Meeting the challenge:
the European Security Research Agenda

A report from the
European Security
Research Advisory Board

September 2006

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2006

ISBN 92-79-01709-8

Printed in Belgium

Meeting the challenge:

the European Security Research Agenda

A report from the European Security Research Advisory Board

ESRAB members

Marek Adamczyk (PL)	*Polish Border Guard Headquarters*
Helmut Bachmayer (AT)	*Novartis International*
Rebecca Bowden (UK)	*National Security Advice Centre*
Christian Bréant (FR)	*Délégation générale pour l'armement (DGA)*
Antonio Cameli (IT)	*Ministery of Interior*
Manuel Carpio Camara (ES)	*Telefónica*
Fernando Carvalho Rodrigues (PT)	*NATO Headquarters*
Bertrand de Cordoue (EU)	*European Defence Agency*
Brian Cranmer (MT)	*Malta Maritime Authority*
Maria Dali-Ziampaka (GR)	*Ministry of Defence*
Cees van Duyvendijk (NL)	*TNO*
Thomas Engel (LU)	*Université de Luxembourg*
Jean-Louis Gerstenmayer (FR)	*Ministère Délégué à la Recherche*
Jacek Gierlinski (PL)	*Ministry of Scientific Research and Information Technology*
Nicole Gnesotto (EU)	*Institute for Security Studies*
Giancarlo Grasso (IT)	*Finmeccanica*
Maud Groenberg (NL)	*Ministry of the Interior and Kingdom Relations*
Rene Hannon (BE)	*Alcatel ETCA*
John-Erik Stig Hansen (DK)	*Statens Serum Institut*
Markus Hellenthal (DE)	*EADS*
Heinz Hoch (DE)	*Diehl VA Systeme*
Milan Holl (CZ)	*Aeronautical Research and Test Institute (VZLÚ)*
John Howe (UK)	*THALES*
Ülo Jaaksoo (EE)	*Cybernetica*
Jérôme Joly (FR)	*l'Institut de Radioprotection et de Sûreté Nucléaire*
Graham Jordan (UK)	*Royal United Services Institution for Defence and Security Studies (RUSI)*
Henryk Knapczyk (PL)	*Research and Development Centre for Mechanical Appliances*
Terry Knibb (UK)	*BAE SYSTEMS*
Helmut Krünes (AT)	*Austrian Research Centers*
Jim Lawler (IRL)	*Enterprise Ireland*
Stephan Lechner (DE)	*Siemens CT*
Erik Löwenadler (SE)	*Ericsson Microwave Systems*
Štefan Luby (SK)	*Slovak Academy of Sciences*
Livio Marchesini (IT)	*Fincantieri*
Gendrutis Mažylis (LT)	*FIMA*
Manel Medina (ES)	*Universitat Politécnica de Catalunya*
Janez Možina (SI)	*Ministry of Higher Education, Science and Technology*
Nuño Goncalo Vieira Matias (PT)	*Associação das Indústrias Marítimas*
Jacques Paccard (FR)	*Sagem Défense Sécurité*
Tamas Rath (HU)	*Ministry of Defence*
Kristiina Rintakoski (FI)	*Crisis Management International*
Carmen Rodriguez-Augustin (ES)	*INTA*
Madelene Sandström (SE)	*FOI*
Stefano Silvestri (IT)	*Instituto Affari Internazionali*
Mariano Simancas (NL)	*EUROPOL*
Jürgen Stock (DE)	*Bundeskriminalamt*
Mark Stroud (UK)	*Home Office*
Willy Tack (BE)	*Federale Overheidsdienst Defensie*
Klaus Thoma (DE)	*Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut EMI*
Alessandro Zanasi (IT)	*TEMIS Italia*

Contents

Preface

Helmut Krünes
ESRAB co-chairman

Markus Hellenthal
ESRAB co-chairman

It is rare on a national level, but even more so at European level, that end-users of security research results jointly define the required medium-term research development alongside the suppliers and performers of security research. This is exactly what the European Commission has successfully managed to achieve with the creation and implementation of the European Security Research Advisory Board (ESRAB).

In a sector as large, complex and sensitive as security, it has been a significant task of more than 300 people and their efforts are mirrored in this report.

Its preparation underlines the importance attached to security research and technology. Without it there can be no progress towards either the social aspirations for a more free, secure and open Europe or the benefits of a more competitive technology supply chain. All of these hopes for the future depend upon new solutions being developed and implemented and these all depend upon Europe having the technological capability.

But this report does much more than look inwards to the exciting research topics the sector must address. It also lays down the necessary implementation rules for successful delivery, the mechanisms for harnessing and embedding research and stimulating innovation as well as putting forward new cooperation and structuring mechanisms to make best use of Europe's combined resources.

It has been our privilege to be the chairmen of ESRAB during the last 16 months and to see the ESRAB report emerge. The report not only meets the Commission's requirements for the seventh framework programme for research and technology development but in addition offers a solid reference framework against which many national, regional, and even private research programmes can be calibrated. It cannot of course be considered a rigid long-term plan and shall need to be periodically updated, probably within the next three years, to allow new information and changed circumstances to be admitted.

On behalf of all the ESRAB members, we commend it to you.

Executive summary

Since the end of the Cold War, the threat of large-scale military aggression has subsided and been substituted by new threats which are multifaceted, interrelated, complex and increasingly transnational in their impact. These were laid out in the European security strategy ([1]) to include organised crime, terrorism, state failure, regional conflicts and proliferation of weapons of mass destruction. Implementing the European security strategy requires a comprehensive suite of internal and external security instruments covering intelligence, police, judicial, economic, financial, diplomatic and technological means. Research and technology can play a supporting role as a force enabler but cannot alone guarantee security.

How it all started

To develop a longer-term perspective in the field of security research, a Group of Personalities (GoP) was set up. Chaired by Commissioners Busquin (Research) and Liikanen (Enterprise and the Information Society), the group was composed of high-level industrialists, Members of the European Parliament, and representatives of international organisations and research institutes. In March 2004, they presented their report to the President of the Commission, entitled 'Research for a secure Europe' in which they recommended the formation of a European Security Research Advisory Board (ESRAB) to draw the strategic lines for European security research and to advise on the principles and mechanism for its implementation within the Commission's seventh framework programme for research and technology development (FP7). Furthermore, they proposed that the board focus on two principal objectives:

- meeting **society's needs** through the definition of clearly defined customer (end-user) needs;
- raising the **global competitiveness** of the European technology supply chain.

ESRAB was formed in April 2005 and signalled Europe's intent to make a significant contribution towards addressing security research and technology needs. It brought together demand articulators and research and technology suppliers in a 50-person-strong board of high-level specialists and strategists with expertise in the field of security research including: public authorities, industry, research institutes and specialist think tanks. In addition, five Members of the European Parliament and representatives from 14 European Commission services participated in the workings of the board. This report, the board's principal output, represents the work of more than 300 people.

The report in summary

Section 1 — Introduction

Section 1 sets out the background to ESRAB's formation and its resultant mandate.

Section 2 — Technology development

Section 2 focuses on the foundation of technical research needed to meet the four FP7 mission areas: namely, protection against terrorism and organised crime, border security, critical infrastructure protection, and restoring security in case of crisis. A capability-based approach, as advocated in the GoP report, was applied to identify the main capabilities, integrated projects and demonstration programmes that should be developed. Only those offering a high potential to deliver European added value were retained. They look to build upon existing research undertaken both nationally and at EU level.

The first research path, capability development, represents the cornerstone of the technical research. While this is not the place to describe each capability individually, it is perhaps useful to highlight certain capabilities to provide an insight into the proposed research.

([1]) A secure Europe in a better world (December 2003)

Detection and identification capabilities represent a key area for EU investment over the coming years. A broad range of application examples include the detection of small boats in blue borders, detection of abnormal crowd behaviour, detection of unattended luggage in open areas and the detection of dangerous goods (drugs, explosives and CBRN) where existing technologies are generally too bulky, too slow, and generate unacceptably high false alarm rates. Complementary capabilities, to be developed in parallel, relate to improving the identification and authentication of cooperative, or non-cooperative, individuals. The underpinning biometric based systems will support the fight against terrorism, be instrumental in the aftermath of a crisis and will improve access control at both border checkpoints and critical infrastructures. Finally detection, identification and authentication capabilities need to be supported by appropriate localisation and tracking capabilities for individuals and goods for a comprehensive approach towards potential threats.

Information management systems that more efficiently and effectively provide first responders and decision-makers with improved situation awareness and interoperable command and control capabilities is another key area for investment. This includes improved surveillance capabilities with respect to coverage and quality and the fusion of real-time sensor data (space, air, land, sea) in order to establish a common operational picture. On occasion planning, modelling and situation analysis tools will also need to be integrated. GMES, and its first wave of services, could play an integral role in this respect. Situation awareness and command and control capabilities should be supported by robust, secure and interoperable communication systems allied to significantly improved protection of supervisory control and data acquisition (SCADA) systems, widely used today for energy generation, transmission and distribution.

Risk assessment, modelling and simulation tools should act as support tools for decision-makers in setting priorities for multiple threats and testing mitigation measures prior to incident intervention. Such tools will also benefit first responders in their efforts to improve training and exercise capabilities. Finally, the development of intervention and neutralisation capabilities, in particular for post-crisis decontamination, is important

The second research path, addressing **system development** through integrated projects, looks to build upon capability development by integrating different capabilities, technologies and disciplines in innovative combinations. ESRAB has identified 20 integrated projects, and whilst not exhaustive, they collectively represent a balanced and considered view across all four mission areas and intentionally range in scope to accommodate greater SME participation.

The third research path, system-of-systems demonstration, recognises that for large security solutions to enter into service, numerous independent but interrelated systems must be integrated and then demonstrated to prove operational effectiveness. In areas of significant European interest, it is recommended that demonstration programmes be established to act as federative frames to coalesce the required research. These European flagships would aim to ensure the coherent development of the required system building blocks, architectures and standards. ESRAB recommends the formation of **five demonstration programmes**:

- aftermath crisis management system — providing a complete integrated and interoperable aftermath crisis management system for a coordinated response from crisis managers and first responders from different agencies within, and across, the EU;
- European-wide integrated border control system — integrated border management system encompassing surveillance, monitoring, identity management and advanced training methods/tools;
- logistic and supply chain security — an integrated approach to risk assessment, product traceability, secure exchange of goods between nations and

across operators and the fast but effective screening of goods and platforms;

- security of mass transportation — consistent and integrated suite of mass transportation security systems, covering secure transport networks, nodes and platforms. Sector-specific needs and the cross-border complexities will be key drivers;

- CBRNE — an integrated approach for CBRNE threat assessment, consequence modelling, detection and identification of agents and devices, incident management tools, prevention, decontamination and medical care.

Section 3 — Security and society

As the GoP report highlighted, technology can only be part of the effective response to security threats and must be applied in combination with organisational processes and human intervention. Solutions shall need to be multidimensional taking into account the different experiences and approaches to life across Europe. The security and society section focuses on important societal related research in five key areas: citizens and security, understanding organisational structures and cultures of public users, foresight scenarios and security as an evolving concept, security economics, and ethics and justice.

The research aims to determine the long-term threats to European security and, in combination with empirical economic research, guide the development of both technologies and policies. Research into ethics and privacy, and the trade-off between improved security and loss of privacy, will influence technology development and in parallel address aspects of how citizens perceptive security and insecurity. The manner in which governments are organised to meet security threats, both structurally and culturally, and furthermore how these threats are communicated between national authorities and citizens in both crisis and normal situations is to be investigated. Finally, as the London and Madrid bombings graphically illustrated, research into understanding terrorist behaviour, radicalisation and terrorist recruitment in the EU is an essential terrorism counter measure.

Section 4 — Enablers

Section 4 brings into focus the importance of the supporting enablers. Important though the mission capabilities and technologies are, considering them in isolation without the requisite enablers, will not yield the optimum benefit for all stakeholders. A combined treatment will be essential if the substantial financial and human resources to be invested are to yield the anticipated returns. Ultimately this will be measured by the amount of research transformed into new products and services. ESRAB identified three key enabling areas.

The **implementation rules** subsection addresses the issue of how to cope with the specificities and sensitivities of implementing European security research. Particular governance structures, mechanisms for handling classified information, reinforcing the protection of intellectual property rights and assessing the suitability of international cooperation are recommended. Specific aspects of evaluation and co funding levels have also been identified.

The **coordination and structuring** subsection outlines mechanisms to address the efficiency and effectiveness of European security research with the objective of avoiding unnecessary duplication and focusing research on high leverage customer driven requirements. All proposed mechanisms aim to deepen end-user engagement with the most ambitious mechanisms calling for the creation of a new European Security Board whose principal aim would be to ensure that all the component parts required to realise an improvement in European security (research, policies, legislation, standardisation, etc.) are synchronised and directed towards commonly agreed priorities.

The **link to innovation** subsection identifies mechanisms by which European security research can stimulate innovation, raise competitiveness and accelerate the pull through of research into procured products and services. ESRAB's principal recommendation is the development of a European security innovation system. It should build upon innovative pre-commercial public procurement, the use of large-scale demonstration programmes, greater SME engagement and the definition and use of European standards.

Section 5 — Findings

Section 5 of the report sets out ESRAB's key findings and the future steps required to meet European security research needs.

ESRAB key findings

1. The ESRAB report represents the successful implementation of the GoP recommendation to **bring together at European level the 'demand' and 'supply' sides** in order to jointly define commonly agreed strategic lines of action for European security research. The report demonstrates both the value and feasibility of such an approach.

2. ESRAB has produced a **strategic framework** to structure the research content covering both **technological and non-technological aspects.** The report identifies and prioritises only those capabilities, integrated projects and demonstration programmes which offer a high potential to deliver European added value.

3. ESRAB recommends that multidisciplinary **mission-oriented research** should be undertaken covering capability development, system development and systems of systems demonstration. Technology development should include new and emerging technologies to address security-specific breakthrough technologies. As a matter of principle, it should **combine end-users and suppliers in project definition and execution**. The programme should be SME inclusive but not SME driven.

4. ESRAB has addressed the special **implementation rules** for European security research. In particular these relate to governance, with a **reinforced role of the Member States' authorities** (programme committee), and the handling of sensitive information, through the use of EU regulation on classified information (still to be updated).

5. Respect of **privacy and civil liberties** should be the programme's guiding principle. In this sense research and development projects should take into account the mutual dependency triangle of technology, organisational dynamics and human impact.

6. Technological research and development must be strengthened, and when appropriate integrated, with research into **political, social and human sciences**. Five areas are identified: citizens and security, understanding organisational structures and cultures of public users, foresight scenarios and security as evolving concept, economics of security, and ethics and justice.

7. Five enabling areas have been identified to **stimulate innovation** and improve **the pull through of research into procured products and services** — they include: technology supply chain competitiveness, SME engagement, standardisation, leveraging best practice and end-user involvement.

8. ESRAB emphasises the need for **effective coordination and transparency** to ensure that unnecessary duplication is avoided and that European security research both informs, and takes account of, other European and international research. The report identifies the mechanisms to achieve this, including the use of technology watches for organisations which share a common technology base, for example the **European Defence Agency**.

9. European security research needs to be complementary to national security research programmes. Where these exist, they should be aligned to the EU programme, and where they do not, it is proposed that these should be established, supported by a critical mass of resources. **Funding at EU level should not substitute national funding in this important area.** A rolling programme of national workshops, aimed at raising the awareness of security research and the manner in which national programmes could complement the European security research, should be initiated in the second half of 2006.

10. ESRAB recommends the creation of a **European Security Board (ESB)**, to foster greater dialogue and a shared view of European security needs. The board should bring together, in a non-bureaucratic manner, au-thoritative senior representatives from a cross stakeholder community of public and private stakeholders to jointly develop a **strategic security agenda** and act as a possible reference body for the implementation of existing programmes and initiatives. Participation in the ESB would involve a commitment to influence all stakeholders to plan their activities in the light of the agenda. Consensus at the ESB level should help in the **sharing of tasks** and shaping relations between national and EU programmes/policies as well as **influencing the deployment of funds**.

Section 1

Introduction

Introduction

Europe has never been so peacefully consolidated, so prosperous and secure yet at the same time so vulnerable. Since the end of the Cold War, the threat of large-scale military aggression has subsided and been substituted by new threats, risks and vulnerabilities. These were laid out in the European security strategy, *A secure Europe in a better world* (2003), to include organised crime, terrorism, state failure, regional conflicts and proliferation of weapons of mass destruction. The recent catastrophic events in Madrid (2004) and London (2005) have shown that Europe is not immune to terrorist attack. Domestic radicalisation of parts of society, including individuals born and brought up in Europe, is forcing many governments to re-evaluate not only their approaches to external security, but also their internal policies on education, job creation, housing, and other social issues.

The new threats underline the fact that internal and external security is increasingly inseparable, with the first line of defence often being abroad. The protection of Europe's external borders will, however, remain of paramount importance, especially if the Union wishes to maintain and promote freedom of movement within its borders. The enlargement of the Union, covering **25 nations and over 450 million people**, made this more challenging by increasing the external borders by 34 % to encompass 6 000 km of land borders and 85 000 km of coastlines. The creation in 2003 of the external borders agency FRONTEX pointed to Europe's commitment to this key area and an already challenging task is likely to become increasingly more difficult. European imports and exports have increased at 8 % per annum over the last decade, most channelled through Europe's seaports. Even at today's throughput, less than 5 % of all containers are scanned for illegal goods, people and hazardous substances. To meet the required future rates of throughput, new affordable solutions are urgently required.

In addition, there is a growing dependence on interconnected infrastructures in transport, energy, information and other fields increasing the vulnerability of modern societies. At the same time, the natural diffusion of technological know-how resulting from scientific and industrial development makes it easier for technological advancements to be used malevolently. In light of this, Europe has recognised the threat to its critical infrastructures and is aiming to provide effective protection through communication, coordination, and cooperation at national and EU level. Although not yet complete, **the Commission is actively engaged** with a broad community of owners, operators, regulators, professional bodies, industry associations and governments to develop a European programme for critical infrastructure protection.

The threats facing Europe are multifaceted, interrelated, complex and increasingly transnational in their impact. It is a simple truth that no single state can accomplish security alone — not even the United Sates. Implementing the European security strategy demands a comprehensive suite of instruments covering intelligence, police, judicial, economic, financial, diplomatic and technological means. Research and technology can play a supporting role as a force enabler but cannot alone guarantee security. In this respect, last year's **formation of the European Security Research Advisory Board (ESRAB)** signalled that Europe is ready to make a significant contribution towards addressing security research and technology needs, in a comprehensive and inclusive manner.

How it all started

There has been an increasing awareness that security, and the many different facets that make it up, present fundamental challenges that will not yield to independent and sector-specific treatment but rather need more ambitious, coordinated and holistic approaches. So, to develop a longer-term perspective in the field of security research, a Group of Personalities (GoP) was set up. Chaired by Commissioners Busquin (Research) and Liikanen (Enterprise and the Information Society), the group was composed of high-level industrialists, Members of the European Parliament, and representatives of international organisations and research

institutes. In March 2004, they presented their report to the President of the Commission, entitled 'Research for a secure Europe' ([2]).

It recommended the formation of ESRAB to draw the strategic lines for European security research and to advise on the principles and mechanism for its implementation within the Commission's seventh framework programme for research and technology development (FP7). It suggested that the board should consist of high-level experts taken from across the full spectrum of security relevant stakeholders and that collectively they focus on two principal objectives:

- meeting society's needs through the definition of clearly defined customer (end-user) needs;
- raising the global competitiveness of the European technology supply chain.

In September 2004, the Commission published a communication entitled *'European security research: the next steps'* subscribing to the main thrusts of recommendations in the GoP report, including the creation of ESRAB which was formed in April 2005. It brought together demand articulators and research and technology suppliers in a 50-person-strong board of high-level specialists and strategists including public authorities, industry, research institutes and specialist think tanks. In addition, five Members of the European Parliament ([3]) and representatives from 14 European Commission services ([4]) participated in the workings of the board.

The Commission decision forming ESRAB outlined the principal tasks it would pursue, which included:

- to ensure consultation and cooperation among all stakeholders in order to outline a comprehensive **European security research agenda;**
- to establish **a network of users and technical experts** in order to interactively identify the technological capabilities to be put in place among the European stakeholders;
- to recommend a **strategy to improve the European industry's technological base** so as to improve its competitiveness;
- to advise on the **strategic and operational aspects** of the future programme taking into account past experience;
- to advise on the required **implementation rules** such as the exchange of classified information and intellectual property rights;
- to optimise the use of **public owned research and evaluation infrastructures**;
- to develop and implement a **communications strategy** to promote awareness of European security research.

The creation of this report over the last 16 months has involved a vast amount of work undertaken under ESRAB's leadership, extending across the full breadth of its stakeholder base. This has been the first time that a proposal on this scale has been attempted in Europe and, in itself, represents a substantial vindication of the concept of bringing together 'demand' and 'supply' to jointly define commonly agreed strategic lines for European security research.

Navigating the report

The report itself is structured into five sections. Section 1 highlights the reasons for, and mandate of, ESRAB whilst the following section focuses on the foundation of technical research needed to address the security missions. Within the same section, a transversal cross mission analysis is provided. Section 3 focuses on societal related research which is acknowledged as being of equal importance for the security of the citizen as technology related research. Section 4 addresses the required enablers to implement the research and make best use of Europe's resources in the security field. The final section highlights ESRAB's principal findings.

([2]) http://ec.europa.eu/enterprise/security/documents_en.htm

([3]) Committees of Civil Liberties, Justice and Home Affairs; Industry, Research and Energy; Internal Market and Consumer Protection; Foreign Affairs and its Subcommittee on Security and Defence.

([4]) Bureau of European Policy Advisers, Budget DG, Enterprise and Industry DG, Environment DG, Information Society and Media DG, Justice, Freedom and Security DG, Joint Research Centre, Internal Market and Services DG, External Relations DG, Research DG, Health and Consumer Protection DG, Secretariat-General, Taxation and Customs Union DG, and Energy and Transport DG.

Section 2

Technology development

Framework, structure and methodology

The current threats facing society are both numerous, complex and fluid. Society is not confronted with a single threat, hazard or vulnerability, but a variety of challenges such as terrorism, organised crime, regional instability and natural disasters that demand a corresponding variety of non-technological and technological actions, of a preventive nature as well as counter measures. These threats, and the responses to them, are described in numerous documents including the European security strategy, Common Foreign and Security Policy and the Hague programme.

The research required to address these threats was, according to the GoP report, to be arrived at using a capability-related approach moving from threats through missions to capabilities and finally technologies. The Commission is in full agreement with this approach and in its FP7 communication of April 2005 it laid out the activities at Community level against four security mission areas and three areas of cross-cutting interest.

This framework and structure formed the foundation of ESRAB's work, with the working groups aligning themselves with the four missions (**border security, protection against terrorism and organised crime, critical infrastructure protection, and restoring security in case of crisis**) and the three areas of cross-cutting interest (**integration/ interoperability, security and society, coordination**).

Two additional groups were created. The first set up to advise on the critical area of **principles and mechanisms for implementation** whilst the second aimed to address the manner in which research could be more rapidly embedded and **innovation** stimulated. In total, over **300 experts** were spread across the nine groups.

Definition of 'security research'

With the framework and structure established, the scope of ESRAB's security research work was defined as being:

'...research activities that aim at identifying, preventing, deterring, preparing and protecting against unlawful or intentional malicious acts harming European societies; human beings, organisations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (also applicable after natural/industrial disasters)'.

It was emphasised that all the activities covered by the above definition would have to be conducted in full respect of European citizens' human rights and fundamental freedoms.

A capability-based approach

Capabilities were chosen as the **principal building block for technology definition** as they represented the smallest complete assembly of technologies and processes that together lead to an ability to perform a specific function, task or operation.

The capabilities were arrived at from **a close analysis of the security missions**, their associated sub missions and related security issues. The analysis was supported by data from over 225 end-user organisations and 150 research and technology providers. The capabilities were an amalgam of both mission-specific and multi-mission entries which combined technology solutions to varying degrees of range, depth and application. In the majority of cases, they were described in terms of their driving operational requirements (e.g. speed, distance, etc.) which provided guidance as to the applicability, or otherwise, of the technology solutions that could be proposed.

Due to the sheer number of capabilities generated and the extent to which they each varied in terms of granularity and breadth of description, a common reference for grouping

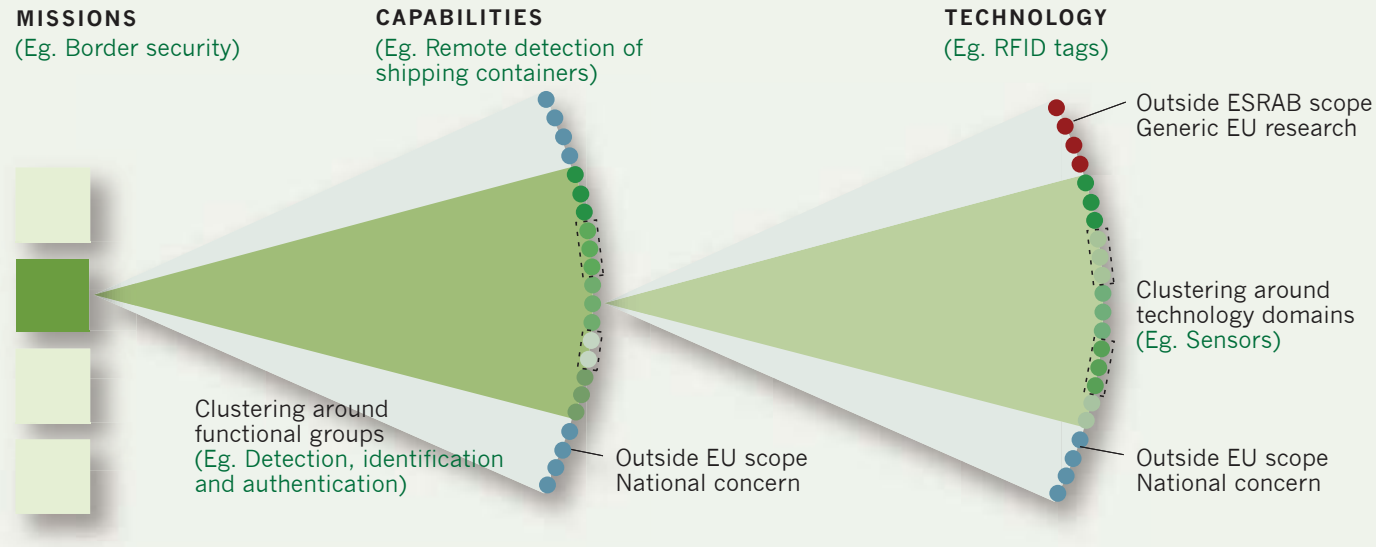

Figure 1: A capability based approach

the capabilities was established. Based on **11 functional groups** (listed below), it runs as a wire frame through the report:

- risk assessment, modelling and impact reduction;
- doctrine and operation;
- training and exercises;
- detection, identification and authentication;
- positioning and localisation;
- situation awareness and assessment (surveillance);
- information management;
- intervention and neutralisation;
- communication;
- command and control;
- incident response.

The chosen functional grouping had the advantage that they were well aligned to common pools of technology which facilitated the subsequent **technology mapping** process. This was undertaken using standardised technology taxonomy to facilitate cross mission technology comparison. The technologies were ranked in terms of their relative importance in meeting the capability requirements. In addition a summary view across all missions as to the relative importance of each of the technology domains can be found on page 50.

The technologies were a combination of three classifications: (a) generic technologies required for the security research programme but whose maturity would be developed, and adequately funded, by other programmes; (b) security-specific technologies not adequately addressed, or funded, by other programmes but which would be addressable at European level; and (c) security-specific technologies of purely national concern. The latter have not been incorporated in the report.

The interlinkages between the different nomenclatures (missions, capabilities, functions and technologies) is schematically illustrated in Figure 1.

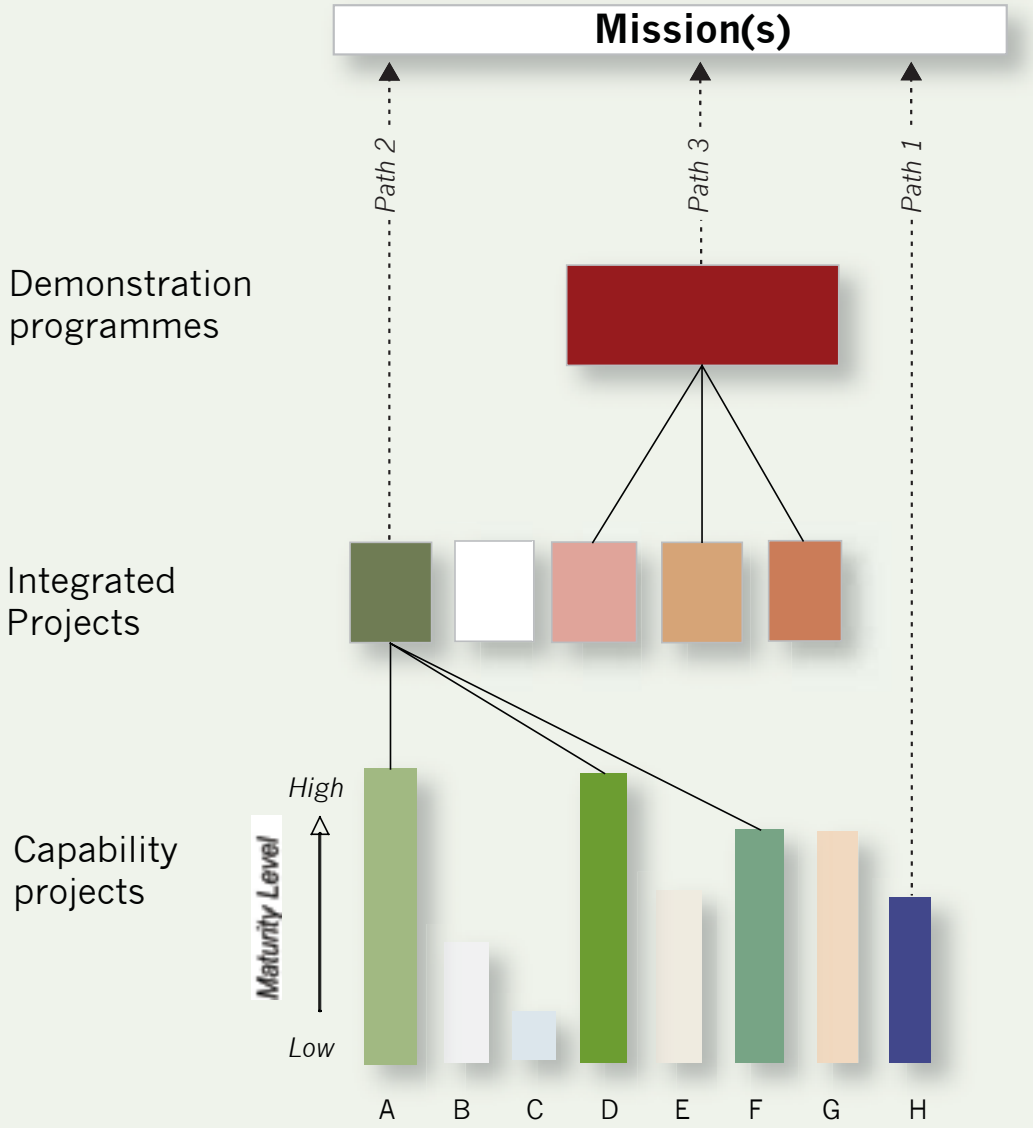

Figure 2: Research paths

Research paths

The scope of ESRAB's work spans the full research spectrum, from technology development through to system of systems demonstration. It covers both short-term advances and longer term breakthrough technical solutions.

ESRAB has grouped its technical research into three distinct research paths as shown in Figure 2:

- **research path 1 — capability development** (multi-mission or mission-specific): technology development to improve the maturity level of a specific capability, or of a complementary and interrelated group of capabilities; technology development should also include new and emerging technologies to address breakthrough technologies that are security specific;
- **research path 2 — system development** (mission specific): integration of a number of capabilities, technologies and disciplines, at an appropriate state of readiness, in innovative combinations in order to deliver significant operational performance advances;
- **research path 3 — systems of systems demonstration** (multi-mission): the challenge of integrating a number of systems in which the integration and demonstration aspect represents the majority of the work, and challenge, to be undertaken; these are intended to be 'flagship' demonstration programmes providing a federative frame to coalesce research in areas of significant European interest.

The successful achievement of the demonstration programmes is dependent upon the coherent, compatible and synchronised development of the requisite capabilities and system 'building blocks' of research paths 1 and 2.

European added value

Not all capability development warrants treatment at European level. The sheer number of capabilities defined, allied to the limited budget available, drove the need to down select capabilities based on defined criteria. These included:

- identifying those capabilities with a **clear impact on EU security**;
- from these, selecting those with clear **European added value**, notably those dealing with:
  - critical mass — specific result unachievable if only dealt with nationally;
  - economy of scale — efficiency and effectiveness significantly improved as compared to only being handled nationally.

From this pool of 'eligible' capabilities, high priority capabilities were identified through a careful analysis as to their importance to the missions, integrated projects and demonstration programmes.

Layout of the technical section

As the tables below demonstrate, the technical section of the report is split into two parts: a **mission area oriented analysis** followed thereafter by a **cross mission area analysis**.

The security **mission area analysis** is structured around a common framework of subsections, outlined below, so that they may easily be compared with each other.

Mission scope	Addressing the boundary of the security mission and the key security issues and considerations as viewed from the mission perspective.
Capabilities	Overview of the highest priority capabilities required to meet the issues identified in the scoping section. Requisite underpinning sub-capabilities and technologies are not elaborated.
Integrated projects	Described in a similar manner across all missions, and identifies those areas where system development is required to demonstrate significant operational or system advances. The project proposals, indicative as opposed to exhaustive, represent a balanced and considered view and intentionally range in scope from broad to narrow to accommodate greater SME participation.
Linkages/ enablers/ constraints	An exploration of the non-technical enabling factors which would be instrumental in delivering the foreseen technological inputs, e.g. standards, legislation, human factors, partnerships, etc.
Overview diagram	A schematic diagram that describes the mission, its associated capabilities and indicative technologies.

The cross mission area analysis is structured in three parts:

Integration, connectivity and interoperability	Highlights the common interoperability and connectivity strands emerging from the previously addressed mission-specific descriptions.
Capabilities and technologies	A cross mission perspective as to the high frequency multi-mission capabilities and an overarching view as to the most relevant technology domains and technologies.
Demonstration programmes	Standardised description detailing the scope, the improvement areas to be addressed and the anticipated benefits of successful delivery.

Table 1: Layout of the technical section

Section 2.1

Mission area analysis

Border security

Mission scope

During recent years, with the increase of major acts of international terrorism, and with the increase of cross-border flows of illegal goods, people and substances, the question of border management has taken on a higher profile. Europe is at the same time faced with a strategic challenge of how to balance the new security requirements with those required to facilitate legitimate trade and flow of people. Ultimately trade and people flows are the basis for socioeconomic convergence, and socioeconomic development itself is an underpinning to European security.

Enlargement has made this task more complex. Europe's border is formed by 6 000 km of land borders and 85 000 km of coastlines with more than 1 200 seaports, 500 airports, and hundreds of railway stations acting as regulated entry/exit points. Schengen cooperation affords entrants to the Union a wide area of mobility thus those protecting the external borders have a key role to play. National authorities have naturally undertaken work in this area but more still needs to be done. Clearly the task is enormous and requires a coordinated and integrated approach. The Unions external borders agency, FRONTEX, is expected to take on an influential role in particular with respect to the convergence of information management systems, interoperability, training and cascading best practice.

The ESRAB work has focussed on illegal immigration and the trafficking of drugs, weapons and illicit substances.

Illegal immigration — The EU estimates that organised crime generates an income of approximately EUR 3 billion per year from activities linked to illegal immigration. Illegal immigrants are smuggled into Europe either across unregulated land, sea or air borders or through regulated security check points using counterfeit/stolen passports or concealed in cargoes. EUROPOL calculates that around 500 000 people enter the European Union illegally every year. The flow of goods and people through regulated checkpoints will undoubtedly increase and the majority of Member States will need to increase their effective capabilities in this area. Novel, reliable and scaleable solutions will be required if illegal immigrants are to be filtered out efficiently whilst not unduly impeding the flow of the vast majority of legitimate travellers and vehicles. Such solutions will naturally have to respect privacy and human rights.

Trafficking of drugs, weapons and illicit substances such as nuclear, biological and chemical agents, remains a threat from criminal and terrorist groups across Europe. Regulated border security crossings represent interception choke points for such material, although cost and screening times mean less than 5 % of containers are currently scanned. The largest volume of trade is carried by sea and reaches, or is exported from, European harbours. Intricate supply chain networks exist to distribute goods, supported largely by trucks and warehouse distribution hubs. A coordinated and integrated security system is required to ensure the security of the supply chain and logistics networks. The transnational and international dimension will inevitably lead to requirements for traceability, standardisation and more affordable robust solutions. For Europe, the major challenge will be to reduce both unit cost and screening times to enhance security whilst facilitating legitimate commerce between countries.

Capabilities

Out of the more than 110 capabilities which were identified as being of importance, 30 have been identified as being priority capabilities for the fight against illegal immigration and illicit trafficking. The 30 capabilities are presented in graphical format in Figure 3 whilst the ones offering the highest impact are described below under their respective functional groups.

Function: Detection, identification and authentication
Taking into account the different types of regulated and unregulated borders — sea, air and land — the following capabilities should be considered as a priority for Europe. Detection and identification of large and small fast boats for blue borders and ports; the detection and identification of personnel and vehicle movements at unregulated borders and their authentication at check-points. Goods and container intrusion control capabilities should be developed to avoid content contamination or biological/chemical attacks and to detect illicit trafficking of drugs or explosives. This should be supported by capabilities to allow the remote detection of shipping containers so that, if required, they could be traced and tracked.

Function: Situation awareness and assessment, including surveillance
Situational awareness involves the capture, fusion, correlation and interpretation of disparate forms of real-time and historical data and their presentation in a clear manner, facilitating effective decision-making and performance in a complex environment. Interoperable databases will be essential to allow surveillance information to be cross-referenced against multiple heterogeneous sources in order to address illicit access of people and goods, for example integrated visa/immigration control systems. Surveillance information itself will come from various sources, however, when looking to the scale and scope of Europe's borders (land, sea and air) capabilities are required for longer endurance platforms, including UAVs, and secure high bandwidth data link for data transfer between them. GMES, and its first wave of services, could also play an integral role in this respect.

Function: Information management
Handling information acquired by many different sources and making it available to those with permission is an essential capability in order to improve awareness at Europe's borders. Techniques related to data and information fusion including data mining, natural language processing technologies, image/pattern recognition and expert systems are key enabling capabilities for this function. Such techniques must be investigated in parallel to intelligent knowledge based systems which look to develop active learning networks to identify and alert border security communities to early warning signs of possible threats.

Priority, however, should be given to the development of information fusion, exchange techniques, gateways and translators, to facilitate the exchange of information between non-interoperable information systems at borders.

Function: Communication
Due to the sensitive nature of policing Europe's external borders, particular attention should be paid to improving end-to-end secure communication in order to facilitate sharing of data within, and between, organisations and countries. To this end capabilities supporting interoperable and robust software defined radio solutions, offering the requisite flexibility to respond to dynamic situations are seen as important.

Function: Training and exercises
Border security is only effective if undertaken by both parties to a high standard. To improve the effectiveness of border security staff, training and exercise capabilities should be enhanced through computer aided training, simulation systems, situation modelling, scenario generation and consequence management. For this to be done effectively there is a need to develop dedicated training, education and simulation facilities.

Integrated projects

The scale and scope of border management is so vast that effective border management can only be achieved by adopting an integrated approach to the requisite technologies, systems and information sources. Some examples of such situations where multiple technologies could be integrated and demonstrated are shown in Table 2.

	Main port security (including containers)	**Sea borders surveillance**	**Unregulated land borders surveillance**	**Check points**	**Extended smart border**
Objectives	To improve situation awareness at main ports through the monitoring and tracking of complex port environments as a consequence of the continuous arrival and departure of cargo, ships, vehicles, staff and passengers.	To prevent smuggling, illegal immigration or terrorist attacks through improvements in sea border security spanning the area from Europe's coastline to the exclusive economic zone (EEZ).	Detect and locate the movements of individuals, vehicles and biological and chemical substances crossing unregulated land borders and, when required, track and trace their movements thereafter.	To enhance the existing screening portals at regulated border crossing points for individuals, vehicles and platforms.	To monitor immigration flows at the external borders and forecast, through the integration of simulated and real-time data, possible scenarios and operational procedures for intervention.
Scope	• Integration, connectivity or interoperability of heterogeneous systems • Rapid dissemination of information, without conversion, interpretation or overload • High performance wireless connectivity for mobile sensors • Integration of ad hoc wireless networks with fixed networks • Integration in a multi-sensor environment of large volumes of data	• Automatic detection and tracking of vessels through fixed (coastal) and aerial sensors, including UAV and satellite monitoring • UAV insertion in air traffic taking into account specific security missions • improvement in data fusion algorithms • improvement in signal processing techniques to expand the performance of individual sensors • Cost reduction technologies	• System of stand-off sensors that combines active imaging for infra red and cameras with radar and passive sensors • Enhance data fusion performance with chemical and biological sensors data • Intelligence sources analysis	• Advanced detection technologies for threats, e.g. explosives, biohazards, chemical and nuclear materials • Integrating detection with automatic video analysis systems, multi-biometrics and mobile OCR technologies • Creation of a shared database of information/intelligence between the European border security operators, to improve situation awareness	• Complex operational scenarios • Integrated in-situ and observed data with intelligence information • Simulation technologies to train operators in preventing illegal immigration • Command and control system interoperability • Man machine interface and decision support data presentation
Outcome	An integrated port security system capable of providing accurate situational awareness and alerting security operators to required interventions.	Maritime border security system that will provide an automatic assessment of the overall threat level for both short and long range.	Adaptable land border security system to detect threats and identify, locate and track illicit trafficking.	Advanced check point system for the identification of individuals, vehicles and platforms.	Complete system that monitors immigration flows and facilitates decision-making through data fusion of intelligence, surveillance and in-situ data.

Table 2: Border security - Integrated projects

MISSION | FUNCTIONS | CAPABILITIES (major) | TECHNOLOGIES (major)

Border security

Situation Awareness & Assessment (including Surveillance)

- Land wide area surveillance (Incl. border lines and Large regions) of people and vehicles
- Information availability, correlation and fusion
- Cross-analysis of databases, integrated visa/immigration facilities control systems
- BLUE Wide Area Surveillance (EEZ and Beyond) in wide areas through active and passive means.
- Land small area surveillance of people, equipment and vehicles in controlled areas
- Remote detection of shipping containers
- Continuity, coverage, performance (incl. UAV; secure data link)
- Small area surveillance (Ports and Harbours)
- AIR 3D Surveillance (Incl. border lines and Large regions), linked to the ATM systems

- RFID based tracing
- Digital signal processing technology
- Image / pattern processing technology
- Surveillance and navigation satellites
- Data and information management technology (DB, …)
- Unmanned land / sea / air vehicles

Information Management

- Data fusion techniques: Design, development and application of data/information fusion techniques. Examples contain data mining, trend detection, forgetting data, optimization analysis.
- Information exchange: techniques to facilitate the exchange of information between non interoperable information systems.
- Semantics, topology: development of topologies and ontologies to facilitate data exchange based on semantic translations and common definitions of content.
- Secure interoperability: techniques to insure secure interoperability between current and future systems, domain different systems (i.e. civil and military) including data access control and data exchange without source availability

- Data fusion techniques
- Text-mining / data-mining
- Information fusion technology

Communication

- Solutions for ensuring end-to-end communication availability, relying on physical and logical technologies, on diversity of hybrid systems
- End-to-end quality of service, covering specific requirements for priority traffic and ensuring the QoS is guaranteed under all conditions
- Interoperable and robust solutions for software defined radio
- Dynamic authentication in ad hoc wireless networks for emergency communication
- Physical integration of C4 equipment and interface with carrying platforms – Equipment of limited cost, dimensions, mass, power supply

- Communications network management and control equipment, network supervisor
- Authentication technologies
- Broadband access to mobile users in dynamic situations / EM difficult scenarios
- Secured, wireless broadband data links for secured communications

Detection, Identification and authentication

- Access control. Authentication of people and vehicles
- Land Small area – detection of potential threats
- LAND Wide Area – Detection of personnel and vehicles movements
- BLUE Wide Area (EEZ and Beyond) – Detection of large and small (fast) boats in a maritime environment
- AIR 3D detection of manned and unmanned, UAV and light aircraft
- Small Blue area (Ports and Harbours) Detection of large and small (fast) boats and swimmers
- Drugs, explosives, Viri, CBRN detection. Very fast early warning. After alert checking of type and identification.
- Detection of people attempting to enter illegally,
- UNDERWATER 3D, Detection of underwater vehicles: at regulated borders (harbours).
- Land Small area – detection of potential vehicle threats

- Earth observation
- Motion sensor systems
- Hyper-spectral / multi-spectral processing
- Explosive detection sensors
- Helicopters
- IR sensor technologies
- SAR / ISAR equipment
- Acoustic sensors
- Radar sensors

- Autonomous small sensors / smart dust technologies
- Hyper spectral / multi spectral sensors
- Non-Co-operative Target Recognition
- Digital fingerprints recognition
- Chemical and biological detection technologies

Training and exercise

- Develop training, education and simulation facilities. Description: With the use of scenario and situation modelling, computer aided training, and simulation

- Training techniques
- Synthetic environments – synthetic force generation
- Mission simulation

Figure 3

Border security

– overview diagram of the main functions, capabilities and technologies

Overview diagram

Border security

Linkages/enablers/constraints

Much of the work in the border security mission relies on adopting harmonised equipment, systems, procedures and methods. In this sense standardisation, regulation and legislation could act as fundamental enablers to achieving an integrated border management system.

By way of example, the new 'e-passport' will allow the positive (or negative) identification of all documented individuals. This new passport, which includes fingerprints and a photograph of the individual, will have to rely on clear and accepted **standards** for documenting biometric data, as well as tools for the collection and storage of such information. The timely and widespread use of such standards is a critical success factor.

In certain instances standards could, in themselves, be insufficient and may need to be augmented with testing, evaluation and certification to ensure proper implementation. The case of fingerprints highlights this problem succinctly in that there are numerous types of technologies giving rise to problems and challenges such as incompatibility and unequal levels of accuracy. Equally **certification** and supporting regulations will be key enablers, ranging in their application from individual pieces of equipment through to the development and implementation of systems, e.g. UAVs. The recommendations put forward in the development of European policies and standards in the link to innovation section (page 73) will make a positive impact in this respect.

The automatic **ship identification system** (AIS) for vessel trafficking is already utilised on larger vessels enabling their automatic identification when reaching port or when nearing the coast line. Currently this does not apply to smaller vessels which handicaps authorities attempting to clamp down on illegal trafficking, typically expedited using these smaller vessels. The diffusion of this technology, together with a recognised European standard, could offer Europe a competitive advantage in a global market.

Research proposed within the security and society section (page 54) will read across to the technology development for border security. In particular the topics related to **abnormal behaviour**, organisational structures and foresight scenarios will affect the manner in which nations train, organise and prepare for controlling and managing their borders.

The integrated projects identified earlier aim to address specific border security needs, but represent building blocks towards the larger **demonstration programmes** identified in Section 2.2. The demonstration programmes entitled 'European-wide integrated border control system' and 'logistic and supply chain security' have the highest relevance to the border security mission.

Protection against terrorism and organised crime

Mission scope

Organised crime, and its undeniable link to terrorist financing, poses large and complex problems for Europe. A symbiotic relationship exists whereby terrorists benefit from the infrastructure that organised crime in many cases can provide while organised crime benefits from the financial ties terrorists have built to fund their assaults.

In both these areas, the rapid advancement in technology and science provides both benefits and significant challenges to law enforcement. Today's organised criminals and terrorist groups are making full use of easily accessible technology to further their activities. Drug smugglers are using encrypted telephones to protect their conversations, counterfeiters are using high-powered computers and laser printers to produce currencies, child pornographers are using the Internet to communicate and trade their illicit wares, and money launderers are utilising sophisticated trade transactions to disguise the movement of funds throughout the world. Uncovering such activities becomes ever more difficult as globalisation and legitimate international trade and financial transactions increase ever more rapidly.

Whilst a significant amount of work has been undertaken nationally, the international and transnational nature of organised crime and terrorism, means that success is dependent on Europe's abilities to work closely together, to communicate effectively, and to exchange information quickly and legally. In this respect, EUROPOL and EUROJUST continue to play and develop an instrumental role.

ESRAB activities in this area covered a wide spectrum of organised crime and counter terrorism activities.

Organised crime — activities range from drug and weapons smuggling, complicated money laundering and child pornography trafficking schemes, individual and private sector fraud, to the illegal movement of equipment, technology and even knowledge which can be used in the development of weapons of mass destruction. The impact of these activities is alarming. Although no European figures exist, the recently formed UK Serious Organised Crime Agency (SOCA) estimated the economic and social harm caused by organised crime to the UK at upwards of GBP 20 billion a year. Trafficking of class A drugs represented 65 % of this figure. In addition, the global illicit drugs market, measured at retail prices, is higher than the GDP of around 88 % of the countries in the world ([5]).

Terrorism, as evidenced by recent tragic events, is a real and growing threat to Europe. Combating this requires secure information and financial networks, robust secure communications and virtual policing of information infrastructures, including the Internet, to uncover and track terrorist activities. In the current digital age it is increasingly essential 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. With respect to terrorist weapons special attention is required to detect, track, trace, identify and neutralise chemical, biological, radiological, nuclear agents and explosives (CBRNE) — both 'traditional' and 'home grown'. Speed, robustness and affordability will be the driving design parameters for technological and system solutions.

([5]) Source: Office on Drugs and Crime (UNODC), 2003.

Capabilities

More than 100 capabilities have been identified that have an impact on the protection against terrorism and organised crime. The 30 most important capabilities are presented in graphical format in Figure 4 and described hereafter against their relevant functional headings.

Function: Detection, identification and authentication
Detecting and identifying specific dangerous goods (drugs, explosives, viri, and CBRN) are important capabilities. Rapid alerting should facilitate early warning and false alarm rates of existing sensors should be reduced. Stand off detection will allow ease of use. The cooperative (or non-cooperative) detection, identification and authentication of individuals using biometric based systems is a key capability alongside the ability to detect individuals, alone or in crowds, exhibiting abnormal terrorist or criminal behaviour.

Function: Information management
The automated production of intelligence by integrating data from interactive multi-sensors in real time is the central capability required. The massive increase in data volumes, types, quality, structure and format demands automated analysis capabilities. Cultural, linguistic and behavioural aspects affecting the appreciation of data and the ability to automate content analysis to track for instance child porn or terrorist messages are also seen as key. Privacy and data protection capabilities will need to be enhanced in order to ensure data fusion and analysis on this scale does not infringe appropriate regulation. Finally, digital forensic capabilities, to track and trace criminal actions in information networks, are seen as important.

Function: Risk assessment, modelling and impact reduction
Threat assessment models are needed to identify appropriate and targeted countermeasures. Modelling the development of terrorism and crime and the measures to prevent criminal or terrorist networks from expanding is seen as an important enabler. Decision models aimed at identifying cost effective and efficient countermeasures to protect physical structures are perceived to be a high value capability. This would cover protection from all weapons either by redesigning, refurbishing, or adding protection measures. Dispersion modelling of CBRN agents remains an important issue.

Function: Positioning and localisation
Tracking and tracing of (non-cooperative) people, vehicles and substances are crucial capabilities. In addition, capabilities for observation in difficult and complex environments (through walls, water, crowds) are needed. Automated observation and monitoring should be supported with accurate and reliable spatial techniques to identify hazardous substances and objects (like detonators). The integration of new sensors into existing monitoring, access, control or logistic networks will improve widespread and affordable observation capabilities.

Function: Situation awareness and assessment
Situation awareness will require a large improvement in existing command and control centres. The prediction and correlation of events requires the development of domain and scenario-specific models to be used for advanced-warning and target assessment. Mobile robust automated surveillance systems are needed to meet increasing surveillance requirements with respect to coverage and quality.

Function: Command and control
Interoperability and information sharing requirements will mandate the interconnection of different networks. To protect information housed in heterogeneous, decentralised and interconnected networks, new techniques are needed to guarantee their safe and secure use.

Function: Intervention
Intervention capabilities aim to nullify or disarm dangerous individuals, vehicles and delivery systems, for example systems of systems protection of commercial aircraft against man portable air defence systems (MANPADS). For unavoidable incidents, a new generation of resilient clothing and personal equipment is needed allowing hazardous work in adverse environments. Improved forensic technologies and analysis capabilities for both digital and physical crime scene investigation are also important.

Integrated projects

As already mentioned, the risks facing society from organised crime and terrorism are many, varied and costly. Effective protection can be only be achieved by integrating various capabilities, technologies and systems in combination with organisational and procedural improvements. Some examples of such situations where multiple technologies could be integrated and demonstrated are shown in Table 3

	Secure strategic information management	**Mobile security kit**	**Intelligent urban environment observation**	**Secure explosives lifecycle**	**Advanced forensic toolbox**
Objectives	To establish a secure strategic security situation awareness system by automatically combining data from disparate high volumes data repositories and analysing the data to facilitate decision-making. The security of the infrastructure to perform this task is also a key objective.	Mobile security kit for rapid deployment. It can be applied for various situations such as VIP security, event security, sport or show event, as well as for disaster early warning and response in critical infrastructure.	To develop a fast, stand-off behavioural observation system for individuals, platforms and goods in complex (urban) environments to meet surveillance and security tasks including compound security, trafficking of illegal goods and safety monitoring and evacuation.	To address the security of the complete explosives lifecycle from production and trading to distribution. The objective should be to prevent the use of detonators and explosives, both legitimate and improvised using widely available precursor chemicals, being used as terrorist weapons.	To improve the speed, quality, cost, information sharing and tools required for the processing of both physical and digital crime scenes.
Scope	• Automated analysis of complex and different cultural/domain data with multiple reference models • The ability to handle and combine real-time data feeds and historical databases • Secure information systems • The policing of existing information systems	• Development of sets of mobile security modules • Tools for situational awareness and response to incidents in critical infrastructures (transport, drinking water, energy, etc.) • Interfacing with local security forces • Multiple sensors • Tools for VIP protection • General security of events	Integration of sensor technologies, data fusion and intelligent observation systems to enable stand-off detection and analysis: • through barriers (walls, shielding, metal), • of substances (CBRNE, drugs, etc.), • of carriers and people.	• Changing the explosive characteristics of precursor compounds • Tagging, tracing and detecting more readily components and detonators • Smart secure detonators • Secure stockpiling • Use and transport of explosives	European standardisation, best practices and common methodologies for: • the selection of appropriate technologies; • the development of equipment • education; • legal framework; • information exchange; • analysis of forensic information.
Outcome	An automated system capable of fusing and analysing information from financial, demographic, mobility and law enforcement data sources to allow complex conclusions to be generated.	Set of deployable modules that can be selected on the basis of a specific mission.	Both a fixed and man portable wide area system to facilitate detection and analysis of behaviour in an urban environment on a 24/7 basis.	A complete system for the detection, monitoring, secure use and transportation of explosives and detonators.	Two advanced forensic toolboxes (digital and physical) capable of providing rapid, accurate on shareable crime scene processing analysis.

Table 3: Protection against terrorism and organised crime — Integrated projects

Linkages/enablers/constraints

The research proposed within the security and society sections (page 54) of the report will have a direct relevance to this mission.

Foresight studies will assist in the identification of new and emerging security threats whilst societal research will assist in understanding the risk of radicalisation, and consequent recruitment, of individuals from local communities. Both are likely to impact government policy, including that of research and development. Additionally the mission's requirement for widespread observation, coupled with the fusion of distributed data and the sharing of information requires that technologies, equipment and systems be developed that are in line with European **ethical and privacy** values. The research will assist in defining this balance. Finally the research proposed into understanding the **organisational structures and cultures of public users** will have an influence in the orientation in which research and development is both undertaken and demonstrated such that it can be readily applied and introduced by public authority end-users.

Research is not an end in itself. As this report demonstrates, for technology to be effective it must be supported and synchronised with the requisite standards, legislation and societal acceptance. Coherence across all these facets is badly needed and the recommendation to create the **European Security Board** (page 67) is a welcome instrument towards this end.

In parallel to the improvement in the requisite technology solutions new **European legislation** regarding their in-service use will be needed to facilitate the smooth transfer from research to commercialisation. This can be strengthened through the development of **European standards** and **product certification** which will benefit both the economic development and the transnational interoperability of products and services.

The possibilities offered by dual use technology and the economic leverage to be gained from maximising dual use research infrastructure in Europe would benefit immensely from an integral approach. In this respect the proposed technology watch (page 69) covering civil, security and defence technologies is a welcome first step. This should be supported by a **defence and security research policy**.

The integrated projects aim to address specific counter measures for terrorism and organised crime. They represent building blocks towards the larger **demonstration programmes** identified in Section 2.2. The demonstration programmes entitled *'CBRNE'*, '*Logistic and supply chain security*' and '*Security of mass transportation*' have the highest relevance to this mission. Additionally the integrated projects '*First responder of the future'* and '*Built infrastructure protection*' proposed within the crisis management and critical infrastructure protection missions respectively also have relevance for this mission.

MISSION

Protection against terrorism and organised crime

FUNCTIONS

Detection, Identification, Authentication

Information Management

Risk Assessment, Modelling, Impact Reduction

Positioning and Localisation

Situation awareness and assessment

CAPABILITIES (major)

- Drugs, explosives, viri, CBRN detection. Very fast alerting on broad substance type for early warning. After alert more precise checking of type and identification. Low false alarm rates.
- Stand off scanning and detection of hidden dangerous materials and/or stowaways
- Access control. Identification, accreditation and authentication of people.
- Detection and system of systems protection of commercial aircraft against MANPAD attack.
- Access Control Vehicle Identification
- Detection of abnormal behaviour of living beings, platforms
- Data fusion techniques including mining, trend detection and optimization analysis.
- Cultural, Behavioural analysis
- Automated information production
- Digital Forensics, monitoring and acting on digital traces
- Facilitate secure communication facilities between departments and nations
- Automated content analysis to track illegal content
- Semantics, topology development to facilitate semantic data exchange.
- Privacy and Interoperability: sharing information within privacy rules
- Data protection / Integrity, Usage rights
- Automated language, translation
- Develop threat assessment models
- Develop models to describe the creation and evaluation of terrorism and crime
- Develop security and safety kits to temporarily increase protection
- Modelling of criminal networks
- Develop and share dispersion models for contamination
- Develop ballistic, blast, impact reducing measures for existing infrastructure
- Develop protection against contaminants in buildings
- Observation through walls, water, metal etc
- Control of property change of chemicals to preclude misuse
- Marking, tracking, tracing of components for substance production
- Integration of sensor systems with transaction, access, use systems
- Detection of common behaviour characteristics in criminal data
- Prediction Correlation models to generate pre-warning of threat assessment
- Methodologies to recognize automatically criminal behaviour
- Mobile sustained automated surveillance systems•

TECHNOLOGIES (major)

- Chemical and Biological Detection/identification techniques
- Facial, Fingerprint, Iris/ retina, Voice signature recognition
- Cyber security policy management tools
- Explosive Detection sensors
- Image / pattern processing technology
- Micro and mm-wave sensor technologies
- Text mining / data mining
- Knowledge management
- Filtering technologies
- Infrastructure to support information management and dissemination
- Data / Information fusion technology
- Natural language processing technology
- Advanced Human behaviour modelling and simulation
- Impact analysis concepts and impact reduction
- Optimization, Planning and Decision Support Systems
- Data fusion techniques
- Anti Blast glasses/concrete
- Data collection, data classification
- Human Behaviour Analysis and modelling
- CBRN sensors
- Radar sensors
- Cameras
- RFID based tracing
- Electronic tagging systems
- Terahertz sensors
- Nanotechnology for sensors
- Text mining, data mining
- IKBS/AI/Expert techniques
- Optimization and decision support technology
- Autonomous small sensors / smart dust
- Data Fusion
- Image / Pattern recognition

Figure 4

Protection against terrorism and organised crime

– overview diagram of the main functions, capabilities and technologies

Overview diagram

Protection against terrorism and crime

Critical infrastructure protection

Mission scope

Critical infrastructures have been subject to a number of significant challenges over recent years, from legacy millennium bug (Y2K) issues to the growth of terrorist activities. These challenges highlighted that **risk assessment** and its implications have not been well understood by private industry, government bodies or politicians. Furthermore they have served to underscore the importance of such infrastructures and subsequently their protection has become a major worldwide concern. Protecting critical infrastructures is, however, difficult due to the sheer number, diversity and dependencies between them.

Critical infrastructures can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents, computer hacking, criminal activity and malicious behaviour. They cover a **diverse number of physical, logical and organisational systems** from sensitive and administrative buildings, train and subway stations, sensitive manufacturing plants, energy production sites and transmission systems, storage and distribution, to information and communication networks or public events ([6]). Within this diversity, certain critical infrastructures have **direct dependencies** on one another. Failure in one may cause a cascading failure in others. Amongst these, the most critical is the robustness of the power transmission and distribution system due to its underlying operational importance to most supporting critical infrastructure equipment and systems. Increasingly, such critical infrastructure dependencies extend beyond national boundaries and it is these which ESRAB has primarily addressed. Their **transnational impact** is felt operationally when failure occurs (e.g. power outage) but also increasingly commercially, as privatisation transfers ownership of critical infrastructure assets to private industries, most notably in the transport and energy sectors.

A European list of critical infrastructure is currently being established and whilst the total number is, as yet, unknown, it is expected that the number of systems employed by those infrastructures will be in the order of thousands. Enhancing the protection of these across such a diverse range of sectors, albeit it to varying levels, will be challenging. With limited financial resources available to both public and private organisations, solutions must be effective and cost efficient by design. With this in mind ESRAB set about developing a **capability 'toolbox'** in which critical infrastructures sharing similar characteristics were grouped together to ensure maximum leverage from capability development in those areas. The philosophy of 'design once use many times' was thus the driving concept. Critical infrastructure owners and operators should draw upon those capabilities of most relevance to their needs.

Significant research efforts are needed ranging from the integration of mature technologies through to the development of new and emerging security-specific technologies. Where efficient, but costly, technologies exist, research efforts should focus on ways to reduce dramatically the cost for similar performances. Where no technological solution exists, the research effort should emphasise **low cost solutions**.

([6]) To avoid overlap with the border security mission, ports and airports were not addressed by the critical infrastructure mission.

Capabilities

Out of the more than 103 capabilities which were identified as being of importance, 30 have been identified as being priority capabilities for inclusion in Europe's critical infrastructure protection 'toolbox'. The 30 capabilities are presented in graphical format in Figure 5 whilst the ones offering the highest impact are described below under their respective functional headings.

Function: Detection, identification and authentication
Capabilities in this area relate primarily to individuals, vehicles and goods. Preventative detection follows a layered approach starting with the detection of abnormal behaviour of individuals (or groups of individuals), vehicles and goods (in terms of abnormal trajectories followed by the goods) on the outside of critical infrastructures. In certain instances, this must be supported by enhanced capabilities for the rapid detection and identification of unwanted entities in close proximity to critical infrastructures. Critical infrastructure entry points will require the fast, physical or logical identification and authentication of individuals and vehicles/platforms, as well as the detection of dangerous goods including CBRN and explosives. Inside the critical infrastructures, detection of abnormal behaviour capabilities must once again be applied. These include additional capabilities focussing on detection of unattended luggage, with automatic tracing and tracking of the earlier carrier of the luggage and the detection of contaminants carried in supply networks, for example in the drinking water system.

Function: Risk assessment, modelling and impact reduction
Capabilities and tools for risk assessment and response modelling in critical infrastructures are needed. These tools will offer important aids for decision-makers to determine priorities among multiple risk factors, and, in some instances, to model the impact of proposed solutions. In addition, capabilities addressing the protection against cascading ('domino') effects are seen as key. In particular, specific tools to protect large electrical power grids and communication grids against cascading effect by automatic isolation in case of failure of interconnected grids, are required. Finally, capabilities relating to the more robust and resilient design of products for the construction and the service of critical infrastructures require more research. A key capability required in this respect will be the means to shield and protect structures, platforms and networks from high power microwave attack.

Function: Communication
The need for robust and secured communication is ubiquitous across the mission, with a special focus on capabilities for automatic authentication of people accessing terminals and networks, and the monitoring of the network traffic to detect malicious suspicious traffic and identify predefined patterns. Research into more robust encoding, not necessarily cryptography, so as to improve the protection and resilience of communication network from jamming and heavy noise signals is also required.

Function: Command and control
Integrated capabilities are required for the protection of supervisory control and data acquisition systems (SCADA) from attack. SCADA systems are widely used for energy generation, transmission and distribution, in the transportation and water sectors, and for manufacturing. SCADA systems and networks, however, are not designed to withstand attacks.

Function: Positioning and localisation
Capabilities to position, track and trace vehicles, ships, and goods inside open or controlled areas are seen as important in order to protect critical infrastructures. Such capabilities are most important for the transportation of hazardous (or 'sensitive') material both within a nation, region and across the European Union.

Function: Situational awareness and assessment (surveillance)
Supporting those capabilities identified in the detection, identification and authentication function, additional capabilities facilitating the permanent monitoring of the environment, both inside and outside a critical infrastructure, operational night and day and in any weather condition, are seen as being of high importance.

Integrated projects

The threats to critical infrastructures are numerous and diversified, and effective protection can be only be achieved by integrating various technologies and systems aimed at a common protection goal. Some examples of such situations where multiple technologies could be integrated and demonstrated are shown in Table 4.

	Abnormal behaviour detection	**Open space security**	**Water distribution surveillance**	**Protection of rail transportation**	**Built infrastructure protection**
Objectives	Detection of abnormal behaviour of a crowd in an open space. The 'abnormal' aspect refers to the attitude of people and also of vehicles and goods.	Global security of an open space including the surveillance and protection of an open space (a street, a square, a large event, etc.). This project will benefit from the results of the abnormal behaviour detection project.	Surveillance of water distribution network in order to identify new relevant contaminants as well as the detection of chemical and biological contamination and their neutralisation.	Improve the security of rail transportation through better protection of railways and trains, and reduce disparity between European railway systems	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).
Scope	• Definition of the abnormal behaviour that have to be detected (people, vehicles and goods) • Integration of various sensors (video, sounds, chemicals, etc.) • Solutions applicable for short and mid-range distance • Validation	• General surveillance of venue • Multi-sensors for presence and intrusion detection • Identification of unwanted people • Localisation of vehicles and ships • Information system • Validation	• Design of methodology to identify new relevant contaminants • Modelling of impact of contamination (preventive and real-time) • Integration of various sensors for chemical and biological detection, in a surveillance system • Tools for neutralisation • Validation	• Detection of abnormal objects on or under ballast • Clearance of trains before daily use • Control of access to drivers' cabin; detection of unauthorised driver • New methods and tools to isolate and secure luggage • Study and tools to reduce disparity of European railway systems' security	• A system 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 must be made feasible
Outcome	Signature of specific abnormal behaviour and advanced integrated technology for the detection of abnormal behaviour. Roadmap for additional research	Set of integrated tools for total surveillance of an open area.	Better prevention of water distribution, with a methodology to identify new contaminants, and better protection, with tools to identify and neutralise an attack.	Better protection and homogeneity of the European rail transportation systems.	The development of a suite of protection portfolios for new and existing building that are operationally viable, infrastructure-specific and affordable.

Table 4 : Critical infrastructure protection - Integrated projects

MISSION

Critical infrastructure protection

FUNCTIONS

Situation awareness and assessment

- Permanent monitoring of environment, night and day, all weather
- Produce domain specific prediction models to facilitate pro-active intervention

Positioning and Localisation

- Localisation and tracking of goods in an area
- Alternate navigational aids in case of major GPS failure

Risk assessment, modelling and impact reduction

- Tools to protect main electric power grids against cascading effect
- Tools to protect main communication grids against cascading effect
- Modelling tools for risk assessment and response models for critical infrastructures and service
- Assessment tool to identify vulnerabilities to cascading effect of power grid
- Assessment tool to identify vulnerabilities to cascading effect of communication networks
- Design more robust and resilient products for construction of critical infrastructures
- HPM shielding for structures, platforms, and networks

Communication

- Monitoring of network traffic, identification of suspicious traffic
- User authentication for terminal and network access
- Physical integration of C4 equipment and interface with carrying platforms
- End-to-end interoperable secure communication infrastructure and service
- Detection and identification of fraudulent control
- Load balancing mechanisms (related to telecommunication networks
- Protection against heavy noise, jamming)

Detection, Identification and Authentication

- Stand-offs scanning and detection of hidden dangerous material
- Detection of unattended goods and of owner
- Detection of abnormal behaviour of people (from single to groups)
- Detection of abnormal behaviour of vehicles and goods
- Identification of searched individuals in a crowd
- Detection/identification of water contamination
- Remote detection of illicit access to pipelines
- Detection of ill and/or infectious people
- Intruder detection in an area
- Vehicle identification (type, plate)
- Secured access control

CAPABILITIES (major)

- Various set of sensors
- Data fusion
- Smart video surveillance

- Electronic tagging
- Device integration/reliability
- Radio navigation
- Direction finding and map guidance

- Alternative power sources and devices
- Early detection techniques
- Protocol technology
- Simulation for decision making
- Structural and smart materials
- EMC evaluation and hardening

- Pattern recognition
- Text and data mining
- Biometrics
- Communication and Information System security equipment
- Information security
- Filtering technologies
- Network management and control
- Protection against hash environment

- Explosive detection
- CBRNE detection
- Visible and IR cameras
- Radars
- Hyper spectral and multi spectral sensors
- Motion sensors
- Biometrics
- Pattern recognition
- Smart video surveillance

TECHNOLOGIES (major)

Figure 5

Critical infrastructure protection

– overview diagram of the main functions, capabilities and technologies

Overview diagram

Critical infrastructure protection

Linkages/enablers/constraints

The identification and authentication of individuals is the most common function required for the protection of critical infrastructures. Almost all proposed solutions to address the requirements of this function are based on the use of **biometric technology**. Implementation of biometric technology has often raised concerns, and its use is controlled by several special regulations.

The research proposed under the security and society section (page 54) will play an instrumental part in guiding the research and development within this mission area. The **ethics and justice** section should provide a rounded and clearly articulated view as to an appropriate balance between security technology application of citizen's privacy thereby guiding policy development in this important. The section on **citizens and security**, aims to undertake research into individual and crowd behaviour. Such research aims to detect abnormal behaviour and the optimum means to realign the situation. Clearly there are strong links between, and impact upon, technology development in this area. The section **security economics**, aims to study the impact of insecurity from an economic perspective and to objectively determine where investments and policy should best directed, including for critical infrastructure.

The sheer number, diversity and (inter-) dependencies of critical infrastructures across Europe points to the need for efficient and affordable solutions which should be met by a globally competitive European technology supply chain. In order for this to be achieved appropriate **European standards**, and in some instances their **certification**, shall be required. In this respect a strong relationship between policy developers, industry and the European Committee for Standardisation (CEN) is seen as a key enabler.

From the perspective of a critical infrastructure operator, the impact on their business model of implementing additional security solutions will almost certainly be negative, especially in view of the highly competitive environments in which they operate. Appropriate **financial support,** or **regulation** preserving the competitiveness of critical infrastructure operators, is seen as an essential enabling element for effective implementation. In this respect the work on-going within the Commission (DG JLS) is welcomed and should be supported.

The integrated projects identified earlier aim to address specific border security needs, but represent building blocks towards the larger **demonstration programmes** identified in Section 2.2. The demonstration programmes entitled *'Logistic and supply chain security'* and *'Security of mass transportation'* have the highest relevance to the critical infrastructure protection mission.

Restoring security in case of crisis

Mission scope

Modern crises are progressively changing their character from 'predictable' emergencies capable of being countered with existing crisis management tools and techniques, to unpredictable catastrophic events for which governments and first responders require new, innovative and affordable solutions. Progress is needed on at least two fronts — ensuring governments, first responders and societies are better prepared prior for an incident, and in parallel, improving the tools, infrastructures, procedures and organisational frameworks to respond and recover more efficiently and effectively both during, and after, an incident. Improving national competencies in this area is aimed primarily at meeting the needs of European citizens but will also benefit international communities by virtue of the assistance provided through the Community's civil protection mechanism.

Improvement in crisis management capabilities are required to address three clear areas.

Terrorism and crime is on the increase — the 15 worst terrorist attacks, in terms of casualties, have occurred since 1982 and of these, more than 80 % have taken place within the last 10 years ([7]). The terrorist attacks in Madrid and London are vivid reminders. Most attackers utilise conventional explosive weapons, however, in the future, weapons of mass destruction and disruption (e.g. CBRN) could be employed. Human and economic losses could rise steeply adding significant complexity and scale to the required responses of governments, first responders and public health systems.

Natural disasters, including pandemics, have equally seen a marked increase over the last decade, resulting in severe loss of life, property, and damage to the environment. The lives of millions of civilians are at risk each time an earthquake, hurricane or other natural disaster occurs, and this is exacerbated in poor countries with less developed infrastructures, high and vulnerable population densities and inadequate emergency preparedness. Hurricane Katrina proves developed nations are by no means exempt from these ravages and the outbreak of avian flu in parts of Europe poses the threat of a new influenza pandemic, similar to the Spanish flu of the last century.

Major industrial accidents/technological disasters can have a significant effect both locally and further a field. No better example exists than the Chernobyl nuclear accident of 20 years ago in which the whole of Europe was affected. Similar examples exist, although not on the same scale. The explosion of a fertiliser chemical plant in Toulouse 2001, the oil-pollution from the tanker Prestige which affected France, Spain and Portugal in 2002, and last year's oil storage terminal explosion in Hertfordshire (UK). Effects of this kind of disaster can be far reaching and, though the onus must lie with each industry to put in place its own contingency plans to deal with emergency scenarios, in some instances external, or even international, assistance may be necessary.

([7]) http://www.oecd.org/dataoecd/19/2/33947990.pdf

Capabilities

The analysis of the requirements to satisfy this mission has led to some 98 capability disciplines being identified. Of these 33 have been identified as having prime importance and are shown in figure 6. However, although new technologies will be helpful in some areas, for example to aid command and control functions and search techniques, much of the research and thought in this area will involve practical experiences and analytical skills to establish and construct the organisation, concepts and operating procedures for emergency crisis management. Achieving agreement from national and international emergency agencies to standardise equipment and operating procedures for ease of interoperability and flexibility will require considerable effort. Similarly, producing best practice from 'lessons learned' will take time.

Function: Doctrine and operations
The design and construct of the whole leadership chain and crisis management organisation will be paramount. Additionally, a best practice exchange network on both global and European levels will enable an effective 'lessons learned' process and lead to additional flexibility, interoperability and responsiveness. Readiness will be further enhanced through **training and exercises** involving the use of realistic modelling and simulation tools in dedicated facilities. Target audiences should principally be crisis managers and first responders although this should also be extended to citizens to enhance their ability to assist themselves, and consequently reduce the burden on authorities, during a crisis.

Function: Command and control
To enable effective command and control, **information management**, intelligent decision support including comprehensive contingency planning scenario checklists, a common operational picture, efficient and interoperable **communication** and message exchange at all levels (warning, alerting, reporting and command functions) and public information will all be crucial to support the crisis management teams and decision-makers.

Function: Situation awareness and assessment
Situation awareness is critical to all steps in crisis management. Sensors and rapid information acquisition to compile and update a common operational picture and to aid **risk assessment** and scenario development will be fundamental to the decision-making process. This will include the integration and fusion of data gathered from a wide array of sensors including space, air, land, sea, and personnel. Software planning tools, modelling, rapid and flexible map production and clear presentational displays will be essential.

Function: Incident response
Effective incident response must be rapid, accurate and where possible use pre-planned check lists customised for relevant scenarios. The incident response cycle will be enhanced by custom built transportation to facilitate rapid response and rescue operations. It must include advanced personal equipment both for first responders and civilians alike (e.g. smart suits and protective coverings). Comprehensive logistic contingency plans for the use of air, sea and land transportation fleets to enable a rapid response, inside and outside the EU, should be drafted. Capabilities for dispersal assessment, decontamination and **neutralisation** or containment of the threat, basic service restoration (energy, water, communication, commerce, etc.), and temporary rehabilitation will also be essential.

Function: Detection, identification and authentication
The detection, identification and authentication of people (wounded, buried alive, ill, deceased or infectious) and dangerous substances (explosives, CBRN, contamination, germs or viri, pollution) including field epidemiology will be necessary. Accurate **positioning and localisation**, reporting and tracking of events and personnel will be important to facilitate effective command and control of aid relief, emergency services, and personnel movements in devastated areas and to contain the spread of contamination and effect.

Integrated projects

The tasks at a large incident are numerous and diversified, and effective crisis management will require a careful integration of planning, organisation, resources, capabilities and technologies. Some examples of such situations where multiple technologies could be integrated are shown in Table 5.

	Network enabled command and control	**First responder of the Future**	**Specialist search and rescue capabilities**	**Post incident basic service restoration**	**European crisis management network**
Objectives	Develop network enabled capabilities for effective command and control of the Emergency Crisis Management Organisation (ECMO).	Enhance the operational effectiveness and capability of first responders and reduce injury or loss of life among first responders and the civil population.	Improve the ability to locate, assess, and rescue, injured and/or contaminated victims in a CBRNE or natural disaster environment.	Improve the ability to deploy and/or rectify basic services (energy/water/communications) after an incident and repair infrastructure and lines of communication	Develop European crisis management training, doctrine and tools. Facilitate efforts to exchange lessons learned and best practice of European crisis managers and first responders.
Scope	Widespread networking has the potential to provide significantly improved access to timely and relevant information to all crisis managers and first responders and to assist in the production of a common operational picture. The project should focus on: • national and international operating procedures; • organisational structures; • information acquisition and management; • decision support; • interoperable communications; • flexibility in planning and execution of operations.	Holistic view to be taken for the project covering: • operational effectiveness; • innovation in equipment and protection of first responders, improving and monitoring of performance and health; • sensors and communication equipment, providing facilities for collaboration at a distance; • procedures and tactics: address decision-making though CROP; • training and cooperation: design training for modern operations.	Research and development in particular should focus on: • detecting buries people; • the use of sensors (acoustics, radars, video streaming, etc.) to enhance situation awareness; • on-site monitoring of damaged structures and the environment; • the ability to transmit, receive, and display data from specialist centres (command and control); • mobile extraction equipment; • biotechnological and medical counter measures; • rapid decontamination.	Research should initially address mobile, scalable micro power grids to provide emergency electric power for key installations and first responders including: • integrated distributed power; • scalable power grids with the capability to connect different power sources; • hardened for operating in harsh crisis management environments; • intelligent power management to prioritise supply — communications, command and control, medical facilities, pumps, etc.	Develop common operational concepts and procedures to facilitate interoperability and effectiveness including: • lessons learned — covering knowledge and experience — positive or negative — derived from actual incidents; • best practices — covering procedures, good ideas, or solutions that have evolved and should be regularly updated from actual experience; • production of operating manuals subject to regular modification.
Outcome	Portfolio of network enabled capabilities to provide a step change improvement in the effectiveness and efficiency of emergency crisis management	Integrated protection systems, equipment, procedures and training methods to improve the performance and security of first responders.	A compatible, effective and efficient set of systems and equipment for the location and rescue of victims in CBRNE or natural disaster environments.	An integrated mobile rapidly deployable micro-power grid and intelligent power management system.	Crisis management handbook of standardised and comprehensive operating procedures. Supporting portal for best practice exchange.

Table 5: Restoring security in case of crisis — Integrated projects

Linkages/enablers/constraints

Much of the research proposed within the security and society section (page 54) of the report has direct relevance to this mission. In particular, the most effective manner for authorities to **communicate with citizens and communities** before, and during, a crisis as well as the key role to be played by the media. All research activities proposed under **'understanding organisational structures and cultures of public users'** also has direct relevance to an effective and efficient crisis management response.

Standardised and interoperable equipment for first responders is essential. As assessment of the current status in Europe shows much more needs to be done, in particular to integrate wired and wireless communication systems. Communication systems are of vital importance to first responders which must be able to seamlessly and dynamically interconnect multiple agency users, who have multiple functions, and multiple information and communications technology systems. The projects '*Network enabled command and control*' and '*First responder of the future*' aim to address this shortfall. The Committee of European **Standardisation** will have a key role to play in this respect.

Sensor information and accurate global positioning are necessary ingredients in building situational awareness for timely and effective command and control, and for the monitoring of resources and personnel and communication relay. In this respect, the **global monitoring for environment and security** (GMES) services offer an effective tool to both national and European crisis management authorities.

The report earlier highlighted that much of the research and thought in the crisis management area will involve practical experiences and analytical skills to establish and construct the organisation, concepts and operating procedures. There is of course already much work done nationally, and this should not be reinvented. **Advantage should be taken of the networking and transparency mechanisms** proposed in the coordination (page 57) and innovation sections of the report (page 71). The aim should be to exchange best practice, standardise operating procedures and equipment and perhaps, in time, develop poles of excellence for key crisis management activities. The '*European crisis management training*' integrated project will be the first step in this direction.

The integrated projects identified earlier aim to address specific crisis management needs, but represent building blocks towards the larger demonstration programmes identified in Section 2.2. The demonstration programmes entitled '*Aftermath crisis management system*' and '*CBRNE*' have the highest relevance to the crisis management mission.

MISSION

Restoring security in case of crisis

FUNCTIONS

Doctrine and operations/ Training and exercises

Command and Control/ Information management/ Communication

Incident response/ Intervention and neutralisation

Situation awareness and assessment (surveillance)/ Risk assessment, modelling and simulation

Detection, identification and authentication/Positioning and localisation

CAPABILITIES (major)

- Tasks, responsibilities and organisation. Establish international/ national/ regional headquarters and Leadership Chain, Organisational interoperability (cross organisation and cross boundary) – procedures and responsibilities
- Contingency plans/ concepts/ operating procedure.
- Information exchange platform for best practices
- Develop training, education and simulation facilities.
- Education and training for people (e.g. Crisis managers, first responders, resource directors, citizens)
- Operational cooperation through developing interchangeable capability units
- Develop common operational picture between departments, nations, first responders etc.
- Warning and Alerting and response coordination: communication, message and information exchange at all levels (local, regional, national, international, EC)
- Intelligent decision support
- Robust and reliable (secure when necessary) communication and message exchange at all levels.
- Interoperability of data, systems, tools and equipment
- Public information: Develop a media strategy for dealing with large scale incidents utilizing the full spectra of media coverage.
- Personal equipment (e.g. for first responders)
- Emergency medical care in all phases: application by first responders and medical teams included security zones, transport and hospital transfer.
- Emergency equipment: Emergency Power Generation, Temporary shelters, Specialist rescue equipment
- Neutralization of devices/effects: containment (limitation) of effects of terrorist device on the environment, including explosives, CBRN and firearms by isolation, shielding etc..
- Basic service restoration (e.g. energy, water, communication), business continuity, domestic/ environmental normality.
- Decontamination: Water Purification/ de-pollution sites and large areas/ decontamination of people, large area.
- Information acquisition – UAVs/ Dedicated platforms/ Remote/ Balloons and satellite
- Rapid and flexible mapping production.
- Scenario development & modelling for hazard prediction and contingency planning
- Integrated sensor fusion
- Detection of people (i.e. wounded, buried alive)
- Detection of ill and/or infectious people (fever, infection, behaviour, etc.)
- Detection and identification of dangerous materials – drugs, explosives, Viri, CBRN
- Tracking of containers/goods/ aid relief in wide open areas
- Land wide area – positioning and tracking of personnel movements, emergency service in wide areas relatively uncluttered but over difficult terrain

TECHNOLOGIES (major)

- Operational Analysis tools and techniques
- Task analysis modelling and scenario analysis
- Infrastructure to Support Information Management & Dissemination
- Evacuation and consequence management techniques
- Individual and team training
- Advanced Human behaviour modelling and simulation
- Mission simulation
- Skills training systems
- Tactical/Crew training systems
- Communications network management and control equipment, network supervisor
- Optimisation, Planning & Decision Support systems
- Human factors in the decision process
- Infrastructure to Support Information Management & Dissemination
- Web and language technologies
- Smart clothes and equipments
- Decontamination techniques
- Biological technologies for biological and medical countermeasures
- Human survivability, protection and stress effects
- Apt models (e.g. atmospheric dispersion or epidemiological models) to support preparedness exercises and actual crisis response
- Data collection/data classification
- Advanced image and geo-spatial analysis technologies
- Image/pattern processing technology
- Information fusion technology
- Data and information management technology
- Prediction of mass behaviour
- Optimisation, planning and decision support systems
- Sensor technologies
- Navigation technologies
- CBRN sensor, in particular biological and chemical threat detection technologies
- Chemical and biological detection techniques
- Explosive detection sensors

Figure 6

Restoring security in case of crisis

– overview diagram of the main functions, capabilities and technologies

Overview diagram

Restoring security in case of crisis

Section 2.2

Cross mission area analysis

Integration, connectivity and interoperability

For each of the four mission areas integration, connectivity and interoperability plays a very specific enabling role both within, and between, missions. The purpose of this section is to draw attention to, and in some instances expand upon, those common issues of importance mentioned within the mission areas. For ease of readability, they have been grouped into three areas — information representation, interoperable secure communications and access control and authentication. In each standardisation, both European and international, is likely to play a key role.

Information representation

The monitoring of threats, events or critical infrastructures produces a wide range of information in the form of data which is subject, in many instances, to coding against a particular data format. Such data is carried across different networks using various technologies. There is a pressing need to define **common standardised data formats** to ensure information coding permits data exchange between people and systems.

It is, however, impractical, and therefore unlikely, that large amounts of data would be retrospectively codified against a common standard for interoperable representation of the information (e.g. common formats, common data model) or even against a common language with the difficulties of achieving a common understanding of nomenclatures across the EU. A more practical approach would be to adopt a common interchange standard for data, either bilaterally between stakeholders or preferably for the EU as a whole. **Gateways and/or translator units** would be used as necessary to convert formats and protocols as required.

Such translators and gateways, where information is formatted in a structured manner, require common data models in order to simplify and automate the translation process. Research into how semantic interoperability could be defined and applied would be valuable. Their definition will, however, be challenging since more than **80 % of the world's database content is in unstructured largely textual format.** The benefits are, however, clear. Commonly formatted data strongly lends itself to the application of data fusion, data mining and information processing techniques — releasing and combining the relevant data would provide a significant improvement to situation awareness across all relevant stakeholders. The following technologies were identified in support of this capability:

- network and protocol independent secured communications;
- protocol technologies;
- data and information management technology (databases, etc.);
- COTS software assessment;
- communications network management and control equipment, network supervisor;
- infrastructure to support information management and dissemination.

Interoperable secure communications

In terms of interoperability, the ability to rely on interoperable communication mechanisms is a key basic enabler across all missions. The ability to **exchange voice and data on demand**, in real time, when needed and to command and control resources across a range of situations and departments is essential. Great progress has been made, but there is much more work to be done. Across Europe there are still too many situations where the various stakeholders, or different services within countries, make use of communication mechanisms that are not end-to-end interoperable. Addressing this issue is critically important and can be achieved in two ways. First is the development of appropriate communication gateways that support the various necessary communication protocols and translate from one to another. Second, the development of new technologies that can be widely adopted in a migration phase from the current mechanisms to the new ones, over the longer term.

End-to-end interoperable communications is the basic foundation for **robust and effective communication** between departments but, in some instances, departments must also ensure that those communications are secured. This

applies to the communication infrastructure itself and the information /data flows. Security mechanisms will need to be developed and deployed on top of the existing communication infrastructure to ensure end-to-end, network independent and secured communications. The protection of the communications infrastructure and the challenges linked to the integrity of the infrastructure components and its management will be key aspects to consider.

The following technologies were identified in support of this capability:
- protocol technologies;
- communications network management and control equipment, network supervisor;
- information security;
- SW architectures;
- network and protocol independent secured communications;
- software-defined radio;
- communication and CIS security equipment;
- infrastructure to support information management and dissemination;
- human factors in the decision process;
- access control;
- encryption, encryption technologies (cryptography) and key management;
- mobile secured communications;
- high integrity and safety critical computing.

Access control and authentication

One of the frequent references, across all mission areas, is the importance of access control to facilities, areas, systems and information. At the heart of access control is **an inherent trust between the parties**. Robust access control and authentication models are required for the sharing and exchange of information, particularly those relating to sensitive data.

Controlling access requires the identification of the accessing entity and thereafter positive confirmation that the claimed identity is correct (i.e. authentication). For this reason access control and authentication need to be closely linked in deployed solutions. **Speed is the driving factor for authentication** and information management techniques, database design and high speed communication bandwidths will all figure strongly in final solutions. Authentication speed is also affected by the chosen method of identification which varies considerably depending on the entity requesting access — be that an individual, system or application. Each will have different requirements affecting their technological solutions and consequently affect interoperability and design parameters.

By way of example biometrics is viewed today, and increasingly so, as the solution of choice for the identification and authentication for individuals. For widespread deployment of biometric-based solutions for identification and authentication interoperability between biometric data readers and their corresponding authentication databases is of critical importance.

The following technologies were identified in support of this capability:
- effective and easy-to-use biometric technologies (e.g. facial recognition, iris/retina, fingerprint, etc.);
- two-factor authentication technologies for IT and network access;
- distributed trust models and technologies;
- access control models and technologies for distributed environments.

Capabilities and technologies

The mission-oriented sections describe the required capabilities and technologies to meet the most pressing security needs. These are a combination of both mission-specific and multi-mission entries which allow the mission requirements to be read in a stand-alone manner.

In order to gain an insight into the required multi-mission capabilities these have been extracted from each of the missions and are presented in **Table 6**. Clearly, they do not represent an exhaustive view of all multi-mission capabilities but rather a filtered list of the most frequently requested entries across the 11 functional groupings.

Similarly an appreciation of the most important technology areas is presented in **Table 7**, taking an overview across all missions and mapping the technologies proposed against the broad technology taxonomy domains. On average the four highest priority technologies per domain have been identified with the list descending in priority order.

It is unsurprising to see information and communication technologies figuring so highly in the table. Technologies for gathering, storing, processing, displaying, using, communicating, and managing information — sensory, temporal, geographic, environmental, situational, status — are becoming pervasive and are revolutionising the manner in which organisations (both public and private) are able to address their security needs. With respect to these transversal technologies the report aims to register their relevance to the security programme without seeking to necessarily develop them through the future security research programme. They represent key technologies required to be integrated into various systems in order to deliver security mission requirements. These technologies should therefore act as a key reference source to other programme constructors at European, national and industrial levels.

Detection, identification and authentication
Intervention and neutralisation
Risk assessment, modelling and impact reduction
Situation awareness
Training and exercises
Command and control
Communication
Doctrine and operations
Incident response
Information management
Positioning and localisation

Table 6 — High frequency multi-mission capabili

Detection of explosives, weapons, drugs, dangerous goods (CBRN), platforms, living beings
Detection of abnormal behaviour of living beings, platforms
Access control via biometric identification and authentication
Incapacitating platforms, individuals and weapons
Isolating individuals, and groups of individuals, through proactive and preventative crowd control
Neutralising the effects of a CBRNE incident
Threat assessment modelling
Risk assessment and response models, for complex or integrated infrastructures and services.
Modelling of the modus operandi of organised crime and terrorism
Collecting or extracting data and finding patterns and correlations to indicate a specific hazard
Presentation of data in manner which aids human decision-making processes
Continuous capture of surveillance data including from remote platforms
Improve front line skill levels through training initiatives such as scenario and situation modelling, computer aided training, and simulation
Improve Education of citizens on the manner in which to behave in case of crisis
Test and audit of front line staff and facilities
Common operational picture shareable between all stakeholders via robust command and control systems, mechanisms and tools
Information management — public information broadcasts/media
Alerting and broadcasting of abnormal behaviour in a timely, consistent and directive manner
Tools and systems to facilitate intelligent decision support
Physical integration of command, control and communication equipment and interface with portable platforms
End-to-end interoperable secure communication infrastructure and services
Fixed and mobile terminal and network access control via user authentication
Assess and realise back-up or redundancy capacity for selected infrastructures and services
Produce customised contingency recovery plans for institutions and major strategic facilities
Develop guidelines and procedures for designing, monitoring and responding to man made or natural disaster incidents
Decontamination of individuals, platforms and infrastructures post attack
Personal protection and equipment for first responders and civilians
Forensics for faster trace testing of chemicals, explosives CBRN on humans and objects.
Basic service restoration and robust business continuity systems
Capabilities to provide data fusion/data mining/automatic information processing
Ability to interrogate unstructured database repositories
Semantics and topology development to facilitate data exchange
Identification, localisation and tracking of platforms, goods, containers, people, emergency services and inventories
Observation of individuals through sub terrain, debris and fixed structures

ties

Technology domain	Priority technology areas
Signal & information technologies	Data fusion techniques, data collection/data classification, image/pattern processing technology, information fusion technology, data and information management technology (DB, etc.)
Artificial intelligence and decision support	Text-mining/data-mining, IKBS/AI/expert techniques, knowledge management, modeling and simulation, optimisation and decision support technology
Sensor equipment	Cameras, radar sensor equipment, NRBC sensors (in particular biological and chemical threat detection technologies), passive IR sensors equipments
Sensor technologies	Hyperspectral/multispectral sensors, hyperspectral/multispectral processing, autonomous small sensors/smart dust technolologies, IR sensor technologies, Terahertz sensors, optical sensors technologies, acoustic sensors — passive
Communication equipment	Reconfigurable communications, mobile secured communications, communications network management and control equipment, network supervisor, network and protocol independent secured communications, information security, secured, wireless broadband data links for secured communications, protection of communication networks against harsh environment
Human sciences	Human behaviour analysis and modeling, population behaviour, human factors in the decision process, teams, organisations and cultures
Information security technologies	Encryption and key management, data-mining, access control, filtering technologies, authentication technologies, encryption technologies (cryptography)
Computing technologies	Protocol technology, SW architectures, secure computing techniques, high performance computing, high integrity and safety critical computing, software engineering
Information warfare/intelligence systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Scenario and decision simulation	Impact analysis concepts and impact reduction, advanced human behaviour modeling and simulation, simulation for decision making (real time simulation), structures vulnerability prediction, evacuation and consequence management techniques, mission simulation
Information systems	Infrastructure to support information management and dissemination, cyber security policy management tools, optimisation, planning and decision support systems
Navigation, guidance, control and tracking	RFID tags, tracking, GPS, radionavigation, direction finding and map guidance, bar code based tracing
Forensic technologies — biometry	Fingerprints recognition (digital fingerprints), facial recognition, iris/retina, voice, handwriting, signature reconnaissance
Integrated platforms	UAVs (air/land/sea), lighter than air platforms, surveillance and navigation satellites
Survivability and hardening technology	EMC evaluation and hardening, smart clothes and equipment, anti-blast glasses/concretes, etc., critical buildings specific architectures, blast and shock effects
Electronic authentication	Electronic tagging systems, smart cards
Biotechnology	Rapid analysis of biological agents and of human susceptibility to diseases and toxicants, decontamination techniques, water testing and purification techniques, food testing and control techniques
Simulators, trainers and synthetic environments	Virtual and augmented reality, tactical/crew training systems, command and staff training systems, synthetic environments
Chemical, biological and medical materials	Chemical and biological detection techniques
Signal protection (warfare)	Non-cooperative target recognition, geographic information systems
Space systems	Earth observation (image and communications)
Light and strong materials, coatings, …	Light materials for human protection, smart textiles, light materials for site protection, self-protective and explosive resistant material technology, surfaces treatments for improvement of life duration, corrosion reduction
Energy generation storage and distribution	Electrical generators, electrical batteries, energy distribution

Table 7 — Priority technology areas by technology domain

Demonstration programmes

The methodology section (page 18) describes, through three paths, the type of research which should be conducted. The third of these paths, systems of systems demonstration, aims at integrating a number of systems to achieve multi-mission objectives. In a certain sense these multi-mission systems of systems programmes could be viewed as European flagships providing a federative frame to coalesce research in areas of significant European interest.

Their successful achievement will depend on the compatible, complementary and interoperable development of the requisite system and technology **'building blocks',** some of which will themselves add value to many demonstration programmes. Many of the projects proposed in the mission sections show a clear link with the overarching demonstration programmes and are the first steps in addressing the required 'building blocks'.

So as to ensure that each demonstration programme is clearly described in terms of the required capability and system 'building blocks', **ESRAB recommends a support activity be awarded to define the strategic roadmaps required for each of the demonstration programmes**. Such roadmaps should take into account completed, ongoing and planned work in each area and lay out, in a coherent and clear manner, the further work required.

The following demonstration programmes are proposed:

Aftermath Crisis management system

Scope

Large-scale incidents require a coordinated response from crisis managers and first responders from different agencies across the EU 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 in the CBRNE programme, in particular for decontamination, should be leveraged.

Improvement and demonstration areas

- Interoperable secure communication systems based on software defined solutions
- Robust and scaleable 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 the EU
- 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).

Outcome

An integrated and scaleable crisis management system capable of providing comprehensive situational awareness to decision-makers to ensure a timely, coordinated and effective response to large-scale disasters both inside and outside the EU.

European-wide integrated border control system

Scope
In the fight against terrorism and organised crime the security of Europe's external borders is essential. An integrated border management system encompassing surveillance, monitoring, identity management, and advanced training methods/tools is required. It should link strongly with the demonstration programmes of '*CBRNE*' and '*Logistic and supply chain security*'.

Improvement and demonstration areas
- Surveillance systems to improve situational awareness and detect anomalous behaviour of people and platforms (vehicles, boats, aircraft)
- Identity management systems including documentation, equipment and supporting databases to accurately identify and authenticate individuals, goods and platforms
- Information management systems to fuse data from disparate systems (identity management, intelligence, etc.) in order to improve decision-making
- Secure communication systems for improved cooperation between national and international border control authorities
- Positioning and localisation systems to track and trace individuals, goods and platforms
- Advanced training methods, tools and systems based on true representation simulation systems
- Improved architectures, processes and systems for border security including extending the legal borders to departure points outside of the EU perimeter

Outcome
A comprehensive and integrated border management system capable of providing concentric layers of protection from pre-entry control measures to cooperation inside, and between, Member States. To be effective, widespread deployment is required, for which innovative business models will be needed.

Logistic and supply chain security

Scope
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 goods 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.

Improvement and demonstration areas
- 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
- Modernisation 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.

Outcome
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.

Security of mass transportation

Scope
Mass transport is of prime economic and strategic importance for Europe. A large demonstration programme to secure transport networks, nodes and platforms is required. Prevention through improved surveillance and detection systems should be augmented with post event analysis systems and threat neutralisation systems and capabilities.

Improvement and demonstration areas
- Surveillance systems designed to meet specific requirements for mass transportation networks, transfer nodes and platform interiors
- Interoperability of different surveillance systems managed by different operators and/or between different EU countries
- Comprehensive threat detection systems fusing data across diverse and distributed networks and analysing threats via spatial/pattern recognition techniques. Detecting, tracking and tracing individuals, crowds and objects within, and across, transport systems
- Post-event situation analysis systems capable of rapidly accessing and piecing together different multimedia and digital data to re-enact a sequence of events
- Common operational picture integrating and displaying data from a diverse set of sources on optimised man machine interfaces utilising intelligence based alarm management
- Neutralisation and containment systems for attack avoidance, suppression or nullification.

Outcome
A consistent and integrated suite of mass transportation security systems taking into account the specific requirements for each sector and the particular cross-border dimension of mass transport. Interoperability requirements will drive standardisation in this area.

CBRNE

Scope
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
- 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.

Outcome
A consistent portfolio of counter measures for CBRNE along the phases 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.

Section 3

Security and society

While seeking effective measures to provide security for its citizens, the European Union and its Member States must be cognisant that security, whilst very important, is just one of the societal values in Europe which must be balanced against others. As members of the EU, the Member States have all signed up to the European Convention of Human Rights and promoting the values of human dignity, freedom, democracy, equality, the rule of law and respect for human and minority rights. The political challenge is, and will continue to be, **striking a socially acceptable balance** between these different values which will need to take account of variances between countries, circumstances and the development of threats and their perceptions.

Technology is an important tool in preventing, responding, managing and mitigating potential threats to European societies. However, as the GoP report highlighted, security technologies are only part of the effective response to security threats and security challenges and **must be applied in combination with organisational processes and human intervention** — themselves based on the shared European values outlined above.

As Figure 7 shows, changes in one leg of the security triangle has consequences for the other two. By way of example, new technology will inevitably lead to changes in how we organise activities and how humans react to uncertain situations. On the other hand, the effectiveness and legitimacy of technology will depend on the human activity that is associated with its use. The overall system is only as robust as its weakest link, and in meeting security needs, human and organisational aspects have proven themselves, on frequent occasion, to be the weakest links. It is therefore recommended that, where appropriate, technical research and development projects awarded under the future security research programme should be evaluated against the criteria of how well they take into account the triangle of mutual dependency of technology, organisational dynamics and human limitations.

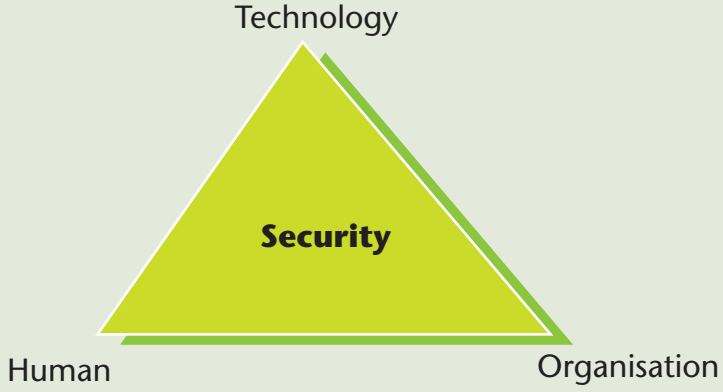

Figure 7 – Triangle of mutual dependency

Noteworthy is the fact that the human aspect, in particular, will mandate that a single **'one size fits all'** European solution **cannot be made to work.** Europe is a collection of 450 million people spread across 25 nations each with their own rich tapestry of history, experience and approaches to life. This aspect in particular has been an underlying assumption running across the areas identified for research. Technological research and development must therefore be strengthened, and when appropriate integrated, with research into political, social and human sciences. Five areas are identified: **citizens and security, understanding organisational structures and cultures of public users, foresight scenarios and security as an evolving concept, security economics** and **ethics and justice**. Only with due respect to these factors will European security research be sure to lead to solutions adaptable to European diversity. Furthermore, such ability to deliver security solutions **adaptable to diverse cultural and institutional settings** may also become a key success factor for European exports.

The following section outlines the required research to be undertaken in support of each of the key areas identified. It uses as its foundation the security research definition defined on page 18 and therefore does not address research into the 'root causes' of insecurity which is already foreseen to be undertaken within the '*Socioeconomic sciences and the humanities*' thematic area of FP7.

Citizens and security

Enhancing security of the European citizen is at the very core of European security research. Therefore, it is important to consider the particular relationship between citizens and their security and its impact on research priorities. From this perspective, the key issues to be addressed include citizens' perception of security and insecurity, communication and instructions between authorities and citizens in crisis and normal situations, and finally understanding terrorist behaviour, radicalisation and recruitment in EU Member States.

These topics are important to be addressed within the European Security research in order to ensure that the selected policies and security technologies are responsive to the needs of citizens and that they create **security approaches rooted, and accepted, by society** and its citizens. Deeper knowledge with respect to the individual citizen's and public perception of security and insecurity helps in the selection of the appropriate technology and other measures, leads to a higher level of perceived security and fosters the emergence of a European security culture.

Research into improving the **understanding of people's behaviour** in both crisis and normal situations and how to best tailor security related communication and instructions are important to improve amongst other evacuation and protection activities. If governments have the ability to communicate risk, threats and security measures in a focussed and optimised way, then citizens are more likely to take coherent, correct and timely action. Fundamental to this process is the understanding of the behaviour of people, crowds and communities in both normal and crisis situations. Major incidents will involve people from differing faith, religious and cultural backgrounds from the survivors, casualties, deceased victims and bereaved families to workers, first responders and affected communities. Responsible agencies must ensure that due consideration is given to their specific needs at the appropriate time.

Researching and **profiling terrorist behaviour** is vital in the long-term prevention of terrorism, terrorist activity and the anticipation of potential risks and threats. The risk of radicalisation, and consequent recruitment, of individuals from local communities is forcing many governments to re-evaluate not only their approaches to security, but also their policies in foreign affairs, education, housing, and other social issues. A deeper understanding of the issues affecting radicalisation, the process of recruitment, and complex motivations of terrorists may facilitate effective counter-measures.

There is an obvious link between the above research topics and the technology mission areas. The behaviour of individuals and crowds in crisis situations and communication of security advice, relates strongly to crisis management (page 39) whilst understanding terrorist behaviour and radicalisation has a strong link to protection against terrorism and organised crime (page 29).

Recommended research topics

- Understanding issues associated with radicalisation (including social disintegration), terrorist behaviour and motivationfor terrorist acts.
- Human behaviour before, during and after crisis situations to understand how people react to threat alerts and security instructions.
- Understanding factors that cause citizens' feeling of security and insecurity and the method to determine it.
- Communication strategies of public authorities (including media strategies) before, during and after crises concerning risks, security threats and measures.
- Signs of 'early warning' to detect trends and weak signals in social polarisation, radicalisation development and segreation, etc.

Understanding organisational structures and cultures of public users

The results of European security research will be taken up by numerous private and public end-users and hence research and technology development projects should be oriented to meet their specific needs in terms of applicability, user friendliness and affordability. To successfully integrate end-users into research and development of security technologies requires an understanding of the organisational structures and distinct cultures of public user organisations, which are **numerous, complex and diverse**. Theoretically driven empirical research should therefore be directed towards the 'human' and 'organisation' legs of the mutual dependency triangle in terms of analysing the consequences on the political, institutional, organisational and human elements underpinning technology-based security policies and programmes. In addition, supporting activities are needed to bolster the end-user perspective in these publicly funded innovations and the proposed creation of the European security research network, as outlined on page 68, is a positive step in this direction.

A European capacity to handle civil security and safety issues builds primarily upon the resources and mandates of the Member States. In order to achieve an **effective joint capability** in this area, the distinct national systems must be interoperable, scaleable and where appropriate mobile. This requires addressing various institutional design questions in order to achieve better connectivity between the existing national systems. Work has already commenced to this end at European level with resources and mandates evolving in support of an enhanced European capability. Institutional design questions concerning conflicting or complementary mandates and resources remain additional areas to be addressed.

Of research importance is the prevalent **procedures for political accountability** and democratic control of public services within the security arena. This is particularly acute as political and judicial commitments are fragmented, sectoral and coexist at multiple levels of authority. In addition, a number of behavioural, organisational and cultural issues have impact on the effectiveness of public users. National differences, linguistic barriers, stovepipe sectoral approaches, organisational mandates and professional outlooks create numerous obstacles to effective information flows and to shared situational awareness.

There is an obvious link between the above research topics and the technology mission areas. The behavioural, cultural and trans-boundary interoperability dimensions resonate with, and strongly support, the crisis management mission area (page 39). Furthermore the research undertaken within this topic will have a direct impact on the development of curriculum for advanced security research and training proposed in the link to innovation section (page 74).

Recommended research topics

- Behavioural, organisational and cultural issues to understand public user needs including those for joint European action.
- Inventories of existing national resources, institutional mandates and practices across relevant sectors are needed.
- Best practices can be identified and disseminated across countries. Institutional design questions, such as mechanisms for democratic accountability, can be addressed at national and European levels.
- A multidimensional effort is required to build a research foundation for a high level of multi-organisational and trans-boundary interoperability.

Foresight, scenarios and security as an evolving concept

Security, dealing with acts perpetrated by intentional adversaries or with rare natural or man-made accidents with major consequences, is a domain where broad qualitative uncertainty is relevant even within the most near-sighted time horizon. Foresight studies are therefore very much needed in the security domain.

Security research has a clear need for foresight by virtue of addressing security challenges. But in addition **broad qualitative uncertainty** — on results and on their usefulness — is prevalent in all research. Therefore an applied research programme in any field without an element of foresight at the outset, risks being outdated before it is completed.

Foresight studies have the potential to discover not only novel threats and technological opportunities but also emerging security related ethical, cultural and organisational challenges. Foresight activities, including the discipline of scenario building, can be designed to **inform systemic risk analysis** — but also to inspire public debate and to foster shared understanding and self-organisation among stakeholders. They are designed to identify and deal with emerging phenomena. Therefore they provide the most promising approach to dealing with security as an evolving concept. This is most acute when, as the security research programme will need to do, one wants to integrate diverse strands of work and results in order to guide, orientate and structure future research activities.

When it comes to the rigorous assessment of **investment alternatives**, intended to prevent or mitigate insecurities with uncertain and potentially catastrophic ramifications, there are no valid alternatives to foresight based approaches (including methodologies like the threat scenarios based approaches used in defence planning). An important aspect in such assessment studies, in addition to financial costs, is the trade-off between security and other societal objectives such as the right to privacy and social cohesion.

Whilst the focus of the foresight work should be targeted specifically at security related issues, a great deal of valuable foresight work will be undertaken both in the 'Socioeconomic sciences and the humanities' thematic area of FP7 and in Member States. In this respect it is recommended that, where appropriate, results between the two FP7 thematic areas are exchanged to improve efficiency and effectiveness. In addition, it is also recommended to create a network similar to the **European Science and Technology Observatory (ESTO)** to foster security analysis and foresight in all Member States.

Recommended research topics

- Research in broad societal foresight to capture new and emerging threats as well as other aspects of security as an evolving concept (e.g. ethical and economic aspects).
- Research on rigorous methodologies for assessment of security investments and trade-off between security and other societal objectives (e.g. privacy and social cohesion).
- Foresight activities as action research for inspiring public debate and fostering shared understanding and self-organisation among stakeholders in the security domain.
- Include focused foresight activities addressing specific technologies or problem areas in technology projects.

Security economics

Security economics is the **analysis of aggregate risk** facing society and the economy using rigorous analytical and empirical economics tools. The rise of organised crime and terrorism has induced a strong interest in this new social science discipline. While the security economy is a general policy issue, it is striking that the economic analysis of security — and in particular its link to the Lisbon agenda — are not debated publicly or academically in depth.

There is a strong need to develop an integrated understanding of the multifaceted challenge of security while also maintaining rigour in the process of analysis and policy advice. Such approach can help achieve the balance between security and other policy objectives, which a singular focus on security and competitiveness cannot. Economic theory in particular can offer key insights, enabling governments to optimise their efforts to **enhance security and growth**.

Insecurity — and reactions to it — is mainly a matter of perception. There is significant evidence that the media, consumers and producers — and by extension policymakers — are poor judges of objective levels of insecurity, leading to imperfect security decisions. Furthermore, regulatory measures can initiate changes in market structures. Analogous to environmental regulation which enables firms to profitably contribute to 'green growth', one can think of regulation that stimulates '**secure growth**' by enabling industries for security-enhancing products or services.

The European capacity for economic analysis and for policymaking in this field is weak, especially when compared to the United States. This is caused by several factors notably geographical and subject dispersion. To address these causes, it is recommended to establish a **security economics network** starting with a small kernel of known individuals or organisations and progressively widen the community through disseminating new research and policy insights emerging from European funded research activities.

Recommended research topics

- Survey the emerging field of European security economics research to provide an analytical framework for complementary research outlined below.
- 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.
- Public finance: studying the scale, function and roles of various types of government security spending across Europe and time. Research to include socio-economic benefit delivered by GMES.
- Effects of insecurity and security policies: on individuals, firms and transaction costs between sectors of the economy. Research to include measures and tools to combat terrorist financing.
- Policy evaluation: implementing scientific evaluations of policy interventions in the field of security economics using natural or social experiments to isolate the effects of interventions, akin to research in the medical sciences.

There are obvious links with the '*Socioeconomic sciences and the humanities*' thematic area of FP7. In this respect it is recommended that, where appropriate, results between the two FP7 thematic areas are exchanged to improve efficiency and effectiveness.

Ethics and justice

Security technologies, and the government policies accompanying them, raise many different ethical and legal concerns amongst the European citizens. The strength of these concerns directly **influences public support and acceptance** of both government policies and the security technologies themselves. To address this issue it is proposed to analyse the wider context of government policies and responses to security threats. Four main strands emerge as relevant: (a) security and privacy, protection of individual data and human rights; (b) acceptability of security technologies — ethical concerns; (c) prioritisation of specific security threats and the use of resources; (d) how to ensure European security while stabilising the neighbouring areas.

Many of the adopted new security measures for example in counter-terrorism are associated with the **potential loss of privacy** or infringement of liberty. In some EU Member States these measures have raised a lively public debate on civil liberties and whether these counter terrorism measures come at the expense of sacrificing some of the most cherished civil liberties and rights of citizens.

Furthermore, the use of certain security technologies raises different ethical and legal concerns, many of which may relate to the invasion to privacy, reliability, social exclusion, feared damage to humans and environment and public regulation problems. The prioritisation of threats and the decisions to allocate resources are important but also sensitive questions. Part of the process assessing the priority of threats and specific targets to be protected is based on **value judgements** on what is vital for society.

A potential ethical concern is the increasing formation of areas of insecurity within Europe (suburbs, poverty stricken inner cities) and immediately **surrounding the EU's external borders**. The recent riots in France have highlighted the need to make sure that all citizens enjoy equal access to societal stability and security. The enlargement process has highlighted the need to enhance regional stability in the EU's neighbourhood in parallel with internal security measures in order to avoid new dividing lines.

In a European context, divergent ethical, religious, historical and philosophical backgrounds can lead to a variety of approaches on ethical and legal questions. In security research these concerns must be addressed by policymakers and the scientific community alike. **In research projects dealing with sensitive issues where ethics and justice meet security all relevant actors (lawyers, industry, data protection officers) must work together to achieve a fair and effective balance.**

There is an obvious link between the above ethical aspects of security technology use (detection, identification, and authentication) and the protection against terrorism and organised crime mission area (page 29) whilst reconciling human rights and security has a strong link to third pillar cooperation in justice and home affairs. Furthermore, avoiding areas of insecurity around EU borders should be linked with the EU's neighbourhood policy.

Recommended research topics

- How to maintain the proportionality between the right to security and civic rights and how this is implemented in practice. The issue of privacy and security should be particularly addressed.
- Ethical aspects of security technologies.
- Ethical implications of the continuum of internal and external security focused both on the implications for neighbouring countries and for the internal exclusionary effects of the evolving security technologies and policies.
- To review existing codes of conduct, best practises, etc. as to the ethical use of security technologies and to develop new ones where shortfalls exist.

Section 4

Enablers

Enablers

Important though the mission capabilities and technologies may be, considering them in isolation without the requisite enablers, will not yield the optimum benefit for all stakeholders. A combined treatment will be essential if the substantial financial and human resources to be invested are to yield the anticipated returns. Ultimately this will be measured by the amount of research transformed into new products and services to meet citizen's needs.

To this end ESRAB has identified three key enablers:

- coordination and structuring — aims to address the efficiency and effectiveness of European security research with the objective of avoiding unnecessary duplication and focusing research on high leverage customer driven requirements;
- specific implementation rules — the requisite implementation and governance mechanisms to accommodate security research sensitivities for example handling classified information, international cooperation and intellectual property rights;
- link to innovation — mechanisms by which European security research can stimulate innovative/breakthrough research and bring more of the research undertaken through to procured products and services.

Implementation rules

Contrary to other parts of the framework programme, security research has certain specificities. On the one hand this relates to the sensitive nature of security and the particular capability gaps that need to be addressed to protect Europe's citizens. On the other hand the recognition that the end-users of the security research results will often be public or governmental organisations and thus Member States will need to be more actively involved in the programme. For European security research to be undertaken successfully, it is therefore essential that the FP7 implementation rules, work programmes, grant agreements and governance structures make adequate provisions for these sensitivities. ESRAB has identified the following issues as being central to successful delivery and reviewed the extent to which they, either directly or indirectly, are adequately reflected in the planned FP7 implementation rules. Where this was found not to be the case, recommended improvements have been proposed, and are summarised hereafter:

- handling classified information and export control;
- governance;
- intellectual property rights;
- participation of third countries;
- co-funding levels;
- proposal evaluation and selection.

It is worth noting that due to the fact that the FP7 implementation rules were being developed in parallel to ESRAB's work, interim findings were provided to the Commission throughout so as to guide and influence their development.

Handling classified information and export control

Part of the security research to be performed at European level may well involve the use, or dissemination, of sensitive or classified information. A mechanism to successfully handle classified information in a consistent, agreed and secure manner must be established in order to avoid dissemination of such data to unauthorised recipients. Failure to define and implement the mechanisms successfully will inevitably restrict the scope of European security research to unclassified data.
Leaving aside the **fundamental that national regulations be complied with**, the most pressing item requiring resolution is the need for the Commission to update its security regulation to include exchange of EU classified information with private companies. The current EU regulation is neither applicable to classified information nor to classified contracts or grant agreements entered into between the Commission and private companies.

It is recommended that:

- European security research operate within the framework of EU classified information;
- the Commission update its security regulation to include exchange of EU classified information with industry in the context of the framework programme;
- the Commission implement a stepwise protection procedure to handle classified information for proposals and projects up to, but not above, EU secret classification. Projects shall not include national 'eyes only' caveats;
- the grant agreement include a security aspect letter (SAL) which specifies the level of classification of all project outputs. This SAL should be approved by the Commission, with the support of the concerned Member States, on the basis of a proposal from the consortium;
- possible European security research participants are made aware of the correct method of submitting, undertaking and delivering classified projects (user guides, workshops, etc.).

Appropriate rules shall be followed for the export outside the EU, from a third country to the EU or transfer within the EU of sensitive knowledge and technologies developed within security research projects and support activities. National, and supporting EU, regulations will necessarily apply. As a guiding principle, projects which could be affected by national export controls, should be identified as early as possible in the process so as to address the issue prior to grant award.

It is recommended that:

- Member States be involved in the selection phase of a call for proposals to identify, and possibly solve, export problems in advance;
- consortia involved in such projects have an adequate management system and procedure to deal with export control issues.

Governance

Comitology and information provision to programme committees will continue to be a feature of FP7. The Commission has proposed that there be a programme committee for each of the four FP7 specific programmes which would meet in different configurations depending on the subject area.

Before assessing the most appropriate type of committee to govern security research, ESRAB addressed whether to recommend separating security research from space research. On balance, ESRAB shared the Council's view of separating the two types of research mainly due to the unique specificities of security research and the desire for budgetary clarity. With respect to the latter, in the event security and space were retained as a single theme, ESRAB recommends that at least 50 % of the budget (over the seven years) be dedicated to security research and that two different configurations of the programme committee (one for space and one for security) be put in place. In addition, the role of the programme committee shall need to be reinforced forsecurity research.

It is recommended that:

- the programme committee be fully involved in the preparation of the work programme;
- programme committee members inform the Committee of their programmes on security research;
- the programme committee be involved in the necessary coordination between the projects of the security theme and the ones launched under other themes of the cooperation programme;
- programme committee members have a role to inform potential national participants about the opportunities to participate in a call for proposals and the requirements for sensitive projects to obtain the necessary clearance or authorisation before submitting proposals;
- the programme committee consider with particular attention projects dealing with classified information as well as projects involving a third-country participant;
- programme committee members have the possibility to raise to the attention of the programme committee projects which they consider do not comply with the proper measures relating to classification, export or dissemination of sensitive information;
- the Commission seek the support of concerned programme committee members to deal with classification or export controls issues related of an activity.

Intellectual Property Rights (IPR)

Collaborative research, by its very nature, will rely on the members of the consortia combining their pre-existing background knowledge and generating, through project execution and delivery, foreground knowledge. The FP7 rules of participation, like those of FP6 before it, address background and foreground IPR in terms of ownership, protection, access rights and use. ESRAB felt that security research has certain specificities which needed to be taken into account. Firstly the possibility for the Commission to control the transfer and dissemination of knowledge for sensitive projects and secondly the requirement for specific project information to the programme committee in order for Member States to be able to inform 'end-users' of research of potential interest to them and to coordinate national research.

It is recommended that:

- provision be made to include in the grant agreement of relevant activities the possibility for the Commission to control the transfer and dissemination of knowledge for sensitive projects;
- specific information in the form of a deliverable executive summary be prepared by the consortium and provided to the programme committee. This communication would be for information only with no right of use.

Participation of third countries

The strategic approach to international cooperation within the framework programme is to enhance EU competitiveness and global sustainable development through partnerships between the EU and third countries. Despite the sensitive nature of European security research, ESRAB believes third-country participation should not be forbidden but rather subject to particular provisions.

It is recommended that:

- any legal entity may seek to participate in an activity in the field of security research subject to preconditions laid down in the call for proposals;
- the programme committee vote for the selection of any successfully evaluated project involving a participant from a third country, taking into account the benefits (e.g. industrial competitiveness) and/or drawbacks (e.g. EU security, project failure due to export regulations, classification issues).

Co-funding levels

As already stated, security research will be subject to the overarching FP7 rules of participation, including those related to co-financing. The Commission proposal, published mid way through ESRAB's work, defined a basic rate of 50 % funding for pre-competitive research, which could be raised to 75 % for SMEs and universities.

It is recommended that:

the possibility of a higher level of co-funding, for a limited number of specific domains, should be retained; this would apply in particular for:

- the development of capabilities in domains with very limited market size and a risk of 'market failure', for example CBRN, high grade cryptographic equipment, equipment for anti-bombing teams or for first-responders in case of natural disasters;

- accelerated equipment development in response to new threats: necessity to respond to new security requirements and to take account of new technologies and new security environments in very short timescales.

Additionally the higher co-financing would counter the recognised additional security-specific constraints, namely regulatory constraints that shape the market and hamper supplier's freedom of movement and specific constraints in terms of confidentiality, dissemination and onward exploitation.

Proposal evaluation and selection

FP7 provides the possibility for specific thematic evaluation criteria to complement the generic evaluation criteria. These are outlined below. Furthermore, in order to take account of the unique character of security research, it is recommended that representatives from the scientific/industrial and end-user communities evaluate proposals. The programme committee will have an additional role to play in this respect.

It is recommended that:

- representatives from the scientific community as well as the end-user community evaluate proposals. Member States should provide, to the Commission, a list of candidate evaluators;

- the generic FP7 evaluation criteria be complemented with the following additional elements:

  - the added value of the research project to security in Europe;
  - the added value of the research project to the reinforcement of the competitiveness for European industry;
  - the effort of the consortium to inform Members States and end-users on the project and its achievements;
  - the proper consideration of the mutual dependency of technology, organisational dynamics and human impact (where appropriate);
  - the compliance of the research proposal with security regulations (export regulation, classified information), ethics principles as well international treaties relevant to security matters and the ability of the consortium to manage it throughout the project;
  - the benefits and drawbacks of the participation of a third-country legal entity.

Coordination and structuring

At the European level both financial and human resources are scarce and furthermore spread thinly across the civil, security and defence arena. The best overall return on investment must therefore come from making efficient use of these scarce resources whilst bringing the most appropriate expertise to bear. It is clear there will be certain areas where coordination and structuring are not sought, or needed, but equally there will be others where coordination and even cooperation would add value.

In attempt to establish how Europe's limited resources could be used more efficiently and effectively, ESRAB canvassed the views of a cross stakeholder community of Member States, industry, academia and research establishments. This section of the report focuses on those themes offering the greatest impact potential.

Creating co-ordination and advisory structures

Alongside the programme committee's more operational role in overseeing the implementation of FP7, ESRAB has identified the need to address the widespread fragmentation of security activities, particularly at the European level, by initiating a structured dialogue across all relevant stakeholders — technology providers, end-users and policymakers. Even though this exceeds the original ESRAB mandate, and enters into a complex political and legal area, ESRAB believes it to be of vital importance in initiating the most efficient and effective use of limited human and financial resources.

Such a communication platform should take account of the established EU coordination structures whilst looking to take a broad, ambitious and more **strategic view** of security related activities. In addition, it could act as an **advisory** sound board for the implementation of existing programmes and initiatives. ESRAB believes that the principal objective should be to ensure that all the component parts required to realise an improvement in **European security** (research, policies, legislation, standardisation and other related activities) are laid down in synchronised, coherent and prioritised roadmaps within a **Strategic Security Agenda**. The aim would be to ensure work undertaken by the various stakeholders is reinforcing and directed towards commonly agreed security needs. Whilst this is not the place to determine terms of reference and organisational details, these will be of crucial importance and shall need to be worked up in the near term.

Clearly delivery cannot be met by a single stakeholder and tasks will have to be shared. Each will have their specific capabilities and resources which will need to be directed and applied. Capabilities and resources will therefore not be taken from the stakeholders but be applied by them. Similar approaches have been developed in other quarters and best practice should be leveraged from these when turning to implementation.

The success of such an approach will almost entirely depend on rallying the stakeholder

communities behind the agreed priorities. If they do so, European security priorities will converge, performance will be more efficient and effective, there will be more opportunities for collaboration, and perhaps most importantly European citizens will be more secure and their industries, more globally competitive.

It is recommended that:

a European Security Board be created in order to foster greater dialogue and a shared view of European security needs with the aim of advising as to the content of a Strategic Security Agenda. The board would bring together, in a non-bureaucratic way, the Commission, Member States and other key public and private stakeholders. The ESB should:

- be operational in the first half of 2007;
- have an ambitious and broad mandate;
- advise on a strategic security agenda to European policymakers, programme constructors, research performers and subsequently update and monitor its implementation;
- share security challenges and research information, including European security research results and assessments.

Security research will clearly be one of the subjects to be covered by the European Security Board and ESRAB recommends that in order to clearly articulate research requirements effectively a **more operational structure** should be put in place to support it.

Such an operational structure should be flexible to accommodate, and adapt to, new and emerging issues and should therefore be based, where possible, on existing organisations and networks (associations, forums, agencies). On the technology supply chain side the main associations of industries, SMEs, research and technology organisation and academia, will provide access to the key actors of their sectors. **Points of contacts** should also be appointed per country from the public user and research departments in order to coordinate requirements and disseminate research results. A steering group should be set up to ensure coherence between, and across, the different stakeholders and activities.

Activities could be structured by mission, or group of missions, with the aim of creating homogeneous network of users and experts. The activities may be intersectoral but must have a common basis of needs and possible solutions. The network should be **supported by an executive secretariat** provided by a 'neutral' sector/academic association and funded by the Commission. Within strict conditions of confidentiality, maximum use should be made of secure IT platforms and networks to exchange relevant data. An ERA-net on specific areas of common interest could act as a complementary activity in this respect (page SS).

It is recommended that:

at the operational level, a 'European security research network' of end-users and technology supply chain experts be established. The network should:

- facilitate a common understanding of needs between end-users, with the support of technology experts, so as to define precise technology solutions to meet the needs;
- for defined areas, propose to the European Security Board strategic R & T roadmaps to guide, orientate and underpin European, national and private research programmes;
- identify possible joint programmes or projects which could be undertaken between services, Member States and EC or international organisations;
- contribute to standards definition.

Transparency

For the European security research programme to optimise its **efficiency and effectiveness** it requires a high level of transparency with other research programme constructors — not only nationally but also at Community level. This is most notably the case for research programmes that develop underpinning technologies which can be 'spun-in' or 'spun-out' to meet either civil, security or defence requirements.

The actors in the civil, security and defence research fields are numerous and vary in terms of outlook, perspective and membership. Whilst the Commission and Member States represent, by far, the largest investors in this area other actors including the **European Defence Agency** (EDA), the North Atlantic Treaty Organisation (NATO) and the Organisation for Security and Co-operation in Europe (OSCE) undertake complementary research.

Comparison across such organisations at programme level would be facilitated by a jointly defined, and commonly applied, **technology taxonomy**. The taxonomy would also assist in addressing the identified technology watch shortcoming, for the timely identification of new and emerging technologies. Work is underway in this respect and advantage should be taken of progress made.

It is recommended that:

a European Security Technology Watch be established, building on existing concepts already in some Member States and the US. Concrete steps should be to:

- create a web based IT system that acts as both a repository for the data (technology watch list) and an interface for interrogating the data to user requirements;
- nominate points of contacts in each organisation responsible for managing the data entries;
- designate a 'neutral' lead coordinator;
- establish a technology watch panel to monitor its implementation and advise the EC, Member States and EU security research community on emerging technologies.

To facilitate transparency it will be necessary to identify, and engage with, **nominated contact points** within each of the relevant actors, and to consider the scope, depth and transparency mechanisms required. Tools to facilitate this sharing will include agreements on protection of intellectual property and handling of classified information, technology taxonomy, and (in time) the development of shared databases, electronic information repositories and other IT solutions. Due to the scale of the task it is recommended to **start initially with a core group for example Commission and EDA** and to expand this group over time. Such information sharing mechanisms should be an active process, in which the Commission seeks to establish links with the relevant actors, and to collect information from them.

It is recommended that:

- the Commission and the EDA should take positive steps to define and develop an information sharing regime;
- the Commission open discussions with Member States and other public authority points of contact to discuss the possibility, and parameters, of a system of security research information sharing.

National security research programmes

The ESRAB survey revealed that **fewer than five Member States have a dedicated national civil security research programme**. That is not to say that security related research is not undertaken in the other nations, but that this is scattered over different departments and research programmes. Due to this fragmentation, Member States may have difficulty establishing how their own security research should complement the European programme, and vice versa. **The creation of national security research programmes** could therefore significantly facilitate coordination and cooperation at national, transnational and Community levels. Furthermore such programmes would provide the catalyst to address sensitive and complex questions which, if solved nationally, would facilitate the move towards common standards, interfaces and definitions at Community level. Such questions would centre on:

- defining the boundary between safety and security;
- addressing the distinction between military and civil security research;
- considering social, economic and cultural aspects in security research;
- handling sensitive information in projects.

It is recommended that:

Member States be encouraged to develop national security research programmes. A series of national workshops should be organised aimed at raising the awareness of security research and the manner in which national programmes could complement the European programme.

Link to innovation

Security research aims to achieve the twin objectives of increased security for Europe's citizens whilst simultaneously improving the global competitiveness of Europe's industrial base. Meeting both objectives depends on 'customers' having well defined needs for which the supply chain creates new products, systems and services. This 'push-pull' innovation system is fundamental, being described by the OECD as '*a network and interplay of public and private institutions in which production, distribution and use of new knowledge and technology take place*'.

The development of a European security innovation system is the guiding recommendation to the Commission. ESRAB has analysed a number of potential key components within a European security innovation system and these have been clustered into the following topics: competitiveness, SME engagement, standardisation, best practice and user involvement.

Competitiveness

In order to gain a better, and more comprehensive, understanding of the industrial and research landscape, it is necessary to have a firm grasp of the capabilities of those organisations within the technology supply chain that develop security products and services. The intention would be to strengthen the competitiveness of companies in Europe by identifying both critical and weaker links within the technology supply chain, the main stakeholders and actors in Europe, and the areas in which possibilities exist to create strong centre of excellences. Inputs should be gathered from various sources, including Member States who should be able to provide a list of critical and relevant suppliers that are already involved in their national security programmes. Whilst the **mapping of the civil security technology supply chain** is clearly far broader then just the defence industry, it is recommended that maximum use is made of synergies with an equivalent mapping the Defence Technological and Industrial Base (DTIB) within the European Defence Agency (EDA). The overall analysis should influence both the Commission and Member States in the planning of their future security research programmes.

The security market in Europe is still not well developed and many in the technology supply chain, particularly the industrialists, are unsure of the market demand. In order to stimulate the demand for new and innovative security products and services, incentives for public authorities, often seen as 'first buyers', should be introduced. New procurement procedures such as those outlined in the Commission's 'Pre-commercial procurement of innovation' ([8]) communication should be applied to the security sector. European groups of public authorities can share risks, costs and benefits by cooperating in **innovative procurement processes.** Groups of public authorities also can be linked in pre-commercial procurement procedures that are related to development of European security research demonstrator programmes.

([8]) 'Pre-commercial procurement of innovation: A missing link in the European innovative cycle', March 2006.

The ERA-NET ([9]) scheme aims to stimulate **coordination of national research programmes and increased competition for research**. Whilst FP7 may look to deepen or broaden cooperation within existing ERA-NETs, new topics such as security research must be supported. The intent to open FP7 ERA-net's to public bodies planning research programmes that are not yet in operation is a welcome step. Furthermore the ERA-NET+ scheme offers the incentive for joint calls for transnational research projects organised between a number of countries. The ERA-NET scheme as a whole therefore provides a tool to create an open European research market by offering researchers from all Member States the opportunity to compete in national and European research programmes. This would naturally have a direct bearing on their competitiveness and simultaneously provide a useful instrument to promote harmonisation of national standards.

It is recommended that:

- the Commission support the work of a continuous mapping of security capabilities and the technology supply chain in Europe;
- the Commission investigate how pre-commercial procurement could be introduced and stimulated by European security research;
- European security research promote, support and utilise the instruments offered through the ERA-NET scheme.

SME engagement

There is a general aspiration amongst organisations across Europe to enhance the competitiveness of the technology supply chain, in particular SMEs. The Commission's framework programmes for research and technology development are essential to support these ambitions, especially for smaller countries. Small companies feel increasingly marginalised in national and international research programmes. There is therefore a need for a positive **system of transparency and increased accessibility** in order to ensure that the full potential of the supply chain is available to industry and society at large.

In order to increase the participation of SMEs in security research, it is recommended that project proposals clearly describe a roadmap to the future, in which transitions from 'development' to 'implementation' are identified. In doing so, project coordinators (or brokerage party/system integrators) should define clear tasks for SMEs to facilitate their participation in both projects and subsequent implementation. In this sense European security research should be SME inclusive not SME driven.

The Commission has launched a proposal for a competitiveness and innovation framework programme (CIP) ([10]). It brings together several existing EU activities that support competitiveness and innovation. It aims to improve the availability and access of innovative SMEs to external sources of financing, including R & D and innovation activities, and promotion of SME participation in FP7 research projects. A close cooperation with the security research programme and CIP is essential for stimulating SME participation in European security research.

([9]) Networking the European research area — Coordination of national programmes.

([10]) COM(2005) 121 final.

It is recommended that:

- European security research project proposals, involving SMEs, which clearly specify their task and role in the project proposal should receive priority;
- the Commission explicitly include the security area in the competitiveness and innovation framework programme (CIP).

Development of European policies and standards

European security policies could be important drivers for boosting research and development. In many areas, for example with respect to the environment, European policies are driving forces for research and development. At the same time research and development can support the development of policies. By way of example, research and development can help in identification and setting of quantifiable targets for security levels in a security policy, as the section of security economics highlights (page 59).

In addition, standards have proven to be important to market creation, as an enabler to international development programmes, and as a tool in procurement. The European Committee for Standardisation (CEN) ([11]) is coordinating European standardisation in the security area, and aims to concretely identify new standardisation needs. A top down assessment is underway to review both existing national and international (ISO, ANSI) standards. This will be supported by a bottom up assessment of needs derived from the research results emerging from the projects awarded under the PASR and other European and national research programmes.

Standards are efficient tools for all relevant stakeholders, as standards deliver interoperability and durability to end-user requirements. However, in some cases, technical standards alone are insufficient and need to be complemented by testing, evaluation and certification, to ensure proper implementation. Interoperability can only be obtained if additional conformity evaluation efforts are conducted either by a third party or by end-users, an effort which is directly related to the end-user requirements. In the security domain, certain missions require not only definition of standards and norms but also mechanisms for conformity tests and certification procedures.

It is recommended that:

- European security research project proposals that clearly contribute to development of European standards should be given priority;
- European security research support and develop research aimed at guiding and informing European security policies;
- European security research support the creation of a network of facilities for test and validation of security products.

([11]) CEN Technical Board/Working Group 161: Protection and Security of the Citizen.

Best practice

European security research should strive for operational excellence in transforming research into commercial products through the use of large-scale demonstrators. Demonstrators, combining a number of capabilities, technologies and disciplines, at an appropriate state of readiness are a useful means of validating system performance thereby gaining end-user acceptance. The inclusion of 'first buyers' within European security research demonstration programmes could therefore be a useful catalyst to spur innovative procurement. Demonstration programmes are a key element in the delivery of the technical work and more detailed descriptions on these can be found on page DDD.

The Commission has a longstanding experience in presenting prizes and awards in specific areas. Since 1995, DG INFSO has been awarding the European IST Prize for the best European innovation in 'information society technology'. A similar prize could be envisaged within the security area. A security innovation contest could scope out a challenge based on a recognised European security technology gap and invite industry and the scientific community to compete to develop the best ground-breaking solution. Alongside a monetary prize, the accolade would provide public recognition and a highly visible profile to a wide spectrum of public and private security stakeholder. Feedback on this new mechanism received widespread support from all stakeholders, especially Member States, when ESRAB canvassed their views.

It is recommended that:

- a number of demonstrators at system level should be supported within European security research in FP7;
- the Commission include European security innovation contests within the security research programme setting aside the appropriate organisational and financial support.

Involvement of the user

User involvement is a prerequisite for solid requirement specification, for innovative procurement, and for market uptake. The proposed creation of the European Security Board and its supporting European security research network are valuable means to this end and will increase the direct involvement of the end-users.

Moreover, research and development is a people intensive activity requiring highly competent producers of research and innovation, qualified demand articulators, competent evaluators of results, as well as public and private users. Security is a new and emerging discipline in its own right and whilst many educational programmes exist to train public officials in the defence sector and other specialised areas of public concern, this is not the case for security. A new generation of officials and industrialists trained to give direction to, and to use the results of, European security research is needed.

It is recommended that:

- the Commission support the development of a curriculum for advanced security research and training at masters and post gradual levels in thematic fields of science and technology that are important for security research.

Section 5

Findings

ESRAB key findings

1. The ESRAB report represents the successful implementation of the GoP recommendation to **bring together at European level the 'demand' and 'supply' sides** in order to jointly define commonly agreed strategic lines of action for European security research. The report demonstrates both the value and feasibility of such an approach.

2. ESRAB has produced a **strategic framework** to structure the research content covering both **technological and non-technological aspects.** The report identifies and prioritises only those capabilities, integrated projects and demonstration programmes which offer a high potential to deliver European added value.

3. ESRAB recommends that multi-disciplinary **mission-oriented research** should be undertaken covering capability development, system development and systems of systems demonstration. Technology development should include new and emerging technologies to address security-specific breakthrough technologies. As a matter of principle, it should **combine end-users and suppliers in project definition and execution**. The programme should be SME inclusive but not SME driven.

4. ESRAB has addressed the special **implementation rules** for European security research. In particular these relate to governance, with a **reinforced role of the Member States authorities** (programme committee), and the handling of sensitive information, through the use of EU regulation on classified information (still to be updated).

5. Respect of **privacy and civil liberties** should be the programme's guiding principle. In this sense research and development projects should take into account the mutual dependency triangle of technology, organisational dynamics and human impact.

6. Technological research and development must be strengthened, and when appropriate integrated, with research into **political, social and human sciences**. Five areas are identified: citizens and security, understanding organisational structures and cultures of public users, foresight scenarios and security as evolving concept, economics of security, and ethics and justice.

7. Five enabling areas have been identified to **stimulate innovation** and improve **the pull through of research into procured products and services**— they include: technology supply chain competitiveness, SME engagement, standardisation, leveraging best practice and end-user involvement.

8. ESRAB emphasises the need for **effective coordination and transparency** to ensure that unnecessary duplication is avoided and that European security research both informs, and takes account of, other European and international research. The report identifies the mechanisms to achieve this, including the use of technology watches for organisations which share a common technology base, for example the **European Defence Agency**.

9. European security research needs to be complementary to national security research programmes. Where these exist, they should be aligned to the EU programme, and where they do not, it is proposed that these should be established, supported by a critical mass of resources. **Funding at EU level should not substitute national funding in this important area.** A rolling programme of national workshops, aimed at raising the awareness of security research and the manner in which national programmes could complement the European security research, should be initiated in the second half of 2006.

10. ESRAB recommends the creation of a **European Security Board (ESB)**, to foster greater dialogue and a shared view of European security needs. The board should bring together, in a non-bureaucratic manner, authoritative senior representatives from a cross stakeholder community of public and private stakeholders to jointly develop a **strategic security agenda** and act as a possible reference body for the implementation of existing programmes and initiatives. Participation in the ESB would involve a commitment to influence all stakeholders to plan their activities in the light of the agenda. Consensus at the ESB level should help in the **sharing of tasks** and shaping relations between national and EU programmes/policies as well as **influencing the deployment of funds**.

Next steps

A great deal of cross stakeholder effort has been marshalled by ESRAB in defining the structure and content of the ESRAB report. ESRAB therefore recommends that the Commission take full advantage of the report in its preparation and implementation of the forthcoming FP7 security research work programme.

In addition, ESRAB recommends the creation of a European Security Board (ESB) in order to foster greater dialogue and a shared view of European security needs with the aim of advising as to the content of a strategic security agenda. The ESB, described in more detail on page 67, should be operational in the first half of 2007 and bring together in a light non-bureaucratic structure, authoritative senior representatives from the Commission, Member States and other key public and private stakeholders. Direct participation would be essential for this process to succeed.

It is recommended that the ESB should:

- launch and approve a strategic security agenda, containing coherent and synchronised roadmaps to meet defined priorities. It should be updated periodically;
- make strategic and operational recommendations and commission future studies for implementing the agenda and on matters affecting European security;
- evaluate the overall results and benefits of the agenda for Member States, the Commission and stakeholder groups;
- develop and implement a communication strategy with two broad objectives:
  - promoting awareness of the agenda within the stakeholder communities and onwards to larger public audiences;
  - disseminating sufficient information on stakeholders' research programmes to facilitate a consensus on priorities.

To maximise its effectiveness, the ESB would need to be supported in executing its tasks by a small, but suitably qualified, secretariat. It would be beneficial if this reflected the composition of the stakeholder community.

Glossary

24/7	24 hours a day 7 days a week
3D	Three dimensional
AI	Artificial intelligence
C & B	Chemical and biological
C4	Command, control, communications and computers
CBRN	Chemical, biological, radiological and nuclear
CBRNE	Chemical, biological, radiological, nuclear and explosive
CIS	Communication information system
COTS	Commercial off the shelf
CROP	Common
DG	Directorate-General
JLS	Justice, liberty and security
EC	European Commission
EDA	European Defence Agency
EM	Electromagnetic
EMC	Electro magnetic compatibility
ERA-net	Networking the European research area
ESB	European Security Board
ESRAB	European Security Research Advisory Board
EU	European Union
EUROJUST	European Union body composed of national prosecutors, magistrates or police officers from each of the European Union's Member States
EUROPOL	European Police Office
FP	Framework programme for research and technology development
GDP	Gross domestic product
GMES	Global monitoring for environment and security
GoP	Group of Personalities
GPS	Global positioning system
GSM	Global system for mobile communications
HPM	High-power microwave
IKBS	Intelligent knowledge based systems
IPRs	Intellectual property rights
IR	Infrared
ISAR	Interferometric synthetic aperture radar
IT	Information technology
OCR	Optical character recognition
OECD	Organisation for Economic Co-operation and Development
QoS	Quality of service
R & D	Research and development
R & T	Research and technology
RFID	Radio frequency identification
RPV	Remote piloted vehicle
SAR	Synthetic aperture radar
SATCOM	Satellite communications
SME	Small and medium-sized enterprises
TETRA	Terrestrial trunked radio
UAV	Unmanned aerial vehicle
VIP	Very important person
WiMAX	Worldwide interoperability for microwave access

European Commission

Meeting the challenge: the European Security Research Agenda.

Luxembourg: Office for Official Publications of the European Communities

2006 — 79 pp. — 21 x 29.7 cm

ISBN 92-79-01709-8

SALES AND SUBSCRIPTIONS

Publications for sale produced by the Office for Official Publications of the European Communities are available from our sales agents throughout the world.

You can find the list of sales agents on the Publications Office website (http://publications.europa.eu) or you can apply for it by fax (352) 29 29-42758.

Contact the sales agent of your choice and place your order.

NB-75-06-348-EN-C

Publications Office
Publications.europa.eu

ISBN 92-79-01709-8
9 789279 017094