WORK PROGRAMME 2009

COOPERATION

THEME 10

SECURITY

(European Commission C(2008)4598 of 28 August 2008)

This work programme includes all activities using the budget of 2009, but does not replace the work programme relating to 2007 and 2008 budget budgetary commitments.

THEME 10: SECURITY

Table of contents

THEME 10: SECURITY

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 acts of terrorist acts and (organised) crime, natural disasters and industrial accidents while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security; to stimulate the co-operation of providers and users for civil security solutions; to improve the competitiveness of the European security industry and to deliver mission-oriented 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], for creating an EU-wide area of justice, freedom and security[2], and to policy areas such as transport[3], health[4], civil protection[5], energy[6] and environment[7]. Through this, the Security theme also contributes to growth and employment in general, innovation and the competitiveness of European industry.

The respect of privacy and civil liberties is a guiding principle throughout the theme.

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 Community 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 actions under the Security theme are oriented towards new methodologies and technologies.

Approach for 2009

[1] *http://ec.europa.eu/comm/external_relations/reform/intro/ip04_1151.htm; http://ec.europa.eu/comm/external_relations/cfsp/intro/index.htm;*
[2] *http://ec.europa.eu/justice_home/fsj/intro/fsj_intro_en.htm;*
[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://ec.europa.eu/dgs/environment/index_en.htm;*

Following the recommendations of the Commission's *European Security Research Advisory Board (ESRAB)*[8], 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** – ESRAB identified 120 capabilities organised in 11 **functional groups**[9] - of the persons and organisations responsible 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, can be 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

[8] *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.*

[9] *For complete list of functions see chapter IV of the ESRAB report.*

The Security theme aims at **meeting its main objectives** – improved security for the citizens, and enhanced competitiveness for industry - **as substantiated in the topics of its 'demonstration projects' which will be the 'flagships' of the Security theme.** 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.

Technology oriented 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):

- On the top level of the building block structure, **demonstration projects** 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 projects will be implemented in two phases:

  Phase 1 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 7th Framework Programme or for the national level.
  Duration: 1 – 1.5 years
  Funding scheme: Coordination and support actions

  Phase 2 will then technically implement the system of systems demonstration projects, taking already into account steps which have to follow the research like standardisation, development of marketable products and procurement. This will mobilise a significant volume of resources.
  Duration (typical): up to 4 years
  Funding scheme: Collaborative projects

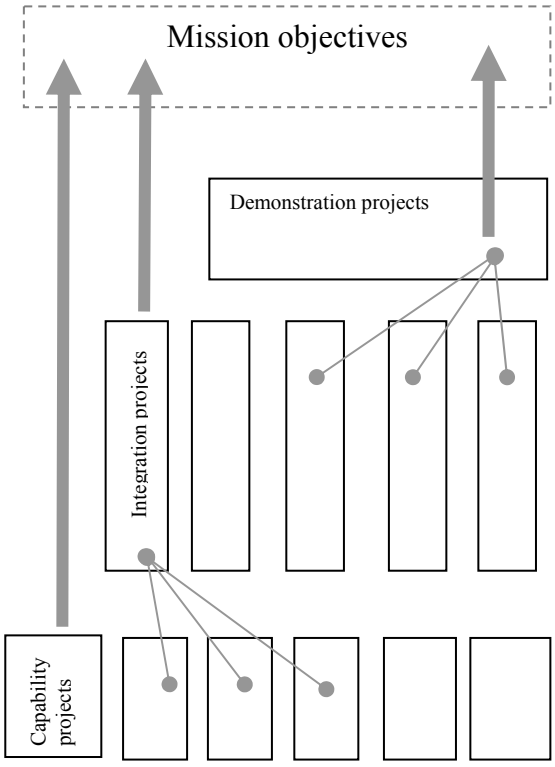

Figure 1: Research routes to meet the Security theme objectives

- 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. They depend upon technology and knowledge building blocks carried out within capability projects or elsewhere.
  Average duration: 4 years
  Funding scheme: Collaborative projects

- 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.
  Average duration: 2-4 years
  Funding scheme: Collaborative projects

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, and society relevant research issues can also be integrated in technology projects. The Security theme should also support the (re)structuring of the European security sector. Thus the following funding schemes are envisaged in 2009:

- For activity 6. *Security and society*, collaborative projects, networks of excellence and coordination and support actions can be chosen as funding schemes.

- For activity 7. *Security Research coordination and structuring*, the funding schemes will be networks of excellence and coordination and support actions. 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.

The **Networks of excellence** scheme aim at research organisations 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', and with a view of creating in this field a European 'virtual centre of research'.

The funding scheme **Collaborative project** will, in the Security Research Call 2, be divided into integration projects (large-scale integrating projects, with indicative Community funding of over EUR 3 500 000), and capability projects (small and medium-scale projects, with indicative Community funding of EUR 3 500 000 and below).

Concerning the **collaborative project** funding scheme in the Security theme, the Community funding may reach a **maximum of 75%** in cases with very **limited market size** and a risk of "market failure" and for **accelerated equipment development** in response to new threats.[10] To claim this higher funding level, proposers need to demonstrate in their proposal that the required conditions apply. The final decision will be based on the recommendations of the relevant evaluation panel.

[10] *Decision 1906/2006/EC of 18/12/2006 on the rules for participation, Art 33.1*

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. The performance and integration of SMEs is furthermore supported through dedicated measures, in particular in topic SEC-2009.7.0.2.

- International Cooperation

All actions of the Security theme are open to **international co-operation** to Industrialised countries as well as to ICPC[11] countries. At this stage, it is not foreseen to have any 'specific international co-operation actions' in the Security theme.

- Dissemination actions

In general, particular networks of security research stakeholders (including both the supply and the user side) are seen as instrumental in promoting the **dissemination** of security research to its end users, national public authorities and citizens alike. Suitable Coordination and support actions to achieve this could also receive funding (see in particular topics in activity 7).

- 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 other 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 consortia is considered of utmost importance.

Security theme actions should be multidisciplinary and mission-oriented. A multi-purpose nature of technologies is encouraged to maximise the scope for their application, and to foster cross-fertilisation and take-up of existing and emerging technologies for the civil security sector. Security research can cover areas of **dual use** technology relevant to both civilian and military applications. Therefore, appropriate coordination mechanisms are envisaged 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 themes of the 7th Framework Programme or

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

of national research programmes. Only issues of **European added value** are covered in the theme and complementary is ensured with all other Community actions. Complementarity with non-EU research will be ensured via the members of the Security Programme Committee configuration.

Due to the sensitivity of the Security theme, the *Rules for participation*[12] foresee the possibility of restrictions to the dissemination of the outcome of the actions on a case by case basis. Special provisions will be taken in the grant agreement.

For the Security Research Call 2, 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 needs to be classified or classified inputs are required. In this case proposers have to ensure *and provide evidence* of the clearance of all relevant persons and 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 *security aspect letter,* indicating the levels of classification required. Appropriate arrangements have to be included in the consortium agreement.

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.

Ethical principles and **gender aspects** in planning, decisions, and funding must always be taken into account. In technological proposals, ethical principles will also concern questions of privacy. 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. Therefore, a balanced representation of women and men at all levels in research projects is encouraged, including in evaluation groups,etc..

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 7th 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) that 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. The Security Research Call 2 offers the possibility to submit a dedicated ERA-NET proposal under topic *SEC-2009.7.0.1 Transparency and networking amongst Member States and Associated Countries.*

[12] *COM(2005)705; Article 22*

II CONTENT OF THE CALL IN 2008

II.1 Security Research Call 2 (FP7-SEC-2009-1)[13]

The primary ambition of the Security theme is to provide enhanced security related technologies, systems and systems of systems and to facilitate their take-up for the implementation of security policies and programmes as soon as possible.

The Security Research Call 2 will include important topics that were not covered sufficiently well in the first Call FP7-SEC-2007-1, and topics that have already been indicated in the first Work programme 2007 as priorities for the Security Research Call 2. The latter will include the phase 1 of three more demonstration programmes in the two security policy missions *Security of citizens* and *Restoring security and safety in case of crisis.* These will demonstrate integrated innovative systems of systems.

In parallel, and supporting this focus from the other building block levels, novel and improved technologies will also be developed, adapted and integrated into systems to be ready for the next generation of integrated security systems of systems to be demonstrated for full scale take-up in the future.

Topic descriptions in this Call are often deliberately kept rather brief and general in order to allow for a variety of promising technological approaches which may address more than one *specific* security application. This ensures that in principle **more than one proposal can be selected for each topic**, thus guaranteeing **competition amongst proposals**. It is also possible *not* to select any proposals submitted to a topic at all, if the quality is not sufficient and evaluators do not recommend it.

The Security Research Call 2 is open to the submission of proposals for actions referring to the following topics.

Activity 10.1: Increasing the *Security of citizens*

The challenge of this activity is to contribute to increasing the logistic and supply chain security, to combating the activities of organised crime (such as drug and weapons smuggling, complicated money laundering and child pornography trafficking schemes, individual and private sector fraud, illegal movement of equipment, technology and knowledge etc.) and terrorism by developing secure information and financial networks, robust secure communications and virtual policing of information infrastructures, including the internet, information assurance related to internet as a tool, to uncover and track terrorist activities; to enhance the intelligence and analysis capabilities (capacity and quality) across a range of sectors in concert with digital forensic technology to track, trace and apprehend terrorists;

[13] Projects that are not identified as either security sensitive or of a strategic nature are likely to be implemented via the Research Executive Agency.

with respect to terrorist weapons to detect, track, trace, identify and neutralise CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives) – both 'traditional' and 'home grown'. Speed, robustness and affordability will be the driving design parameters for technological and system solutions.

Area 10.1.1: Demonstration projects

The Security Research Call 2 calls for the *first phase* of these demonstration programmes, which will define their strategic roadmap and ensure Europe wide awareness.

Topic SEC-2009.1.1.1 Logistic and supply chain security (phase 1)

.

The scope and technical content of the full demonstration project (phase 2, which will build upon phase 1) will be the demonstration of an efficient, reliable, resilient and secure network of supply chains that guarantees the security of the goods produced and transported whilst having minimal impact, in terms of cost and time, on commercial operators and enterprises.

Supply chains are the backbone to Europe's economy. They involve numerous manufacturers, logistic nodes, operators, platforms and checkpoints. Their security will require an integrated approach to risk assessment; product traceability, secure exchange of good between nations, and across operators and the fast but effective screening of goods and platforms. The programme has strong linkages to the integrated border management demonstration programme. The areas of improvement and demonstration are:

- Supply chain risk assessment systems and sector specific models to ascertain weaknesses and appropriate mitigation measures
- Product traceability systems covering manufacturing to end user
- Secure, compatible and interoperable information transfer system for shipment of goods
- Secure exchange of goods, platforms and containers between operators (intermodal transport security)
- Inspection systems for goods and packaging, including smart container solutions
- Authentication systems for goods and operators
- Modernization of customs procedures to facilitate further the free movement of individuals, operators, goods, and platforms
- Intelligence of shipped products for pre-screening; content and inventory monitoring
- Protection of supply chain infrastructure including strengthening interdependency linkages.

It should contribute to increasing the efficiency of the security mission under activity 1.

Scope of Phase 1 (open): The action will define the strategic roadmap required for the demonstration project which should take into account relevant completed, ongoing and planned work and lay out, in a coherent and clear manner, the further research work required. It will assess the relevant factual and political situation and trends as well as potential classification requirements and issues related to IPR, also with a view to procurement. It will ensure Europe wide dissemination of the preparation of the demonstration project proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the co-operation of third country participants is required or recommended.

Call: Security Research Call 2
Funding scheme: Coordination and support action (aiming at supporting research activities).

Topic SEC-2009.1.1.2 CBRNE (Chemical, Biological, Radiological, Nuclear agents and Explosives (phase 1)

The scope and technical content of the full demonstration project (phase 2, which will build upon phase 1) will be the demonstration of a consistent portfolio of counter measures for CBRNE along the chain from prevention to response and recovery. Interoperable and mobile solutions will significantly lower unit cost whilst international cooperation, and multiple domain application, offer strong multipliers for success.

CBRNE will require an integrated approach to threat assessment and consequence modelling, detection and identification of agents and devices, incident management tools, infrastructure protection mechanisms for individuals and environments, decontamination processes/techniques and medical care. Improvement and demonstration areas are**:**

- Affordable networked sensor systems for CBRNE alerting and detection;
- Rapid identification sensor equipment and systems for CBRNE and precursor chemicals
- Integrated monitoring system of CBRNE sensors combined with a monitoring system that traces and tracks people, goods and platforms.
- Development of portfolio of real time spread prediction models capable of integration into existing command and control environments
- Integration of CBRNE monitoring networks in existing sensor, transaction and distribution networks.
- Protection measures, systems and processes for infrastructure and civilian populations.
- Decontamination systems and methods applicable to civilian environments.
- The development of large scale pre- and post-incident medical care.

Scope of Phase 1 (open): The action will define the strategic roadmap required for the demonstration project which should take into account relevant completed, ongoing and planned work and lay out, in a coherent and clear manner, the further research work required. It will assess the relevant factual and political situation and trends as well as potential classification requirements and issues related to IPR, also with a view to procurement. It will ensure Europe wide dissemination of the preparation of the demonstration project proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the co-operation of third country participants is required or recommended.

Call: Security Research Call 2
Funding scheme: Coordination and support action (aiming at supporting research activities).

Expected impact**:** *Through comprehensive preparation (not proposal preparation) of the demonstration project, the action will provide a solid basis for the description of its phase 2 in the Work Programme of Security Research Call 4 in 2010 as well as for sequencing and describing research tasks to be called for in future security Work Programmes. It will achieve qualified Europe wide awareness of relevant industries (including SMEs), universities and research establishments of the upcoming demonstration project identifying key players and performance profiles of other required contributors, allowing for their effective and balanced*

access to the action. It will also achieve qualified Europe wide awareness of relevant end users, governments and other bodies, facilitating and providing guidance concerning the real-life implementation of the system of systems to be demonstrated.

Area 10.1.2: Integration projects

The Security Research Call 2 calls for the following actions:

Topic SEC-2009.1.2.1: Information and knowledge management for the prevention of terrorist acts and organised crime

The task is to create a large system, using different modules integrated within an open architecture. These modules will address all the stages of the value chain of information management for the fight against and terrorist acts and organised crime (smuggling, trafficking, fraud, etc.):

a) **Information Acquisition** should use the means for all data-format (multilingual text and speech, image…) and sources (open source, disparate high volumes data repositories, network flows…) to be collected and adequately stored and controlled;
b) **Information Processing** should comprise all levels of data extraction, transformation, mining, etc.;
c) **Information Exploitation** should correlate real-time and historical data to allow automatic and under-demand (hypothesis building) analysis and decision-making, as well as support for the coordination of law enforcement actions.
Integration, interoperability, scalability and intrinsic security are to be key elements of this system.

***Expected Impact*:** Current tools for the fight against terrorist acts and organised crime include information technology systems, typically ad-hoc for each law enforcement agency, that are somehow capable to generate added value from disperse data by means of correlation, comparison and tracking. The importance of these systems reside on their ability to provide evidence and warnings on facts that otherwise would not be detected during investigations; at the same time they can provide co-ordination for different agencies tackling same or similar actions or suspicious events/people. However, considering the wide scope of potential parameters and variables to be taken into account, several limitations apply: sources or information are too wide and format (written, oral, digital, analogue…) and language dependant; legal aspects regarding the information to be used or the persons to which it relates (privacy); interoperability of systems; information sharing and security aspects of the systems and of the information itself; trans-national considerations; etc.
Through this action it is intended to tackle the availability of the widest range of information types and sources, data extraction and transformation tools and processes for knowledge management against terrorist acts and crime. At the same time it should demonstrate the possibility of integrating them in a larger system, where each agency is determined by modules and secured information handling is at the core of the system.

Call: Security Research Call 2
Funding scheme: Collaborative project

Area 10.1.3: Capability projects

The Security Research Call 2 calls for the following actions:

Function: Detection, identification & authentication

Topic SEC-2009.1.3.1: B-detection. Very fast alerting on broad substance type and identification. Low false alarm rates.

Technical content / scope: Detecting and identifying specific dangerous goods are important capabilities for the protection against terrorist acts. The task is to develop new capabilities for the on the field detection and identification of viri and B-agents in the air, indoor and/or outdoor environments. Rapid alerting should facilitate early warning and false alarm rates of existing sensors should be reduced. Stand off capability, portability (miniaturisation, autonomy…) and maintenance issues will allow ease of use. Networkability and affordability of detectors have to be considered.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Topic SEC-2009.1.3.2: Drug precursors

Technical content / scope: In order to limit the import of chemicals for the production of narcotics and psychotropic substances new types of reliable, portable/deployable, low-cost and 'easy to operate' sensor systems are needed. These sensors are envisaged to be used primarily by customs officers for controls at the EU external frontier and law enforcement for intra-Community checks.
Analysis should thus be simple, fast, hand-held and preferably non-invasive. Projects should develop prototypes for the detection of key chemicals (drugs, drug precursors and potentially derivatives of key precursors) used in the production of narcotics related criminality, such as Amphetamine-type-stimulants (ATS), in Europe. Ideally multiple substances could be detected simultaneously.
The systems to be developed should be fully functional ranging from sampling to read-out. In order to guarantee high specificity, high sensitivity and a minimized amount of false positive signals, the systems could integrate several independent advanced sensor technologies.

There is also a need for systems which allow for high throughput during initial screening where e.g. optical probing and technologies to analyse airborne traces of the specific chemicals can be employed.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Topic SEC-2009.1.3.3 Properties of improvised explosive devices, additives to precursors to explosives to prevent precursors from being used to manufacture explosive devices

Technical content / scope:

Properties of improvised explosive devices (in particular liquid explosives) regarding in particular additives to precursors to explosives, either to prevent them from being used to manufacture improvised explosive devices *(inhibitors)*, or to allow an easier detection *(markers)*.

Call: Security Research Call 2
Funding scheme(s): Collaborative project.

Topic SEC-2009.1.3.4: Advanced forensic toolbox

Technical content / scope: The task is to develop:

1) A methodology and technological standard for the reconstruction of physical [and/or digital] crime scenes with the aim to improve interpretation and presentation in all stages of the legal process: from police briefing, case conferences through expert testimony in court in all EU member states and associated states. This includes the development of tools for recording of crime scenes, scenario-driven evidence collection and decision making.

2) Mobile technologies for 'real time' analysis and screening of trace materials (DNA, CBRN, explosives, drugs) at large scale crime scenes and mass disasters caused by terrorist incidents. This technology is aimed at quickly retrieving information that is needed to enable scenario based evidence selection, information guided investigation, risk assessment and to enable decontamination of terrorist incident scenes in such a way that disruption of trace evidence is prevented.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Expected impact**:** *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

Activity 10.2: Increasing the *Security of infrastructures and utilities*

The challenge of this activity is to protect critical infrastructures and utilities (both physical and logical systems from e.g. sensitive and administrative buildings (often also of symbolic value), train and subway stations, dams, sensitive manufacturing plants, energy production

sites, storage and distribution, storage sites of nuclear waste, to information and communication networks or public events etc.) against being damaged, destroyed or disrupted by deliberate acts of terrorism, sabotage, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. Their direct, often trans-national dependencies and the cascading failures generated in case of failure in one of them (special emphasis is given to the robustness of the power transmission and distribution system due to its underlying operational importance to most others) will be taken into account, as well as the consequential dependencies to the commercial environment. Cost effectiveness will be addressed as one of the driving design parameters. Efficient technological solutions need to be developed. Where no efficient solution exists, the research effort should emphasise low cost solutions; where efficient but costly technologies exist, research efforts should focus on ways to reduce dramatically the cost for similar performances.

Area 10.2.1: Demonstration projects

No demonstration projects are foreseen in this activity for the Security Research Call 2.

Area 10.2.2: Integration projects

The Security Research Call 2 calls for the following actions:

Topic SEC-2009.2.2.1: Integrated protection of rail transportation

Technical content / scope: The task is to develop an integrated system to improve the security of rail transportation through better protection of railways and trains, and to reduce disparity in security between European railway systems. This will include the immunity of signal and power distribution systems against electromagnetic terrorist acts, the detection of abnormal objects on or under ballast; clearance of trains before daily use; control of access to driver's cabin, detection of unauthorised driver; new methods/tools to isolate and secure luggage; as well as a study and tools to reduce disparity of European railway systems' security. The action will demonstrate the potential of the European rail transportation systems for improved protection and homogeneity. This will also include the physical protection of railway assets (train, railway system and- underground-station buildings etc).

Call: Security Research Call 2
Funding scheme: Collaborative project.

Topic SEC-200.;2.2.2: Integrated comprehensive approach to airport security

Technical content / scope: The task is to create an integrated comprehensive airport (land, surrounding infrastructure and adjacent airspace) security system capable of providing accurate situational awareness. It aims to develop a cost and time effective system with a passenger security focus that covers the whole airport area and integrates relevant technologies that together can meet current and coming security threats. The proposed system must respect passenger privacy and keep time spent at check-in, security controls etc to a minimum. Aspects to be addressed include passenger, crew and staff screening (including detection of non-metallic weapons, explosives, drugs, etc); passenger area surveillance

(abnormal behaviour, illicit substances and objects); outdoor 24h surveillance at the airport area; and checked luggage and cargo screening (including detection of explosives and other illicit substances or objects). This integrated approach could include a comprehensive threats analysis, and the research needs for the detection and the protection of commercial aircrafts against MANPAD attacks. The system will improve situation awareness at airports through the monitoring and tracking of complex transport environments as a consequence of the continuous arrival and departure of cargo, planes, vehicles, staff and passengers, and also the potential threats by vehicles and individuals inside and at the surroundings of the airport area. This will include mobile and fixed detection and recognition systems in order to provide intelligent event detection, supporting the decision control; investigation into cargos and luggage scanner outputs fused with airplane passenger and cargo list information, external risk assessment and a-priori threat knowledge which allows for automatic anomaly detection.

Call: Security Research Call 2
Funding scheme: Collaborative project.

***Expected impact*:** *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces. In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

Area 10.2.3: Capability projects

The Security Research Call 2 calls for the following actions:

Function: Detection, identification & authentication

Topic SEC-2009.2.3.1 Built infrastructure protection, including building in resilience to attack at the design stage

Technical content / scope: To identify and define the required design requirements and additional physical protection measurements to counter security threats in newly built and existing infrastructures susceptible to terrorist threat (embassies, government buildings, stations, bridges and tunnels).

- A multi-disciplinary approach integrating threat analysis, infrastructure analysis, incident analysis and protective measures analysis is needed to make the right decisions regarding a protective portfolio.
- The development and application of additional protection – compatible with other building management issues - must be made feasible.

The expected outcome would be the development of a suite of protection portfolios for new and existing building that are operationally viable, infrastructure specific and affordable."

Call: Security Research Call 2
Funding scheme: Collaborative project.

***Expected impact*:** *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

Activity 10.3: *Intelligent surveillance and* enhancing *border security*

The challenge of this activity is to address border security in the context of integrated border management ensuring legitimate trade and flow of people, thus supporting the Schengen co-operation, the efforts of national authorities and those of the European Union's external borders agency FRONTEX with respect to the convergence of information management systems, interoperability, training and cascading best practice. Actions will refer to issues relevant for all the consecutive tiers of the *European border security strategy*[14].

The Commission presented on 13.02.2008 its vision on the development of the European Union's external border management system, including concrete measures on the FRONTEX Agency and on control of maritime borders.[15]. Proposals in activity 3 are meant to be coherent with this vision and to complement other on-going activities, both at the national and international level.

The link to standardisation, regulation and legislation as well as to related testing, evaluation and certification will be crucial. The focus of this Work Programme is on illegal immigration as well as on trafficking of drugs, weapons and illicit substances. With respect to illegal immigration the objective is to develop novel, reliable and scalable solutions to efficiently identify illegal movements, whilst not unduly impeding the flow of the vast majority of

[14] *As part of the definition of the EU Border Management Strategy, see Council Conclusions of Justice Home Affairs Council of 20-22 September 2006.*
[15] http://ec.europa.eu/justice_home/news/intro/news_intro_en.htm

legitimate travellers and vehicles. Naturally, privacy and human rights will need to be taken into account. With respect to the trafficking of drugs, weapons and illicit substances such as CBRNE (Chemical, Biological, Radiological, Nuclear and Explosives) agents, the objective is to create a coordinated and integrated security system to ensure the security of goods supply chains and logistics networks, while addressing traceability, standardisation and more affordable robust solutions as well as reduction of unit cost and screening times.[16]

Area 10.3.1: Demonstration projects

No demonstration projects are foreseen in this activity for the Security Research Call 2.

Area 10-3.2: Integration projects

The Security Research Call 2 calls for the following actions:

Topic SEC-2009.3.2.1: Main port area security system

Technical content / scope: The task is to conceive and design a state-of-the art integrated surveillance / security system capable to satisfy border control constraints at main ports. The system shall take into account their organizational structure and operational modalities, including, if appropriate, sea hinterland traffic and transport-logistics relations.

The system should be adaptable to different configurations of ports and it should allow the integration of existing legacy components.

This system should combine and integrate preventive measures to protect port facilities against threats of intentional unlawful acts. It should be suitable for implementation in the complex port environment and should fit into the normal flow of operations without introducing delays.

It should provide persistent surveillance of port facilities, monitoring of goods, personnel and passengers, tracking of vessels, vehicles and containers and should be capable of alerting port security operators for activation of immediate and effective reactions.

The system will integrate, in a single security network:

- information acquisition,
- handling and exchange tools,
- consideration should also be paid to the facilitation of information sharing within and between main sea ports, and/or between sea ports and hinterland terminals and operational services, such as police or other intervention forces..

The system should be based on a sound security gaps analysis and should also include elements for the training of security operators enabling them to act whenever required minimizing the loss of lives, goods and the interruption of logistic business.

Call: Security Research Call 2

Funding scheme: Collaborative project.

[16] *Actions under this activity can take up solutions provided e.g. by GMES (see theme 9 Space) or Galileo (see theme 7 Transport (including Aeronautics)).*

Topic SEC-2009.3.2.2: Sea border surveillance system

Technical content / scope: The task is to improve sea border surveillance. Key problem areas in achieving this are:

- Networking of relevant (heterogeneous) sensors, sensor networks and other information sources. Interoperability and integration are the key elements.
- Integration and fusion of data and information from the sensors, sensor networks and other information sources

Protection of sea borders relies on accurate maritime surface pictures of vessels of all types. The priority is monitoring ship movements along extended sea borders in areas of high-traffic or with special environmental concerns.. This includes detection (identification) and tracking of small, large, non-reporting and reporting vessels. Application of both wide-area surveillance and local observation nodes is important. The sensors can be land based, vessel based, airborne (also situated on unmanned platforms), underwater or space borne. Sensor networks for sea border surveillance will typically consist of combinations of land, vessel, air, underwater and space sensors.

More specific goals are to improve:

- monitoring of vessel movements (including non-reporting vessels) on the European sea border
- confirmation of the identity of reporting vessels and detection
- vessel tracking and classification
- detection of small vessels
- detection of suspicious behaviour (e.g. deviations from expected routes)
- understanding of intentions of the vessels
- early identification of potentially threatening situations.

The outcome would be an integrated and cost-effective sea border surveillance system capable of providing accurate situational awareness including early identification of possible threats and illegal actions.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Topic SEC-2009.3.2.3 Exploitation of Open Source Information in Support of Decision Making Processes

Technical content / scope:

The task is to develop an advanced integrated toolkit to exploit open source information for decision support. The toolkit should be developed allowing the collection of all kinds of

multi-lingual and -format open source information (hard- and softcopy), that can then further be processed via entity extraction, text- and data-mining, and visualisation in support of hypothesis building and scenario development. The toolkit should allow the decision-maker to trace back the underlying information and reasoning processes on which the hypotheses were built. The toolkit should be developed around an "open" architecture, in order to allow integration with other existing or newly developed tools and interfaces as easy as possible.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Expected impact**:** *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to ethics, performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

Area 10.3.4: Coordination and support actions

Topic SEC-2009.3.4.1 Continuity, coverage, performance (incl. UAV), secure data link

Technical content / scope: The task is to develop an open architecture for the operation of unmanned air-to-ground wide area land and sea border surveillance platforms in Europe. The architecture should be based on the developing concepts and scenarios for aerial surveillance and the developing legislation for insertion of unmanned aerial systems into controlled civil airspace in Europe. The technical aspects of the open architecture should include among others, concepts for surveillance sensors, platforms (including various take-off and landing strategies), secure data up- and downlinks and platform independent ground stations to control cost and maximise efficiency and effectiveness of the operation of the unmanned aerial system. In developing the project maximum use should be demonstrated of ongoing initiatives in Europe and beyond. The nature of non-military use of UAV requires cost-efficient solutions to be found.

Call: Security Research Call 2
Funding scheme: Coordination and Support Action

Activity 10.4: *Restoring security and safety in case of crisis*

The first challenge of this activity is to ensure that governments, first responders and societies are better *prepared* prior to unpredictable catastrophic incidents using new, innovative and affordable solutions. The second challenge is to improve the tools, infrastructures, procedures and organisational frameworks to *respond and recover* more efficiently and effectively both during, and after, an incident.

Three areas are to be addressed, namely incidents caused by: (1) terrorist acts and (organised) crime, including the use of conventional explosive weapons and weapons of mass destruction and disruption (e.g. CBRNE); (2) natural disasters including pandemics; and (3) major industrial accidents or technological disasters. Many of the relevant capabilities might also be suitable for deployment in humanitarian crises.

Area 10.4.1: Demonstration projects

This Security Research Call calls for the first phase of this demonstration programme, which will define its strategic roadmap and ensure Europe wide awareness.

Topic SEC-2009.4.1.1: Aftermath crisis management (phase 1)

The scope and technical content of the full demonstration project (phase 2, which will build upon phase 1) will be the demonstration of an integrated and scalable crisis management system capable of providing comprehensive situational awareness to decision makers to ensure a timely, co-ordinated and effective response to large scale disasters both inside and outside Europe.

Large-scale incidents require a coordinated response from crisis managers and first responders from different agencies across Europe and with resources from all levels of government. A common operational picture, well trained and equipped teams, secure communications, and flexibility in planning/executing crisis management missions (man made and natural) are the underpinnings. Equipment and systems developed under CBRNE activities, in particular for decontamination, should be leveraged. Improvement and demonstration areas are:

- Interoperable secure communication systems based on software defined solutions
- Robust and scalable situational awareness systems that combine and integrate, in real time, data from different systems to improve decision making.
- Network enabled capabilities and decision support for shared command and control
- Comprehensive logistic and resource planning systems to enable a rapid response, inside and outside Europe.
- Robust, lightweight and mobile search and rescue systems for all situations
- Portfolio of solutions for interagency/international training, exercises and best practice exchange based on realistic modelling and simulation tools.
- Development and adaptation of national and international operating procedures and organisational structures to a common or interoperable crisis management system.
- Rapid post incident systems to restore basic services (energy, transport, telecoms)
- Methodology and tools for medical care,
- Fast deployment in harsh environment,

- Forecasting tools for contamination spreading,
- Containment techniques,
- Traceability of contaminated people, and
- Decontamination of equipment and infrastructures (threshold)

It should contribute to increasing the efficiency of the security mission under activity 1.

Scope of Phase 1 (open): The action will define the strategic roadmap required for the demonstration project which should take into account relevant completed, ongoing and planned work and lay out, in a coherent and clear manner, the further research work required. It will assess the relevant factual and political situation and trends as well as potential classification requirements and issues related to IPR, also with a view to procurement. It will ensure EU wide dissemination of the preparation of the demonstration project proposal to the relevant stakeholders from both the supply and user side. It will also indicate where the co-operation of third country participants is required or recommended.

Call: Security Research Call 1
Funding scheme: Coordination and support action (supporting action).

Expected impact: *Through comprehensive preparation (not proposal preparation) of the demonstration project, the action will provide a solid basis for the description of its phase 2 in the Work Programme of Security Research Call 4 in 2010 as well as for sequencing and describing research tasks to be called for in future security Work Programmes. It will achieve qualified Europe wide awareness of relevant industries (including SMEs), universities and research establishments of the upcoming demonstration project identifying key players and performance profiles of other required contributors, allowing for their effective and balanced access to the action. It will also achieve qualified Europe wide awareness of relevant end users, governments and other bodies, facilitating and providing guidance concerning the real-life implementation of the system of systems to be demonstrated.*

Area 10.4.2: Integration projects

This Security Research Call calls for the following actions:

Topic SEC-2009.4.2.1: First responder of the future

Technical content / scope: The task is to enhance the operational effectiveness and capability of first responders and reduce injury or loss of life among first responders (and the civil population).

The project should present a holistic view covering
- Operational effectiveness
- Improved logistics concepts (including cross-border) involving the different first responders (medical teams, police, fire brigades, specialised CBRN teams,..)
- Interoperability and interchangeability of equipments and systems;
- Improved availability of appropriate transport means, measures for safe hand over of casualties to hospitals;
- Optimisation of personal protection equipment, including sensors and communication means;

- Indoor communication and guidance of first responders in the field;
- Harmonisation of existing CBRN activities.
- Development of European standards for certification of equipment and personnel;
- Harmonisation of the legal framework of intervention (including cross-border aspects)
- Training under realistic conditions (and co-operation), design training for real life operations
- The required interoperability between civil first responders and special military and or intervention forces operating side by side with their civil colleagues in terrorist attack situations
- Attention to the well-being and/or resilience of the first responder

Proposals should build on projects launched in previous calls. The expected outcome would be integrated protection systems, equipment, procedures and training methods to improve the performance and security of first responders.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Expected impact**:** *While taking into account the mutual dependency of technology, organisational dynamics and human factors as well as related legal issues, actions in this area will achieve a substantial improvement with respect to performance, reliability, speed and cost. They will also identify standardisation requirements and provide information concerning further research needs with a view to future security Work Programmes.*

Through the performance of the integrated technology system, actions will allow product and service developers to verify and optimise their technologies at all development stages. This will reinforce their potential to create important market opportunities for European industry and establish leadership.

Actions will demonstrate the technology based potential for enhancing the effectiveness of European authorities in implementing their security policies and the capabilities of security forces. In addition, the actions will provide guidance for their implementation, including privacy relevant aspects.

Area 10.4.3: Capability projects

This Security Research Call calls for the following actions:

Function: Intervention and neutralisation

Topic SEC-2009.4.3.1: Neutralisation of CBRN effects following a terrorist event

Technical content / scope: In order to contain and limit the effects of terrorist CBRN (Chemical, Biological, Radiological and/or Nuclear agents) devices, the task is to develop novel, fast, wide range, mobile and easy to use counter-measure approaches to the neutralisation of devices and their effects. It should focus on the crisis management aspect after the occurrence of such an event and include techniques and systems for isolation, shielding, decontamination, medical counter-measures etc. Human factors for both responders and victims have to be considered.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Function: Incident response

Topic SEC-2009.4.3.2: Bio-dosimetric tools to manage radiological casualties

Technical content / scope: Improvement and adaptation of existing, and the development of new, bio-dosimetric tools to enable them to be applied in a timely and reliable manner to mass casualties from the malevolent use of radiation or radioactive material and to responders to such events. Speed of response and applicability to very large numbers of potentially exposed people will be critical in the use of these tools for triage. Given the diversity of potential radiological events, a range of tools is likely to be needed and an integrated approach – both in terms of hardware and software – should be developed. The tools should be validated, training provided on their use and opportunities for their commercial exploitation identified and pursued. A multi-disciplinary approach will be needed.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Function: Training & exercises

Topic SEC-2009.4.3.3: Simulation, planning and training tools and methods for management of crises and complex emergencies

Technical content/scope: The task is to address the needs for tools to help prepare for, and better manage large civil crises and complex emergencies. Complex crises and emergencies can last for long periods of time and typically involve many different organisations and regions, sometimes also with a cross-border element. Here participating organisations and nations commonly have different mandates, goals, means and methods of handling crises, which makes cooperation difficult. Therefore, there is a need to develop tools to support better planning and training of crisis management across organisational and geographic boundaries.

The goal is to develop tools and methods that:

- support information sharing and cooperative planning across organisations and nations, also dynamically in an ongoing crisis
- enable distributed training of crisis management across organisations and nations
- enable methods; models and tools exchange between organisations and nations
- include the management of "soft" aspects such as the impact of culture on crisis management across organisational and geographic boundaries.

The expected outcome would be tools and methods that help people prepare for, and better manage, complex emergencies and crises across organisations and nations.

Call: Security Research Call 2
Funding scheme: Collaborative project.

Expected impact: *Actions in this area will provide the (adapted) technology basis and relevant knowledge for security capabilities needed in this (and also other) mission(s), as required by integrating industry and/or (private and/or public) end users, while achieving a significant improvement with respect to performance, reliability, speed and cost. At the same time, actions will reflect the mutual dependency of technology, organisational dynamics, human factors, societal issues as well as related legal aspects. This will reinforce European industry's potential to create important market opportunities and establish leadership, and it will ensure sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding harmonisation and standardisation, potential classification requirements, international co-operation needs, communication strategies etc.) as well as for further research needs with a view to future security Work Programmes.*

Activity 10.5: *Improving Security systems integration, interconnectivity and interoperability*

This activity is **not open** for self-standing actions in the Security Research Call 2. However, proposals dealing with system integration, interconnectivity and interoperability issues *related to the four missions* can be submitted under activities 1, 2, 3 and 4 and will be considered 'in scope' there, as long as they are equally in line with the corresponding technical content and scope.

The Joint Call ICT & Security 1 covered self-standing actions dealing with system integration, interconnectivity and interoperability issues *related to the security of infrastructures and utilities, in particular in the domain of energy and transport.*

Activity 10.6: *Security and society*

Technology is an important tool in preventing, responding, managing and mitigating potential security threats to European societies, but it is only part of the effective response. It must be applied in balanced combination with organisational processes and human intervention, which all determine each other and must be addressed by the actions. Cultural background plays an essential role, and also in balancing security as a societal value against other values. Thus research into political, social and human issues is required to complement the technology oriented research. In this context, gender differences may exist, which must then be addressed as an integral part of the research to ensure the highest level of scientific quality. Appropriate dissemination strategies should also make an integral part of the research. Many of the activities to be funded under this theme will make positive contributions to education and training and to raising general levels of awareness of the nature of the research undertaken and the benefits likely to accrue.

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*,

Expected impact**:** *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 do* not *generate general or specific knowledge about (in-)security, its reasons and consequences etc., but attain a broad and well-based understanding of the public administrative, cultural and societal framework 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.*

The following actions will be open for **Collaborative Project, Network of Excellence and Coordination and Support Action.**

The Security Research Call 2 calls for the following actions:

Area 10.6.1: Citizens and society

The security of the European citizens is at the core of the Security theme. 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 in particular address violent radicalisation risks, terrorist behaviour and activity etc. Thus it will provide authorities as well as future technology related research with valuable information and recommendations to improve their performance.

Topic SEC-2009.6.1.1 Better understanding of the rationale and the drivers underlying the violent radicalisation processes and how these drivers interact

Technical content / scope: The task is to obtain a deeper understanding of the issues affecting violent radicalisation, the process of recruitment, and complex motivations of terrorists, which may facilitate effective counter-measures.

The knowledge on violent radicalisation processes is mainly based on superficial data (e.g.: biographical standard data like age, gender, educational background et cetera) and / or theory based assumptions. The state of knowledge is not sufficient to enlighten the driving forces of radicalization.

In order to get more in-depth insights into the psycho-social dynamics of radicalisation processes it is intended to initiate empirical research on this topic from a social-science perspective. Due to the phenomenon's complexity the research design should be multi-disciplinary and comparatively shaped and based e.g. on a life history approach (method). The research guiding question is: Do different social as well as cultural environments and conditions lead to different psycho-social patterns of violent radicalisation processes? Though, due to the recent challenges, the main focus is put on religiously motivated extremism / terrorist acts, radicalisation towards other kinds of extremism / terrorist acts

should be considered as well in order to be able to identify the specific characteristics of the diverse patterns of extremism / terrorism within Europe.

It is expected that the research findings are reflected upon in view of counter measures in terms of practicable preventive approaches to the violent radicalization phenomenon.

Call: Security Research Call 2
Funding schemes: Collaborative Project, Network of Excellence and Coordination and Support Actions.

Area 10.6.2: Understanding organisational structures 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. It will also improve applicability concerning political accountability and democratic control aspects of public services within the security arena.

Topic SEC-2009.6.2.1: Inventories of existing national resources, institutional mandates and practices across relevant sectors

Technical content / scope: The task is to address the need for general/operational interoperability, scalability and where appropriate mobility of the Member States' and Associated States' distinct national systems, in order to achieve an effective joint European capability to handle civil security issues. This will include in particular institutional design and issues concerning conflicting/complementary mandates and resources/best practices, in order to achieve better European connectivity between the existing national systems. The research should take into account behavioural, organisational and cultural issues that can have an impact on the effectiveness of public users, in particular linguistic barriers or stovepipe sectoral approaches.

The expected impact of the proposal should therefore be 1) identification of robust cultural traditions shaping local practices in the field, 2) comparison of different national and/or local structures of information processing, decision-making and allocation of resources to handle security issues, 3) identification of best practices to be implemented at a European level and 4) establishment of a platform for the monitoring and coordination of national security policies

Call: Security Research Call 2
Funding schemes: Collaborative Project, Network of Excellence and Coordination and Support Action.

Area 10-6.3: Foresight, scenarios and security as an evolving concept

The security domain is 'by definition' one with broad uncertainty even within the most near-sighted time horizon; foresight studies and scenario building techniques are therefore very much needed for all missions. 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 or preparedness and to make the appropriate trade-offs between security and other societal objectives such as the right to privacy and social cohesion.

Topic SEC-2009.6.3.1: Foresight research activities to inspire public debate, to foster shared understanding and self-organisation among stakeholders in the security domain

Technical content / scope: The task is to conduct in-depth research in areas concerning security and strongly security-related industries and markets where expertise at European level is limited. Focused foresight activities addressing specific technologies or problem areas in technology projects should also be included.

The industry's supply chain structure and relations between supply and demand sides and their effects on the national and European technological and industrial base should be taken into account, as well as trade and investment flows within the EU and vis-à-vis third countries, and emerging industrial and market issues in the next 20-year timeframe.

Call: Security Research Call 2
Funding schemes: Collaborative Project, Network of Excellence and Coordination and Support Action.

Topic SEC-2009.6.3.2 Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)

Technical content / scope: The task is to develop foresight based methodologies for the rigorous assessment of investment alternatives, intended to prevent or mitigate insecurities with uncertain and potentially catastrophic ramifications. Both financial costs as well as the trade-off between security and other societal objectives, such as the right to privacy and social cohesion, should be addressed.

Call: Security Research Call 2
Funding schemes: Collaborative project, Network of Excellence and Coordination and Support Action

Area 10-6.4: Security Economics

Security economics is the analysis of aggregate risks facing society and economy using rigorous analytical and empirical tools of economics, which should be regarded in particular with reference to the Lisbon agenda. Policy makers may tend to take imperfect security decisions (e.g. regulations) based on a public perception of (in)security, with an impact to market structures. A singular focus on security or competitiveness would be too narrow; research under this area will offer key insights that will contribute to balancing security and

the overall policy objectives. Economic theory in particular can offer key insights, enabling governments to optimise their efforts to enhance security and growth.

Topic SEC-2009.6.4.1: European Security Indicator: methodological research to provide a few select indicators of security and security policy in Europe measuring the effects of both insecurity and security policies on the economy

Technical content / scope: The task is to develop a set of indicators that together could serve as 'European Security Indicator'. Both the level of factual security as well as the security related impact of political measures should be addressed, with a view to achieving an objective reference instead of relying on (in)security as perceived by public opinion. This will include an assessment of the economic implications of both insecurity and of the implementation of security policies. It will also assess potential changes in market structures that might be initiated by regulatory measures which aim at stimulating "secure growth" and thus stimulate industries to provide security-enhancing products or services. Eventually it will take into account changes in criminality and assess crime risks.

Call: Security Research Call 2
Funding schemes: Collaborative Project, Network of Excellence and Coordination and Support Action.

Activity 10.7: *Security Research coordination and structuring*

The Security theme, which aims at contributing to increased security for Europe's citizens whilst 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.

***Expected impact*:** *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.

The Security Research Call 2 calls for the following actions:

Topic SEC.2009.7.0.1 Transparency and networking amongst Member States and Associated Countries

Technical content / scope: With a view to ensuring effectiveness and efficiency of the Security theme and also to exploit opportunities outside the Community scope, the task is to establish a Member States' and Associated countries' network of competent and politically relevant national and where appropriate regional contact points that will (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); (c) explore and demonstrate coordinated and/or joint initiatives in these core areas. The action will be similar to the principles of ERA-NET and can involve countries that already have or are about to finalise the preparation of national and/or regional security research strategies and funding programmes.

This topic is alternatively open for full scale ERA-NET proposals, to be submitted under this call[17].

Call: Security Research Call 2
Funding schemes: Network of Excellence and Coordination and Support Action.

Topic SEC-2009-10.7.0.2 Supply chains and market integration

Technical content / scope: With a view to involving the best intellectual and technological capabilities available throughout Europe in the security technology supply chains, including the yet untapped potential, and promoting their Europeanization, the task is to identify opportunities and weak spots in the supply chains, to identify appropriate organisations (in particular SMEs) not yet involved or settled in the security (research) domain, to help them understand security related targets, mechanisms and opportunities and to facilitate their access to the main stakeholders and integrators of these technology supply chains. The action needs to take into account and if possible build upon relevant ongoing initiatives.

Call: Security Research Call 2
Funding schemes: Network of Excellence and Coordination and Support Action

[17] *The Security Theme is not included in the second joint call for ERA-NETs across the Themes (See Annex IV)*

III IMPLEMENTATION OF CALLS

Call title: Security Research Call 2

- Call identifier: FP7-SEC-2009-1
- Date of publication: 3 September 2008[18]
- Deadline: 4 December 2008, at 17.00.00 h Brussels local time[19]
- Indicative budget: EUR 117.9 million [20][21]
- **Topics called**:

ACTIVITY/ AREA	TOPICS CALLED	FUNDING SCHEMES
10.1. Security of citizens */ 1.1 Demonstration projects*	*SEC-2009.1.1.1 Logistic and supply chain security*	*Coordination and support action (supporting)*
	SEC-2009.1.1.2 CBRNE (Chemical, Biologica, Radiological, Nuclear agents and Explosives)	
10.1. Security of citizens */ 1.2 Integration projects*	*SEC-2009.1.2.1 Information and knowledge management for the prevention of terrorist acts and organised crime*	*Collaborative project*
10.1. Security of citizens */ 1.3 Capability projects*	*SEC-2009;1.3.1 B-agent detection. Very fast alerting on broad substance type and identification. Low false alarm rates*	*Collaborative project*
	SEC-2009.1.3.2 Drug precursors	
	SEC-2009.1.3.3 Properties of improvised explosive devices, additives to precursors to explosives to prevent precursors from being used to manufacture explosive devices	
	SEC-2009.1.3.4 Advanced forensic toolbox	
10.2. Security of infrastructures and utilities */ 2.2 Integration projects*	*SEC2009.2.2.1 Integrated protection of rail transportation*	*Collaborative project*
	SEC2009.2.2.2 Integrated comprehensive approach to airport security	
10.2. Security of infrastructures and utilities */ 2.3 Capability projects*	*SEC-2009.2.3.1 Built infrastructure protection, including building in resilience to attack at the design stage*	*Collaborative project*
10.3. Intelligent surveillance and	*SEC-2009.3.2.1: Main port area security system*	*Collaborative*

[18] The Director-General responsible for the call may publish it up to one month prioir or after the envisaged date of publication

[19] At the time of the publication of the call, the Director-General responsible may delay this deadline by up to two months

[20] Under the condition that the preliminary draft budget for 2009 is adopted without modifications by the budget authority

[21] 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.

***border security** / 3.2 Integration projects*	*SEC-2009.3.2.2: Sea border surveillance system*	*project*
	SEC-2009.3.2.3 The Exploitation of Open Source Information in Support of Decision Making Processes	
***10.3. Intelligent surveillance and border security** / 3.4 Coordination and support actions*	*SEC-2009.3.4.1 Continuity, coverage, performance (incl. UAV; secure data link*	*Coordination and support action*
***10.4. Restoring security and safety in case of crisis** / 4.1 Demonstration projects*	*SEC-2009.4.1.1 Aftermath crisis management system*	*Coordination and support action (supporting)*
***10.4. Restoring security and safety in case of crisis** / 4.2 Integration projects*	*SEC-2009.4.2.1 First responder of the future*	*Collaborative project*
***10.4. Restoring security and safety in case of crisis** / 4.3 Capability projects*	*SEC-2009.4.3.1: Neutralisation of CBRN effects following a terrorist event*	*Collaborative project*
	SEC-2009.4.3.2: Bio-dosimetric tools to manage radiological casualties	
	SEC-2009.4.3.3: Simulation, planning and training tools and methods for management of crises and complex emergencies	
***10.6. Security and Society** / 6.1 Citizens and security*	*SEC-2009..6.1.1 Better understanding of the rationale and the drivers underlying the violent radicalisation processes and how these drivers interact*	*Collaborative projects, Network of Excellence, Coordination and support action*
***10.6. Security and Society** / 6.2 Understanding organisational structures and cultures of public users*	*SEC-2009.6.2.1 Inventories of existing national resources, institutional mandates and practices across relevant sectors*	
***10.6. Security and Society** / 6.3 Foresight, scenarios and security as an evolving concept*	*SEC-2009.6.3.1 Foresight research activities to inspire public debate, to foster shared understanding and self-organisation among stakeholders in the security domains*	
	SEC-2009;6.3.2 Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion)	
***10.6. Security and Society** / 6.4 Security Economics*	*SEC-2009.6.4.1 European Security Indicator: methodological research to provide a few select indicators of security and security policy in Europe measuring the effects of both insecurity and security policies on the economy*	
10.7. Security Research coordination and structuring	*SEC-2009-7.0.1 Transparency and networking amongst Member States and Associated States*	*Network of Excellence, Coordination and support*
	SEC-2009-7.0.2 Supply chains and market integration	

		action

- **Eligibility conditions:**

The general eligibility criteria, as set out in Annex 2 of the work programme, apply to all topics of this call.

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[22] and Networks 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 type)	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 type)	At least 1 independent legal entity.

- **Evaluation procedure**:

  A one-stage submission procedure will be followed.

  Proposals will be evaluated in a single-step procedure.

  Proposals may be evaluated remotely

- **Indicative evaluation and contractual timetable**: This call in 2008 invites proposals to be funded in 2009. Evaluations of proposals are expected to be carried out in January/February 2009. It is expected that the grant agreement negotiations for the short listed proposals will be opened in the first half of 2009.
- **Consortia agreements** are required for *all* actions.
- **Particular requirements for participation, evaluation and implementation**:

  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 persons and facilities*;

[22] The funding scheme **Collaborative project** will in this Call be divided into integration projects (large scale integrating projects with indicative Community funding of over EUR 3 500 000), and capability projects (small- and medium scale projects with indicative Community funding of EUR 3500 000 and below).

- 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.

Proposers claiming that their proposal should receive Community *funding up to 75%* should demonstrate in the proposal that the required conditions (very limited market size and a risk of "market failure", the need for accelerated equipment development in response to new threats) apply. The final decision will be based on the recommendations of the relevant evaluation panel.

Consortia are strongly encouraged to actively involve *SMEs and end users*.

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.

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.

Coordinators of all integration project proposals and of all demonstration projects (phase 1) 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.

- The forms of grants which will be offered are specified in Annex 3 to the Co-operation work programme.

Indicative budget allocation for the Security Work Programme 2009

A total of EUR 121.44[23] million is to be committed from the 2009 Community 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	2009 EUR million
Call FP7-SEC-2009-1	**117.9**
General Activities (cf. Annex 4)	**1.48**
Other Activities: • Expert Evaluators (EUR 0.8 million) • Calls for tender (EUR 0.3 million) • Support to conferences; impact assessment; monitoring, information / communication, studies, etc (EUR 0.76 million) • Support to SRC'09 (EUR 0.2 million)	**2.06**
Estimated total budget allocation	**121.44**

Summary of budget allocation to general activities for 2009 in million EUR (cf. Annex 4)

Cordis	0.39
Eureka / Research Organisations	0.01
COST	1.07
ERA-NET	0.01
Total	**1.48**

[23] Under the condition that the preliminary drat budget for 2009 is adopted without modifications by the budget authority

Security Research Call 2 (FP7-SEC-2009-1)

An indicative **40%** (deviation possible from 30% to 50%) of the budget for topics to be implemented through **Integration Projects** (Areas 2.2, 3.2, 4.2).

An indicative **50%** (deviation possible from 40% to 60%) of the budget for topics to be implemented through **Capability Projects** (Areas 1.3, 2.3, 3.3, 4.3, activity 6).

An indicative **10%** (deviation possible from 5% to 20%) of the budget for topics to be implemented through **Coordination and Supporting Activities** (activities 6 and 7), including **Demonstration Projects** (Phase 1) (Areas 1.1, 4.1), and **Networks of Excellence** (activity 6 and 7).

Up to an indicative 3% can be used for international co-operation, and up to an indicative 3% can be used for ERA-NET.

IV OTHER ACTIONS

The funding of projects and activities through the above schemes and call, and the development of the programme, will be supported by:

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

- **Monitoring, evaluation and impact assessment**: The Security research theme will comply with the requirements for monitoring, evaluation, and impact assessment. This may involve studies and surveys (implemented through public procurement) as well as panels of nominated experts.

The Security Research theme has the objectives to contribute both to the security of citizens and to growth, employment and competitiveness of the European security industry. In this context, it will facilitate the various actors to cooperate and coordinate in order to avoid unnecessary duplication and explore synergies. Therefore, **support to policy related actions** in the relevant areas of Security Research is envisaged;

- **Calls for Tender** for public procurement will be issued by the Commission, where appropriate, such as specific studies or services required to achieve the programme objective.

- The theme will also support **events and conferences**, in particular those organised by the rotating presidency of the European Union, with the objectives of:

- The dissemination of information on activities of FP7 Security research (including information seminars, audiovisual aids, exhibitions, competitions, etc).
- To bring together the main European players of research and development in the field of security.

In 2009 support will in particular be given to:

Topic SEC-2009-7.0-03 Support to the European Security Research Conference – SRC ‘09

The Swedish presidency is hosting the “European Security Research Conference - SRC '09” The conference will take place in Stockholm on 29-30 September 2009 and will allow the participation of about 1000–1200 people.

The named beneficiary for the grant is:

VINNOVA - Swedish Governmental Agency for Innovation Systems
SE-101 58 Stockholm

The EC contribution will not represent more that 50% of the total cost of the conference and is limited to EUR 200 000.

The EC contribution will be implemented as a grant through a support action, funding scheme: *Coordination and support action (supporting)*, 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 of this work programme. The director general of DG Enterprise and Industry shall be empowered to conduct the evaluation/negotiation process for the grant agreement.

In addition to direct financial support to participants in RTD actions, the Community will improve their access to private sector finance by contributing financially to the **'Risk-Sharing Finance Facility' (RSFF)** established by the European Investment Bank (EIB). Further information on the RSFF is given in the Annex 4 of this work programme.

V. INDICATIVE PRIORITIES FOR FUTURE CALLS

Indicative roadmap for publication of future calls

07/2009: Security Research Call 3
09/2009 Optional Call (for Demonstration projects phases 2)
07/2010: Security Research Call 4
09/2010 Optional Call (for Demonstration projects phases 2)
07/2011: Security Research Call 5
07/2012: Security Research Call 6

Indicative approach of future calls

- **Security Research Call 3** will be open for the *second phases* of the demonstration projects[24] called for in Security Research Call 1, as well as for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

- **Security Research Call 4** will be open for the *second phases* of the demonstration projects called for in Security Research Call 2 and for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

- **Security Research Calls 5 and 6** will offer reserve opportunities for the second phases of the demonstration projects called for in Security Research Calls 1 and 2, in case no proposal will have been selected for funding in earlier calls, and for more integration and capability projects to establish all necessary building blocks. Activities 6 and 7 will be open as well.

All calls will follow the **building block approach** of the Security theme. While focussing on the demonstration projects, these will be supported and enabled by the output of the capability and integration projects.

[24] If required, additional calls to the main annual calls can be launched especially with a view to the second phases of demonstration projects.