approach of Theme 8 *Socio-Economic Sciences and the Humanities (SSH),* of the Cooperation Programme, as well as to the *Science and Society* area of the Capacities Programme.

The objective of the Socio-Economic Sciences and the Humanities is to generate in-depth, shared understanding of complex and interrelated socio-economic challenges in Europe. Security is addressed as one of these challenges and set in the general landscape.

Science and Society has the objective to stimulate, with a view to building an open, effective and democratic European knowledge-based society, the harmonious integration of scientific and technological endeavour, and associated research policies in the European social web by encouraging pan-European reflection and debate on science and technology and their relationship with the whole spectrum of society and culture. In that context, ethics in science and technology is addressed.

The security and society activity in the Security theme is targeted towards security challenges and addresses immediate and medium term issues.

Coordination between these activities takes place on a regular basis in order to ensure synergy and take advantage of the available knowledge.

This activity is divided among five areas: **Citizens, media and security; Organisational structure and cultures of public users; Foresight, scenarios and security as an evolving concept; Security economics; Ethics and Justice**.

Area: 10.6.1 Citizens, media and security

Research in this area will ensure that selected policies and technologies are responsive to the needs of the citizens, and that they create security approaches that are rooted and acceptable by society and citizens, with differing cultural backgrounds. It will also support political accountability and democratic control aspects of public services within the security arena.

This activity is complementary to the more general approach of Theme 8 *Socio-Economic Sciences and the Humanities*, of the Cooperation Programme.

The objective of the Socio-Economic Sciences and the Humanities (SSH) is to generate in-depth, shared understanding of complex and interrelated socio-economic challenges in Europe. Security is addressed as one of these challenges and set in the general landscape.

The security and society activity in the Security theme is targeted towards security challenges and addresses immediate and medium term issues.

To reach these objectives, a coordination is established between the Security Theme and the SSH Theme on the Impact for society of surveillance systems as presented for topic SEC-2011.6.1-5 below.

Topic SEC-2011.6.1-1 Analysis of the security systems in Europe[25]

Description of the topic:
The objective is to explore and compare relevant cultural phenomenon and legal determinations of civil security across Europe, taking into account the existing significant differences between countries and regions. Firstly, a sample of a few diverse security regional architectures should be studied in a comparative analysis regarding the sharing of responsibilities between public and private bodies and the role that citizens play in regional security architectures. Secondly, it should be studied how the identified differences affect the effectiveness and efficiency of different kinds of security systems.

Funding schemes: Coordination and Support Action

Expected impact: To give policy stakeholders a clear view which kind of systems that could successfully enhance the security in certain regions. The result should contribute and give EU-added value to the debate concerning "not one security fits all".

Topic SEC-2011.6.1-2 Protection of European citizens abroad

Description of the topic:
At the present moment no system can broadly localise and communicate with EU citizens abroad in case of a disaster (e.g. earthquakes, tsunami) within the right time frame and in all locations. The aim of the action is to investigate and define the capabilities and procedures which would help localise and inform consular personnel and citizens in crisis situations. It is important to take into consideration legal, sociological and ethical aspects, including preserving privacy.

Funding schemes: Coordination and Support Action

Expected impact:
Increase to the security of EU citizens abroad and contribute to the emergence of a European common approach.

Topic SEC-2011.6.1-3 Signs of 'early warning' to detect trends and weak signals in social polarisation, violent radicalisation development and segregation

Description of topic:
The task is to obtain a deeper understanding of the signs of 'early warning' and weak signals of social trends that may lead to violent extremism and even terrorism (e.g. polarisation, violent radicalisation development and segregation at collective or individual level), in order to facilitate effective policies and counter-measures and increase the society resilience. The first goal should be to use these signs to build indicators allowing to curb, stop or prevent these social processes. The second goal should be to understand whether and how specific contextual and structural conditions (e.g. residential segregation, social exclusion,

[25] Policy related action: the management of the grant agreement will *not* be externalised to the REA.

unemployment etc) may foster the adoption of extremist views resulting in violence/terrorism. Thirdly, technical and social environment (including Internet) should also be considered because they create rules and boundaries at the same time that they open new possibilities for terrorist activities. The internet should be treated as a stand alone context insofar as it offers a unique venue for information sharing, indoctrination, recruitment and organisation of attacks.

A particular effort should be made at measuring and predicting the technological capabilities of groups that are likely to radicalise violently. An attempt should also be made at forecasting technological evolvement which would lead into more dangerous forms of terrorism and defining early warning signs for such activities. This will enable monitoring of technical capabilities in addition to social driving forces. Main actors that are best positioned to provide early warnings should be identified and best practices and efficiency of existing action plans should be assessed. Alternative approaches and best practices tried out in different European cities, such as cooperation between police, schools and community activities should be looked into.
The research should in addition, address the possible pitfalls or risks of developing early warning indicators. It should integrate in the process ethical and legal issues, including on national level and elucidate in the results the relationships between the devised tools and privacy.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: Contribution to the 'European Union Counter-Terrorism Strategy' and more particularly to the 'Strategy and Action Plan on Radicalisation and Recruitment' adopted by the Council in December 2005. Actions in this area will improve the understanding of the threats posed by individuals and groups and provide to the local and regional deciders the possibility to adapt prevention measures early to avoid security problems caused by social phenomena leading to terrorism or violent extremism.

Topic SEC-2011.6.1-4 Reduction of the cognitive biases in intelligence analysis

Description of topic:
Intelligence analysts are involved in analytical processes to assess and react to certain situations. Throughout that analytical process, they might be subject to cognitive biases that may have a negative impact on the quality of the final assessment. The purpose of this topic is: a) to have an overview of cognitive biases (synthesis), b) to explore the extent to which cognitive biases can be described and modelled with the objective to reduce the risk for cognitive biases (feasibility) in analysis, and c) to investigate the potential integration of these models into analysis tools in a service oriented open architecture.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: Better understanding of cognitive biases and reducing their impact in intelligence analysis will improve the quality of information provided to security decision-makers.

Topic FP7-SEC-2011.6.1-5 Surveillance and the challenges for the security of the citizen [26]

(coordinated with the topic SSH.2011.5.1-2[27] Surveillance and the challenges for democracy and an open society of the 2011 SSH Work Programme.)

Description of the topic:
A wide range of surveillance systems and technologies have been developed and used by both public authorities and private actors over time, with a peak in the aftermath of the terrorist attacks of 2001. This has also been the case in the European Union, and the trend is likely to continue. It is thus necessary to examine the factors underpinning such development and –especially- their implications in terms of actual effectiveness in fighting crime and terrorism, social and economic costs, protection or infringement of civil liberties and fundamental rights and ethical aspects.

The topic aims at evaluating the impacts of different surveillance systems for the security of the citizens. Aspects such as reduction/displacement of criminality, prevention vs. prosecution, efficiency of treatment / storage of information, effectiveness in fighting terrorism, social and economic costs, etc should be taken into account, as well as legal and ethical aspects.
A large and comprehensive review of systems, procedures, use of surveillance systems in Europe and their effects on security, and the perception of them by the citizens, would allow decision makers to make better choices (how relevant the systems are for the planned applications, etc), and to give them a better understanding of the acceptance/non-acceptance by the citizens of different types of surveillance systems. It would further help manufactures to adapt their systems, and help users to adapt the deployed systems more efficiently. The

[26] Policy related action: the management of the grant agreement will *not* be externalised to the REA.
[27] The description of the SSH theme topic given below is for information purposes only. For details please consult the 2011 SSH work programme.

Topic SSH.2011.5.1-2. Surveillance and the challenges for democracy and an open society
A wide range of surveillance systems and technologies have been developed and used by both public authorities and private actors over time, with a peak in the aftermath of the terrorist attacks of 2001. This has also been the case in the European Union, and the trend is likely to continue. It is thus necessary to examine the factors underpinning such development and –especially- their implications in terms of actual effectiveness in fighting crime and terrorism, social and economic costs, protection or infringement of civil liberties and fundamental rights and ethical aspects.

Surveillance in diverse forms can help to fight crime and reduce violence in society, nonetheless it affects some fundamental rights and influences the way public discourse takes place. The open nature of democratic societies can make them more vulnerable to attacks on infrastructures or people; at the same time it can make them more resilient to those attacks in terms of social, economic and institutional responses. Research should address how surveillance affects the democratic society and societal values, including the way that surveillance and retention of data may be perceived in different contexts, including in post-totalitarian societies; how human relationships are affected under conditions of visible and invisible surveillance in public and semi-public realms; how fears are induced by terrorist and criminal attacks or manipulated by political, economic or media actions; how fears may public opinion in favour or against specific technological or policy measures; how insecurity may undermine open debate, democratic decision making and effective response to crime and terrorism; options for enhancing social, economic, institutional resilience should be also identified based on a comparative analysis of past and current experiences in Europe and elsewhere.

work should also take into account any previous studies and projects in this area also within other themes of FP7/FP6 (notably SSH and Science in Society).
The active participation of the different stakeholders and, in particular, involvement of end-users is essential. A large dissemination of the results is expected.
Funding schemes: Collaborative Project (small or medium-scale focused research project) and Coordination and Support Action

Expected impact: The outcome of the work should provide decision- makers with a better understanding of the impacts of different surveillance systems, and also help manufacturers and end-user better adapt the systems and their deployment.

Area: 10.6.2 Organisational structure and cultures of public users

An objective European joint security capability to handle security matters has to be based upon the resources and mandates of the Member States and Associated Countries. The distinct national systems must be interoperable, scalable and allow for mobility where appropriate. Research under this area will look at the organisational structures, behavioural and cultural issues of end user organisations in order to ensure applicability, user friendliness and affordability of security technologies and solutions.

Topic SEC-2011.6.2-1 Best practices for enhancing security policy in urban zones

Description of the topic:
Crime and instability in urban areas emerge from a variety of factors, for example, economic decline; poor urban planning; pre-existing ethnic/religious divides; endemic organised or gang crime; tensions due to immigration; etc. Such problems persist in many European cities and are likely to be amplified by the recent economic downturn. There is a need to identify and tackle these underlying problems as soon as possible to prevent undesirable security scenarios arising.
Tackling such security issues requires actions which are interlinked in a complex way. In order to mitigate these undesirable security scenarios the task is to examine best practice in successful urban zones – especially those that already have managed a successful transformation - and thereby to develop metrics that can inform local policymakers in distressed environments.
These metrics will consider the economic, environmental, educational and social actions which need to be orchestrated to suit local issues and context. It is expected that the metrics will be adopted and implemented by representative urban areas and that progress will be benchmarked throughout the course of the project.
The task might also consider the provision of an early warning system where metrics are used to alert authorities to the above dangers.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected Impact: The outcome of the project should be a systematic methodology that offers the prospect of a measurable increase in the resilience of some of Europe's distressed urban areas while taking account of variables such as culture, geography, etc. This best practice will

be implemented for selected urban areas leading to a demonstrable increase in economic prosperity, security and citizens' perceptions of security.

Area: 10.6.3 Foresight, scenarios and security as an evolving concept

Research under this area will improve our understanding of novel threats as well as technological opportunities and emerging security related ethical, cultural and organisational challenges. It will help authorities to assess investment alternatives for prevention, early warning or preparedness and to make the appropriate choices in addressing threats to public security that achieve social cohesion and fully respect fundamental rights, in particular the protection of personal data.

Topic SEC-2011.6.3-1 Assessing trends and threats in a society

Description of the topic:
In maintaining the agenda for Security Research aligned with future threats, continuous benchmarking of the activities is needed. This action should:

- analyse the results of completed, on going and planned security related research activities (in the context of the FP7 Security theme but not only,),
- analyse and compile previously identified needs,
- identify future possible/probable threats through possible scenarios,
- derive related needs and associated research priorities.

Possible scenarios should result from a comprehensive analysis of factors of the human / societal system, including: e.g. crisis prevention, new forms of terrorism; increased accessibility of technologies that could be used for malevolent intents.

The efficient use of new technologies available to administrative bodies in charge of the planning of security relevant research should be emphasised. This includes: modelling tools, treatment of experts opinions; virtual reality tools; risk monitoring; a 'Watch' function for early warning of weak societal signals, tools for the analysis of different factors or events to prevent crisis scenarios, etc…

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact:
To improve the integration of the results of the various FP7 security research projects in order to improve the situation awareness of the administrations and the population. To maintain up to date the Security research agenda.

Area: 10.6.4 Security economics

Research should include all economic impacts of security aspects, investigate the economic causes and consequences of insecurity, and the direct and indirect costs of security policies and how they contribute to or hinder economic growth. Understanding how perceptions, for example fear of terrorism, shape economic behaviour is also important. Evaluating the cost-

benefit relationship of security measures, even if difficult to assess, is important. Cost calculations should place specific emphasis on less visible impacts, including increased hidden costs, decreased efficiency and trans-boundary impacts, such as the interaction between security behaviour and economic growth over time. Society needs basic market data to understand the structure, conduct and performance of the security sector. Economic theory can offer key insights, enabling policy makers to optimise efforts to enhance security and growth.

Topic SEC-2011.6.4-1 Develop socio-economic methodologies which can be adapted to different missions in security research

Description of topic:
Citizens' needs, rights and expectations affect society's specific requirements on security. Even when taking those societal needs into account not all security measures are as effective as expected. Existing and future methodologies should handle new and future needs, which require being reviewed, improved and tested. The objective of the topic refers both to the analysis and definition of future expectations in terms of security and the methodologies to be applied to detect inefficiencies, according to the aim of a safer and sustainable society. The existing and future methodologies could be applied to the different missions defined in security research, in particular transport or critical infrastructure protection.
Transport and Critical infrastructure (CI) play a pivotal role for upholding primary societal functions. Their disruption or destruction would create a deep impact on the economic and social well being of the citizens. Researching the implications of such failures states a central condition for relevant safety and security measures to be developed and implemented by the responsible public and private security providers (end-users). Develop socio-economic methodologies which can be adapted to different missions defined in security research such as transport or critical infrastructure protection in order to help and support decision-making processes
The action could also assess the external dimensions of an attack on a CI, for instance energy supply lines, that would have not only a massive long term effect on the EU economy but also consequences regarding the relations with third countries.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected Impact: It is expected that the action under this topic will define a socio-economic methodology which could be properly adapted and used into different missions defined in security research, such as transport or critical infrastructure protection, in order to help and support decision-making processes on the viability of security measures, taking into account the impact on citizens, and to identify factors allowing a realistic impact assessment.

Area: 10.6.5 Ethics and Justice

Security technologies and policies raise various ethical and legal concerns, which influence public support and acceptance. Research under this area will address the privacy, data protection and human rights issues as well as acceptability, ethical and prioritisation issues, while taking into account a variety of approaches to ethical, social and legal questions based on divergent ethical, religious, historical and philosophical backgrounds. Aspects of social

exclusion, lack of social cohesion that may lead leading to the formation of areas of insecurity within Europe may also be considered, as well as aspects of the European Neighbourhood Policy relevant to security. This will contribute to the general discussion and help both security solution suppliers as well as end users to make better decisions when selecting and applying security technologies and solutions.

Topic SEC-2011.6.5-1 Conflict resolution and mediation

Description of the topic:
The overall idea for this topic is based upon restorative justice (RJ) containing theories, ideologies and practices of conflict resolution within civil and public societal sectors, involving people in democratic processes for peace building at different societal levels.
Being an alternative to other legal justice forms, the RJ approaches focuses on the relationships between people at conflict, not on adversaries; on parties and not on counterparts; i.e. emphasising solutions for the common future and giving less weight to the objective facts of the past. This approach may differ and constitute an alternative to academic as well as practice fields so far dominated by historical, technical and political scientific studies of peace, war, terrorism, risk, security and gross national/population violence.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected Impact: To provide alternative understanding of how to handle conflicts within democratic societies. The relativity of peace, war, terrorism, violence and insecurity may be at stake when alternative epistemologies are applied to human interaction in peaceful as well as violent contexts. The topic challenges the methodology of registering such interaction in different security contexts as well as asks for gender and age perspectives as pivotal parts of this endeavour within security studies.

Topic SEC-2011.6.5-2 The relationship between Human privacy and security

Description of the topic:
Several governments, and the European Union as a whole, have chosen to invest in new technological devices to foster a proactive attitude against terror (e.g. closed circuit television, passenger scanning, data retention, eavesdropping, biometric passport, etc).
Although these technologies are expected to enhance public security, they are subjecting ordinary citizens to an increasing amount of permanent surveillance, potentially causing infringements of privacy and a restriction of fundamental rights.
The traditional approach frames the relationship between privacy and security as a trade-off, whereby any increase in security levels would inevitably curb the amount of privacy enjoyed by any citizen. Therefore, mainstream literature on the public perception of security technologies generally aims at enquiring how much privacy citizens are willing to trade in exchange for security. The trade-off model has however been criticised, because it approaches privacy and security in abstract terms, and because it reduces public opinion to one specific attitude, which considers these technologies as both useful in terms of security and potentially harmful in terms of privacy, and alternative attitudes may exist and are allegedly more common. The proposal should explore the actual relationship between Trust and Concern, on the one hand, and Privacy and Security on the other hand.

In doing so the following questions should be addressed:

- Do people actually evaluate the introduction of new security technologies in terms of a trade-off between privacy and security?
- What are the main factors that affect public assessment of the security and privacy implications of given security technology?

The data should be gathered across Europe, for instance via surveys/questionnaires to a representative sample of the population. It should be analysed, and both national outcomes and comparative outcomes be generated.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected Impact: Provide to the users a decision support system providing them for insight into the pros and cons of specific security investments compared to a set of alternatives taking into account a wider societal context.

Activity: 10.7 Security research coordination and structuring

This area provides the platform for activities to coordinate and structure national, European and international security research efforts, to develop synergies between civil, security and defence research as well as to coordinate between the demand and the supply side of security research. Activities will also focus on the improvement of relevant legal conditions and procedures.

The Security theme, aiming at increasing the security for Europe's citizens and simultaneously improving the global competitiveness of Europe's industrial base, needs to utilise limited resources in an effective and efficient manner. It is embedded in a fabric of other relevant research work carried out under various other programmes both on the European level as well as in the Member States and Associated Countries. It can only reach its objective, if its outcome is eventually applied by the relevant end user communities.

This activity provides the platform for actions to coordinate and structure national, European and international security research efforts, to develop synergies between, and avoid duplication with, civil, security and defence research as well as to coordinate between the demand and the supply side of security research. Activities also focus on the improvement of relevant legal conditions and procedures.

It is understood however, that there will be certain areas where coordination and structuring are not sought, or needed, but equally there will be others where coordination and even co-operation would add value.

Actions in this activity will provide deeper insight and wider awareness of the European security related research and industrial landscape and the public environments and frameworks in which stakeholders operate. In particular actions will indicate opportunities and constraints for developing and strengthening a European security related market. Actions will ensure enhanced networking, coordination and co-operation of the Member States and Associated Countries as well as between relevant organisations on the European level. All this

which will contribute to the overall impact of the Security theme by making it more effective and efficient, it will raise the innovation level in the security domain and will achieve increasingly harmonised implementation approaches. It will also contribute to the design of future Work Programmes of the Security theme.

This activity is divided in six areas**: ERA-Net, Small and Medium Enterprises; Studies; Other coordination; End users; and Training.**

Area: 10.7.1 ERA-Net

Topic SEC-2011.7.1-1 Co-ordination of national research programmes in the area of Security research (ERA-NET)[28] [29]

Description of topic:
With a view to ensuring effectiveness and efficiency of the Security theme and also to exploit opportunities outside the EU scope, the task is to support cooperation and coordination of national and where appropriate regional research activities also in view of effectively meeting the specific needs of the security end-user groups. An ERA-NET should aim to (a) exchange information on the general situation of security research in their countries and define core areas of common interest to prevent duplication and identify synergies; (b) develop common strategies in the core areas and appropriate transparency mechanisms (referring to a joint capability and technology taxonomy, and considering scope and depth of the transparency as well as agreements on protection of intellectual property and handling of classified information); and (c) explore and demonstrate coordinated and/or joint initiatives in the area of European Security research.

Funding schemes: Coordination and Support Action (coordinating action)

Expected impact: Actions will ensure enhanced networking, coordination and co-operation of the Member States and Associated Countries as well as between relevant organisations on the European level. When appropriate, to ensure the effective achievement of the activities, ERA-NETs are encouraged to involve the largest possible number of security end-users in their consortia. All this which will contribute to the overall impact of the Security theme by making it more effective and efficient and will achieve increasingly harmonised implementation approaches. It will also contribute to the design of future Work Programmes of the Security theme and could take advantage of existing examples of end-user cooperations already active in this field.

Area: 10.7.2 Small and Medium Enterprises

Topic SEC-2011.7.2-1 Effective approach between end-users and SMEs

In the previous calls of the security research theme, measures have been promoted for the consolidation of a Security European market. The key idea has been the promotion of the

[28] See page 57 the specific eligibility criteria for ERA-NET
[29] Policy related action: the management of the grant agreement will *not* be externalised to the REA.

establishment of a value chain, namely, all actors, from the end-users to the scientific research providers were aligned according to security missions. However, this overview implies that the resolution of the more demanding security problems will be addressed from a global large scale perspective, in which the SMEs are always subsidiaries of large companies and integrators. On the contrary, there are problems that need a much more immediate approach and which do not depend on establishing all the links of the value chain, but that can be provided as a service or as a product supply. In such situations, the ability of dialog of the SMEs depends much of its commercial activity, which is normally very limited

This topic aims at funding projects that propose actions to facilitate the relationship between the end-users and the SMEs within a framework of European cooperation, learning from experiences from other sectors, and taking into account the particular characteristics of the security market, the end-users needs, and the ability of response from the SMEs. It is also required to propose platforms and procedures for information exchange and brokerage, based on previous success cases. All that will be complemented with information on the technological needs of each party and the possibility of launching an initiative or specific program to facilitate it.

Funding schemes: Coordination and Support Action

Expected Impact: To facilitate the exchange of information between the end users and the European SMEs to access to cutting edge technologies produced by small technology-oriented businesses. To provide to the SMEs a wider market in which the economies of scale allow them to address more effective solutions and also envisage riskier ideas and projects.

Area: 10.7.3 Studies

No specific topic for this area has been planned for this call.

Area: 10.7.4 Other coordination

Topic SEC-2011.7.4-1 Networking of researchers for a high level multi-organisational and cross-border collaboration

Description of topic:
An increasingly large number of experts in Europe work on security research, with knowledge and specialisation in this area. However it is sometimes difficult to find and identify the right expertise at the right location and the right moment. Dedicated training actions in the domain of security are also relatively scarce in Europe. European security research experts are spread over many EU countries, thus stressing the need to create virtual centres of research competence to network all this expertise, to exchange knowledge, develop new ideas and new trends in their respective area.
The topic aims at an integration and reinforcement of existing co operations and cross-border collaborations, as well as establishing new ones, at high level in the security research domain, and at the same time stimulate appropriate training activities. Researchers and entities (research centres, stakeholders, from both academia and industry, as well as end-users) ready to integrate a part of their research activities should become part of this network. This

integration should start around some concrete technical projects and aim for a long lasting cooperation based on a joint programme of work leading to the emergence of a 'virtual research centre' in a specific security domain. This network could focus on specific areas of Security research. Activities on cyber-defence, secured communication or related to the societal dimension of security are strongly encouraged.

Funding schemes: Network of Excellence

Expected impact: Virtual centre(s) of competence in specific domain of security research should increase the quality and impact of relevant training and research in Europe by bringing together the top specialists and encourage the exchange of knowledge, development of new ideas and new trends in the respective area. By virtue of such a virtual structure the innovation process should be significantly enhanced, to the benefit of the competitiveness of EU security industry and the enhancement of the security of the citizens. The research networks could also be used for providing advice to policy-makers in their respective domain.

Area: 10.7.5 End users

Topic SEC-2011.7.5-1 Innovation and research within security organisations

Description of the topic:
Organisations dedicated to the provision of security services, especially public end-users, have many difficulties to address the innovation management aspect, since most of the operational missions are conducted with time-pressure and with difficulties to obtain records and analyze the data that have been gathered. This leads to an extremely dependent position when trying to assess the technology and a weakness when trying to expose their needs.

The main objective of this action is to analyze the main aspects of Innovation Management in the security-related operators (end-users), both public and private. It should include the adaptation of effective tools for technology watch, road mapping and forecast to the security sector. It should find mechanisms that encourage an appropriate use of technology responding new threats, in the medium to long-term. It should seek the promotion of the innovation culture within the end-users with an important workload. It should support the early demand in R&D. It should foster new business models for the Security sector that may emerge after a change of vision with regards to technology. It should promote the security and privacy requirements at the early stages of systems developments ("Security and Privacy by design"). It should promote a rationalisation of gap analysis and procurement strategies.

Taking fully into account that technologies by themselves could not solve the security challenges, the action should include the analysis and impact of new technologies and review their ethical and legal implications.
The action should be the opportunity to networking activities and exchanges of best practices between the security end users in Europe, contributing to the emergence of common needs and common cultures. The active participation of a large range of end users is essential.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected Impact: To forecast the possibilities of accessing to strategies and to implement innovation management systems in the security research field. Assessment of the training needs and opening new areas of action that would lead to greater effectiveness in operations.
For the suppliers: To reinforce the cooperation between the product/services suppliers with the end-users. To develop products/services compliant with end-users' needs.
This would cause greater efficiency in the organisations and the release of resources for other tasks. It should also ease the rationalisation of the market while contributing to the development of European standards.
For the scientific-technological agents: New areas of collaboration with manufacturers and also with the Security operators.

Topic SEC-2011.7.5-2 Definition of requirements by civil Security end-users for large air transport systems[30]

Description of the topic:
In a case of a large crisis (e.g. earthquake) that destroys the infrastructures or where infrastructures barely exists or cannot be safely used, transport and deployment of responders and their equipment has proven to be a difficult point, especially for the last miles. Available equipment or resources cannot always been transported on the location where they are urgently needed. Air transport means exist already but are often not exploitable either due to the destruction of infrastructure or due their difficulties to fulfil the needs of civil end-users and to be inserted in their process.

The objectives of the action are:

- to investigate the possible use of high capacity air transport systems for security users;
- to gather and define clear requirements for civil security users;
- and to feed these requirements and including a dual-use dimension at an early stage of the definition of large programme, mainly targeted to military use.

The action should include the definition of potential missions (e.g. deployment of first responders, maritime rescue operations, evacuation operations, flying hospitals, fire fighting, deployable command and control centre, etc.), cost and maintenance issues and their compatibility with a civilian use, training, interoperability, communications, certification, etc.
The active involvement of a broad range of potential users and the links with existing parallel activities for the definition of the military use are essential.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: To significantly facilitate the availability and the practical use of large air transport systems for civil security missions, to support a common European approach for the definition of such large systems while reducing theirs costs of development and of operation.

Area: 10.7.6 Training

[30] Policy related action: the management of the grant agreement will *not* be externalised to the REA.

Topic SEC-2011.7.6-1 Development of a European training curriculum for international crisis management

Description of the topic:
The action aims at developing European training curricula for professional crisis response actors like first responders and strategic crisis managers confronted to a large scale crisis such as (large) natural disasters, humanitarian crisis (e.g. displaced populations), conflict prevention, mediation or security sector reform.

- Development of a set of European standards, concepts, methods and doctrines
- networking of existing training institutes

The European dimension and the involvement of concerned public authorities, international organisations (e.g. UN) and NGOs are essential. It is important to take into account existing initiatives, and, if possible, involve a wide range of stakeholders.

Funding schemes: Collaborative Project (small or medium-scale focused research project) or Coordination and Support Action

Expected impact: Improved the preparation and the availability of trained personal facilitate coordination and effective management of large crisis.

III IMPLEMENTATION OF SECURITY RESEARCH CALL 4

- Call identifier: FP7-SEC-2011-1
- Date of publication: 20 July 2010[31]
- Deadline: 2 December 2010 at 17.00.00, Brussels local time[32]
- Indicative budget: Total call budget **EUR 221.43 million**[33]
  - An indicative **45%** (deviation possible from 35% to 55%) of the budget for topics to be implemented through **Integration Projects** (Topics 1.3-3, 2.2-1, 2.4-1, 3.4-1, 4.1-1, 4.2-2 and 4.2-3).
  - An indicative **55%** (deviation possible from 45% to 65%) of the budget for the other topics.
  - Within the above indicative limits, up to 3% can be used for *international co-operation*, and up to 3% can be used for *ERA-NET*.
  - The final total budget awarded to this call, following the evaluation of proposals, may vary by up to 10% of the total value of the call.
- **Topics called:**

Activity/ Area	**Topics called**	**Funding Schemes**
Activity: 10.1 Increasing the Security of the Citizens		
Area: 10.1.1 Organised crime	SEC-2011.1.1-1 Digital forensic - Capability Project	CP-FP
Area: 10.1.2 Intelligence against terrorism	SEC-2011.1.2-1 Strategies for countering a terrorist attack in an urban environment – Capability Project	CP-FP
Area: 10.1.3 Explosives	SEC-2011.1.3-1 Improvised Explosive Device (IED) neutralisation in urban / civil environment - Capability Project	CP-FP
	SEC-2011.1.3-2 Forensic analysis of an explosion or an unexploded IED- Capability Project	
	SEC-2011.1.3-3 Comprehensive toolbox for humanitarian clearing of large civil areas from anti-personal landmines and cluster munitions - Integration Project	CP-IP
Area: 10.1.4 Ordinary Crime and Forensic	SEC-2011.1.4-1 Understanding of unintended consequences of global illicit-drug control measures – Capability Project	CP-FP
	SEC-2011.1.4-2 Innovative techniques for safe external control of non cooperative vehicles – Capability Project	
	SEC-2011.1.4-3 Advanced forensic framework - Coordination and Support Action	Coordination and Support Action
Area: 10.1.5 CBRN Protection	SEC-2011.1.5-1 Development of detection capabilities of difficult to detect radioactive sources and nuclear materials - Capability Project	CP-FP

[31] The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication.
[32] The Director-General responsible may delay this deadline by up to two months.
[33] Under the condition that the draft budget for 2011 is adopted without modifications by the budget authority.

	SEC-2011.1.5-2 Identification and Development of low-risk alternatives to high-risk chemicals – Capability Project or Support Action	CP-FP and Support Action
	SEC-2011.1.5-3 Development of improved forensic tools applied to radiological contaminations – Capability Project	CP-FP
Activity: 10.2 Increasing the Security of infrastructures and utilities		
Area: 10.2.1 Design, planning of buildings and urban areas	none	
Area: 10.2.2 Energy, Transport, communication grids	SEC-2011.2.2-1 Airport checkpoints - Integration Project	CP-IP
	SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic Attacks - Capability Project	CP-FP
Area: 10.2.3 Surveillance	none	
Area: 10.2.4 Supply chain	SEC-2011.2.4-1 International postal supply chains - Integration Project	CP-IP
Area: 10.2.5 Cyber crime	SEC-2011.2.5-1 Cyber attacks against critical infrastructures - Capability Project	CP-FP
Activity: 10.3 Intelligent surveillance and enhancing border security		
Area: 10.3.1 Sea borders	none	
Area: 10.3.2 Land borders	none	
Area: 10.3.3 Air borders	none	
Area: 10.3.4 Border checks	SEC-2011.3.4-1 Security of biometric data and travel documents – Integration Project	CP-IP
	SEC-2011.3.4-2 “Artificial sniffer”- Capability Project	CP-FP
	SEC-2011.3.4-3 Border crossing points of the future - Capability Project	
Area: 10.3.5 Border intelligent surveillance	none	
Activity: 10.4 Restoring security and safety in case of crisis		
Area: 10.4.1 Preparedness, prevention, mitigation and planning	SEC-2011.4.1-1 Crisis management modelling tool - Integration Project	CP-IP
	SEC-2011.4.1-2 Psycho social support of Crisis Management – Capability Project	CP-FP
Area: 10.4.2 Response	SEC-2011.4.2-1 Post crisis lesson learned exercise – Capability Project or Coordination and Support Action	CP-FP or Coordination and Support Action
	SEC-2011.4.2-2 Unmanned search and rescue solutions – Integration Project	CP-IP
	SEC-2011.4.2-3 Rapid deployment of shelters, facilities and medical care resources following a major disaster - Integration Project	
	SEC-2011.4.2-4 Enhancing crisis response abilities of the public – Coordination and Support Action	Coordination and Support Action
Area: 10.4.3 Recovery	none	
Area: 10.4.4 CBRN response	SEC-2011.4.4-1 CBRN individual Protective Clothing - Capability Project	CP-FP
Activity: 10.5 Improving security systems integration, interconnectivity and interoperability		
Area: 10.5.1	SEC-2011.5.1-1 Evaluation of identification	CP-FP or Coordination

Information Management	technologies, including Biometrics	and Support Action
Area: 10.5.2 Secure Communications	SEC-2011.5.2-1 Technical solutions for interoperability between first responder communication systems - Capability Project	CP-FP
Area: 10.5.3 Interoperability	SEC-2011.5.3-1 Establishment of a first responders Platform for interoperability	Coordination and Support Action
	SEC-2011.5.3-2 Operational data exchange	CP-FP or Coordination and Support Action
	SEC-2011.5.3-3 Developing interoperability frameworks for mission-oriented security systems	CP-FP or Coordination and Support Action
	SEC-2011.5.3-4 Video archive search - Capability Project	CP-FP
Area: 10.5.4 Standardisation	SEC-2011.5.4-1 Towards standardisation of CBRN detection and identification	Coordination and Support Action
Activity: 10.6 Security and society		
Area: 10.6.1 Citizens, media and security	SEC-2011.6.1-1 Analysis of the security systems in Europe	Coordination and Support Action
	SEC-2011.6.1-2 Protection of European citizens abroad	Coordination and Support Action
	SEC-2011.6.1-3 Signs of 'early warning' to detect trends and weak signals in social polarisation, violent radicalisation development and segregation	CP-FP or Coordination and Support Action
	SEC-2011.6.1-4 Reduction of the cognitive biases in intelligence analysis	
	SEC-2011.6.1-5 Surveillance and the challenges for the security of the citizen **(topic coordinated with the SSH theme)**[34]	
Area: 10.6.2 Organisational structure and cultures of public users	SEC-2011.6.2-1 Best practices for enhancing security policy in urban zones	CP-FP or Coordination and Support Action
Area: 10.6.3 Foresight, scenarios and security as an evolving concept	SEC-2011.6.3-1 Assessing trends and threats in a society	CP-FP or Coordination and Support Action
Area: 10.6.4 Security economics	SEC-2011.6.4-1 Develop socio-economic methodologies which can be adapted to different missions in security research	CP-FP or Coordination and Support Action
Area: 10.6.5 Ethics and justice	SEC-2011.6.5-1 Conflict resolution and mediation	CP-FP or Coordination and Support Action
	SEC-2011.6.5-2 The relationship between Human privacy and security	CP-FP or Coordination and Support Action
Activity: 10.7 Security research coordination and structuring		
Area: 10.7.1 ERA-Net	SEC-2011.7.1-1 Co-ordination of national research programmes in the area of Security research (ERA-NET)	Coordination and Support Action
Area: 10.7.2 Small and Medium	SEC-2011.7.2-1 Effective approach between end-users and SMEs	Coordination and Support Action

[34] The implementation of this topic is coordinated with the SSH theme. When applying for this topic, please also consult topic SSH.2011.5.1-2 Surveillance and the challenges for democracy and an open society of the 2011 SSH Work Programme.

Enterprises		
Area: 10.7.3 Studies	none	
Area: 10.7.4 Other coordination	SEC-2011.7.4-1 Networking of researchers for a high level multi-organisational and cross-border collaboration	Network of excellence
Area: 10.7.5 End users	SEC-2011.7.5-1 Innovation and research within security organisations	CP-FP or Coordination and Support Action
	SEC-2011.7.5-2 Definition of requirements by civil Security end-users for large air transport systems	CP-FP or Coordination and Support Action
Area: 10.7.6 Training	SEC-2011.7.6-1 Development of a European training curriculum for international crisis management	CP-FP or Coordination and Support Action

- **Eligibility conditions**

  The general eligibility criteria, as set out in Annex 2 to the work programme, and in the guide for applicants, apply to all topics of this call. Please note that the completeness criterion also includes that part B of the proposal shall be readable, accessible and printable.

  Only information provided in part A of the proposal will be used to determine whether the proposal is eligible with respect to budget thresholds and/or minimum number of eligible participants.

  The standard minimum number of participating legal entities for all funding schemes are used in this call, in line with the Rules for Participation and in the below format:

Funding scheme	**Minimum conditions**
Collaborative projects	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Network of Excellence	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Coordination and Support Actions (coordinating action)	At least 3 independent legal entities, each of which is established in a MS or AC, and no 2 of which are established in the same MS or AC
Coordination and Support Actions (supporting action)	At least 1 independent legal entity

Additional eligibility criterion

- The following budgetary thresholds are applied as eligibility criteria: Collaborative Projects in this work programme are divided into a) small or medium-scale focused research project (CP-FP) with requested funding of EUR 3 500 000 and below, and b) large scale integrating project (CP-IP) with EU requested funding of over EUR 3 500 000.

- Proposals containing any classified information shall be declared ineligible.

Specific Eligibility Criteria for ERA-NET proposals (topic SEC-2011.7.1-1)

The aim of ERA-NET actions is to network research programmes carried out at national or regional level, with a view to their mutual opening and the development and implementation of joint activities. Such programmes shall have all of the following characteristics:

- Be strategically planned (i.e. be composed of a number of research projects focused on a defined subject area or set of problems, that are scheduled to run for a set period of time and that have a co-ordinated management).

- Be carried out at national or regional level.

- Be either financed or managed directly by national or regional public bodies, or by structures (e.g. agencies) closely related to, or mandated by, public authorities.

The minimum number of participants in an ERA-NET consortium is ***3 independent legal entities*** which finance or manage publicly funded national or regional programmes***. Each of these must be established in a different Member State or Associated Country***.

Partners for ERA-NET actions eligible to satisfy the above condition are:

- Programme owners: typically national ministries/regional authorities responsible for defining, financing or managing research programmes carried out at national or regional level.
- Programme 'managers' (such as research councils or funding agencies) or other national or regional organisations that *implement* research programmes under the supervision of the programme owners.
- Programme owners (typically national ministries/regional authorities) which do not have a running or fully fledged research programme at the moment of submitting an ERA-NET proposal, but which are planning, and have committed, to set up such a programme, are also eligible if their participation is well justified and adds value to the overall programme coordination. As such, countries or regions which have less diverse research programmes (in particular new Member States and candidate Associated Countries) will find their involvement in the ERA-NET scheme greatly facilitated.

Please note that research organisations or universities which are not programme owners or managers are not eligible partners for ERA-NET actions.

In addition to the minimum number of independent legal entities mentioned above, private legal entities (e.g. charities) which manage research programmes may enter the consortium if their participation is well justified and adds value to the overall programme coordination.

Sole participants (as referred to in Article 10 of the Rules for Participation) may be eligible if the above-mentioned specific criteria for eligible ERA-NET partners are respected. A sole participant shall explicitly indicate which of its 'members' forming a sole legal entity is either a programme owner or programme manager in the proposed action and indicate for these members, the respective national/regional programmes which are at the disposal of the proposed ERA-NET action.

- **Evaluation procedure:**

The evaluation criteria and scoring scheme are set out in Annex 2 to the work programme.

Proposal page limits: Applicants must ensure that proposals conform to the page limits and layout given in the Guide for Applicants, and in the proposal part B template available through the EPSS. The Commission will instruct the experts to disregard any pages exceeding these limits. The minimum font size allowed is 11 points. The page size is A4, and all margins (top, bottom, left, right) should be at least 15 mm (not including any footers or headers).

A one-stage submission procedure will be followed.

Proposals will be evaluated in a single-step procedure.

Proposals may be evaluated remotely.

- **Indicative timetable:** This call in 2010 invites proposals to be funded in 2011. Evaluations of proposals are expected to be carried out in January/February 2011. It is expected that the grant agreement negotiations for the short listed proposals will be opened in the first half of 2011.

- **Consortia agreements** are required for *all* actions.

- **Particular requirements for participation, evaluation and implementation:**

  Classified Information

  Proposals must not contain any *classified information* (note that the proposed action itself *can* involve classified information). If classified inputs are required to carry out a proposed action or the output of the action needs to be classified, proposers have to ensure the following:
  - provide evidence of the *clearance of all relevant facilities*;
  - clarify issues such as e.g. access to classified information or export or transfer control with the National Security Authorities (NSA) of their Member States / Associated Countries, and provide evidence of the *prior agreement* of their NSAs;
  - provide a *Security Aspect Letter* (SAL), indicating the levels of classification required at deliverables/partners level.

  Absence of any of these elements may lead the Commission to decide not to proceed to negotiation of a grant agreement even if the proposal is evaluated positively. Furthermore, appropriate arrangements have to be included in the consortium agreement.

  If the proposal is evaluated positively and invited for the negotiation, a definitive version of the SAL and of the SCG will be annexed to the Description of Work and must be worked out during negotiations. Special clauses will be introduced in the Grant Agreement. National security authorities will be consulted after the evaluation and before the negotiation through their representatives in the Security Assessment ad-hoc group from the Security Programme Committee. They will have the possibility to make recommendations regarding ‘classified information’ issues to be taken into account during the negotiation.

  For projects based on proposals which did not contain SAL but that have been subject to security recommendations following the above procedure, a SAL and its SCG annex could be required during the negotiations.

Ethical Review
Proposed activities shall be carried out in compliance with fundamental ethical principles. If ethical issues, including privacy are raised, they should be addressed in the core of the proposed activity. In addition, the potential impact of the resulting technologies and activities on Fundamental Rights, ethical principles and societal values should be addressed as part of the proposed research.

Small and Medium Enterprises (SME) and end-users
Consortia are strongly encouraged to actively involve *SMEs and end users*.

Evaluation

The *evaluation criteria* (including weights and thresholds) and sub-criteria, together with the eligibility, selection and award criteria for the different funding schemes are set out in Annex 2 to this work programme.

Coordinators of all integration project proposals and of all demonstration projects (phase II) proposals that pass all the evaluation thresholds may be invited to a *hearing*.

As a result of the evaluation, a ranked list of proposals retained for funding will be drawn up as well as a reserve list of proposals that may be funded in case budget becomes available during negotiations.

Positively evaluated proposals involving sensitive and classified information, those involving international co-operation as well as those collaborative projects where 75% funding for all participants is foreseen will be flagged to the members of the *Security Programme Committee* configuration and dealt with according to its Rules for Procedure.

- The **forms of grants and maximum reimbursement rates** which will be offered are specified in Annex 3 to the Cooperation work programme.

  Proposers claiming that their proposal should receive EU funding for research activities up to 75% for specific reasons as described on page 8 of this document should demonstrate in the proposal that the exceptional required conditions apply.

  In accordance with Annex 3 to this work programme, this call provides for the possibility to use **flat rates to cover subsistence costs** incurred by beneficiaries during travel carried out within grants for indirect actions. For further information, see the relevant Guides for Applicants for this call. The applicable flat rates are available at the following website: http://cordis.europa.eu/fp7/find-doc_en.html under 'Guidance documents/Flat rates for daily allowances'.

IV OTHER ACTIONS[35]

In addition to the above schemes and call for proposals, the following actions will be supported by:

– **Call for tender[36] [37] : Electronic tools allowing the secured exchange of EU RESTREINT classified information**

Exchange due to the possibility of managing classified reports in the context of a given project, there is a need for tools that could allow exchange of EU RESTREINT information via stand e-mail tools. The European Commission is willing to support the EU accreditation process of such a tool, which could be an existing one or a newly developed for this particular use. Open source solutions are welcome.

Indicative Budget: up to EUR 1 000 000.

Funding scheme: Coordination and Support Action - public procurement

Expected Impact: Facilitate the management of EU RESTREINT research projects

– **Call for tender[38] [39] : Pre-commercial procurement and innovative aspects of public procurement, possibilities to enhance European competitiveness in the field of security**

The step between research and the commercialization of its results is not always easily achieved due to different reasons. The main activity in this topic would be the study of the advantages and possibilities of the pre-commercial procurement in the countries where these procedures are already taking place. Thereafter, the effective establishment of these procedures should be analysed in the EU framework. New and innovative aspects of public procurement and the mechanisms to set it out should be proposed and analysed thoroughly. Possible areas where this kind of procurement could take place should be proposed and justified.

Indicative Budget: up to EUR 1 000 000.

Funding scheme: Coordination and Support Action - public procurement

Expected impact: Improvement of the efficiency in the commercial availability of research results. Facilitate the accessibility of research results as commercial products. Improve the

[35] In accordance with Articles 14, 17 and 27 of Regulation (EC) No 1906/2006 of 18 December 2006 laying down the rules for the participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013).
[36] Call for tender can also be attributed via a framework contract.
[37] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.
[38] Call for tender can also be attributed via a framework contract.
[39] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.

public procurement procedures which new ideas and pave the way to set standards in public procurement.

– **Call for tender[40] [41] : Mapping and monitoring of security R&D capabilities in Europe**

This action aims at mapping and monitoring security R&D capabilities in Europe, including the assessment of the European "level of ambition" with regards to future R&D

In comparison with other security-relevant areas like e.g. the assessment of the EU security market and the competitiveness of its security industry or the mentioned specific activities dedicated to critical infrastructures and technologies, the knowledge of the overall situation in the European security R&D landscape is rather poor.

Any future, holistic R&D strategy development, particularly public R&D strategies, will depend also on a comprehensive and up to date overview of the existing R&D capabilities, indicating potential investment needs where capabilities are missing or not sufficient.

While a lot of efforts are already made in the EU and its Members States in the area of critical infrastructures definition, protection and identification of related research needs, and, newly, in the field of critical and emerging technologies' identification and assessment, it becomes evident that the available security R&D capabilities in Europe itself (industry, research and academia, including their R&D infrastructures) comprise potential criticality, which need to be understood.

An assessment of those R&D capabilities in Europe is essential with regard to the future "level of ambition" Europe might want to have in security R&D, i.e. where R&D capabilities allow

- for the development and integration of security systems and even beyond (system-of-systems),
- for R&D up to component/sub-system level,
- for at least a general assessment and advice capability that would allow Europe to be a "smart customer" of foreign products, and where already critical dependencies on foreign R&D exist because of gaps in European security R&D capabilities.

The task in this project is to survey and to map security R&D capabilities and infrastructures in the EU and its Member States, public and private, including

- The development of a methodology for a mapping and monitoring of security R&D capabilities, taking into account different aspects of R&D, e.g.
  - European or national availability, public or private,
  - Potential criticality and how to measure it (capacity of R&D, R&D infrastructure, dealing with critical or emerging technologies, etc.),
  - Current R&D level (general assessment and advice capability, component/sub-system capability, system/system-of-systems capability);
- Comprehensive mapping of existing security R&D capabilities (public and private), based on the developed methodology,
  - Including the European level and the 27 EU Member States,
  - Including relevant (dual-use) defence R&D capabilities,

[40] Call for tender can also be attributed via a framework contract.

[41] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.

- Integrating potentially other, related mapping and monitoring activities, e.g. in FP7 Capacities programme "Research Infrastructures" or in the defence sector,
- Including the development of a process and implementation plan for the continued monitoring of existing security R&D capabilities;

- Awareness raising and dissemination of project results, focused on public and private R&D strategy developers to be identified on European level and in the 27 EU Member States.

Indicative Budget: up to EUR 1 000 000.

Funding scheme: Coordination and Support Action - public procurement

Expected impact:

- Achieving Europe wide awareness of the importance and potential criticality of indigenous security R&D capabilities,
- Providing a unique, comprehensive overview of existing security R&D capabilities in Europe for an improved policy support to R&D strategy development in the EU and its Member States,
- Providing recommendations for the management of critical R&D capabilities (e.g. potential subsidisation of R&D capabilities, risk assessment and management of dependencies, Security of Supply etc.).

– **'Support to the Polish Presidency European Security Research Conference – SRC'11'**[42]

The Polish presidency will host the "European Security Research Conference – SRC'11". The objective is to support the conference, which aims at disseminating information on activities of FP7 Security Research (including information seminars, audiovisual aids, exhibitions, competitions, etc and bringing together the main European players of research and development in the field of security.

The named beneficiary for the grant is:
PIAP - PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW
202 ALEJE JEROZOLIMSKIE
02 486 – Warsaw
Poland

The maximum EU requested contribution is limited to EUR 220 000 and will not represent more than 50% of the total cost of the conference.

The EU contribution will be implemented as a grant to the named beneficiary. It will be evaluated in accordance with the standard FP7 evaluation criteria (including weight and thresholds) and sub-criteria, together with an eligibility, selection and award criteria for the funding scheme as set out in Annex 2 to this work programme.

Funding scheme: Coordination and Support Action – grant to a named beneficiary

[42] Policy related action: the management of any resulting contract(s) will *not* be externalised to the REA.

Expected impact: Support the dissemination of the FP7 Security theme activities; Enable debate and provide political guidance for Security research programmes; Facilitate the dialogue within the Security community (supply side, user side, security authorities…).

- The use of appointed **independent experts** for the evaluation of proposals, and as independent observers at these evaluation, and where appropriate, for the reviewing of running projects.

Indicative Budget: up to EUR 1 300 000.

Funding scheme: Coordination and Support Action - expert appointment letters

- **Support to workshops, conferences, communications activities or studies**

Funding scheme: Coordination and Support Action
Indicative Budget: up to EUR 1 000 000.

V BUDGET

Indicative budget allocation for the Security Work Programme 2011

A total of EUR 229.54 million[43] is to be committed from the 2011 budget. The indicative budget allocation is given in the below table. More information will be provided on http://cordis.europa.eu/fp7/calls/.

Call/activity	2011 EUR million
Call FP7-SEC-2011-1	**221.43**
General Activities (cf. Annex 4)	**2.59**
Other Activities: • Expert Evaluators (EUR 1.3 million) • Calls for tender (EUR 3.0 million) • Support to workshops, communication activities, studies, etc (EUR 1.0 million) • Support to SRC'11 (EUR 0.22 million)	**5.52**
Estimated total budget allocation	**229.54**

Summary of budget allocation to general activities for 2011 in million EUR (cf. Annex 4)

Cordis	0.40[44]
Eureka / Research Organisations	0.02
COST	2.12
Strategical oriented support action	0.03
Cooperation with non-University Research Performing Organisations	0.01
Experts (horizontal activities)	0.01

[43] Under the condition that the drat budget for 2011 is adopted without modifications by the budget authority.
[44] This amount is reserved to support the CORDIS activities in 2011. The exact content of the CORDIS activities in 2011 will be specified through an update of Annex 4 to the Cooperation work programme at a later stage.

Total	**2.59**

All budgetary figures given in this work programme are indicative. The final budgets awarded to actions implemented through calls for proposals may vary by up to 10% of the total value of the indicated budget for each call.

For actions not implemented through calls for proposals:

- The final budgets for evaluation, monitoring and review may vary by up to 20% of the indicated budgets for these actions;
- The final budget awarded for all other actions not implemented through calls for proposals may vary by up to 10% of the indicated budget for these actions.

VI Indicative priorities for future calls

Indicative Roadmap of future calls

Security Call 5 (FP7-SEC-2012-1) – open 2nd half of 2011
Security Call 6 (FP7-SEC-2013-1) – open 2nd half of 2012

Indicative approach of future calls:

Security Call 5:

Demonstration project(s) phase II for CBRNE
Demonstration project(s) phase II for Security of Supply chains and logistic
Countering weapons trafficking
Automatic treatment of (large amount of) images and videos
Tools to facilitate intelligence and information sharing for law enforcement agencies
ERA-NET for national security research programme (could be focused on specific areas)
Detection of explosives/IEDs in a civil environment
Early detection of a CBRN event or a significant health threat (e.g. pandemic)
Protective clothing and equipment (e.g. bullet proof jacket)
Air Traffic Management Security

Security Call 6:

Demonstration project(s) phase II for Crisis Management
Advanced Forensic toolbox
Integrated deployable Command and Control centre incl. decision support, fusion of data from observation, intelligence, communication.
Stand-off detection of biological agents