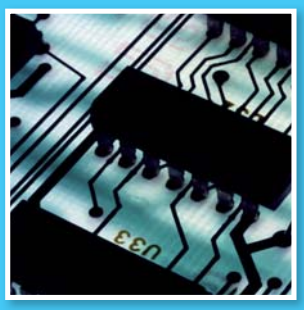
EUROPEAN SECURITY RESEARCH & INNOVATION FORUM

ESRIF

ESRIF FINAL REPORT



DECEMBER 2009

Foreword

Dragutin Mate,
Chairman of ESRIF and former Minister of Interior of Slovenia

Over the past two years, more than 600 experts and 65 distinguished personalities from all over Europe intensively debated in an open forum aspects of European Research and Innovation deemed essential to enhancing the security of our citizen. ESRIF (European Security Research and Innovation Forum), is the name of that forum. ESRIF tasks itself to define the European Research and Innovation needs for the mid- to long term, following the 'public – private dialogue' as a model.

I took over ESRIF's chairmanship a year ago from **Mr Gijs de Vries**, together with my two co-chairmen **Mr Jürgen Stock**, the Vice President of the German Federal Criminal Police Office and Mr **Giancarlo Grasso**, Senior Advisor to the Chairman and CEO of FINMECCANICA. We are proud to present the Final report of the Forum. The ESRIF final report consists of an '*Executive summary*', '*Part-1*' which constitutes the main report and '*Part-2*' giving the individual reports of the working groups as well the detailed listing of security research topics to be considered for funding.

Europe's main objective is to preserve its values as an open society and respect for fundamental rights and freedom while addressing the increased security threat. At the same time, our society is very dependent on technologies and infrastructures. We however insisted that 'Human Dignity' is the most precious and is an 'end' by itself and as such it can never become a 'means'.

ESRIF looked at scenarios with a 2030 time horizon to frame. These scenarios embraced a range of risks, from natural to man-made incidents; Capabilities and Capacities need to be mobilised to deliver equipment and services to deal with these risks and we need to obtain them from those that can provide these best. Being prepared is key to minimising the impact.

We believe that European security solutions must have their foundations in the European way we desire security for our citizen. ESRIF considers that research and innovation leading to security equipment and services can only become a market success if it can find broad public acceptance. Following these principles we wish to guide investments to make our industry strive for global leadership by creating a 'European market' that aids efficiency and effectiveness.

On behalf of those that have been actively contributing to ESRIF, I can say that we are confident to have started an important European process; a process that is not finished with this 'final report'; it merely begins here.

Brussels, in December 2009
Dragutin Mate

Table of Content

PART 1

PART 2

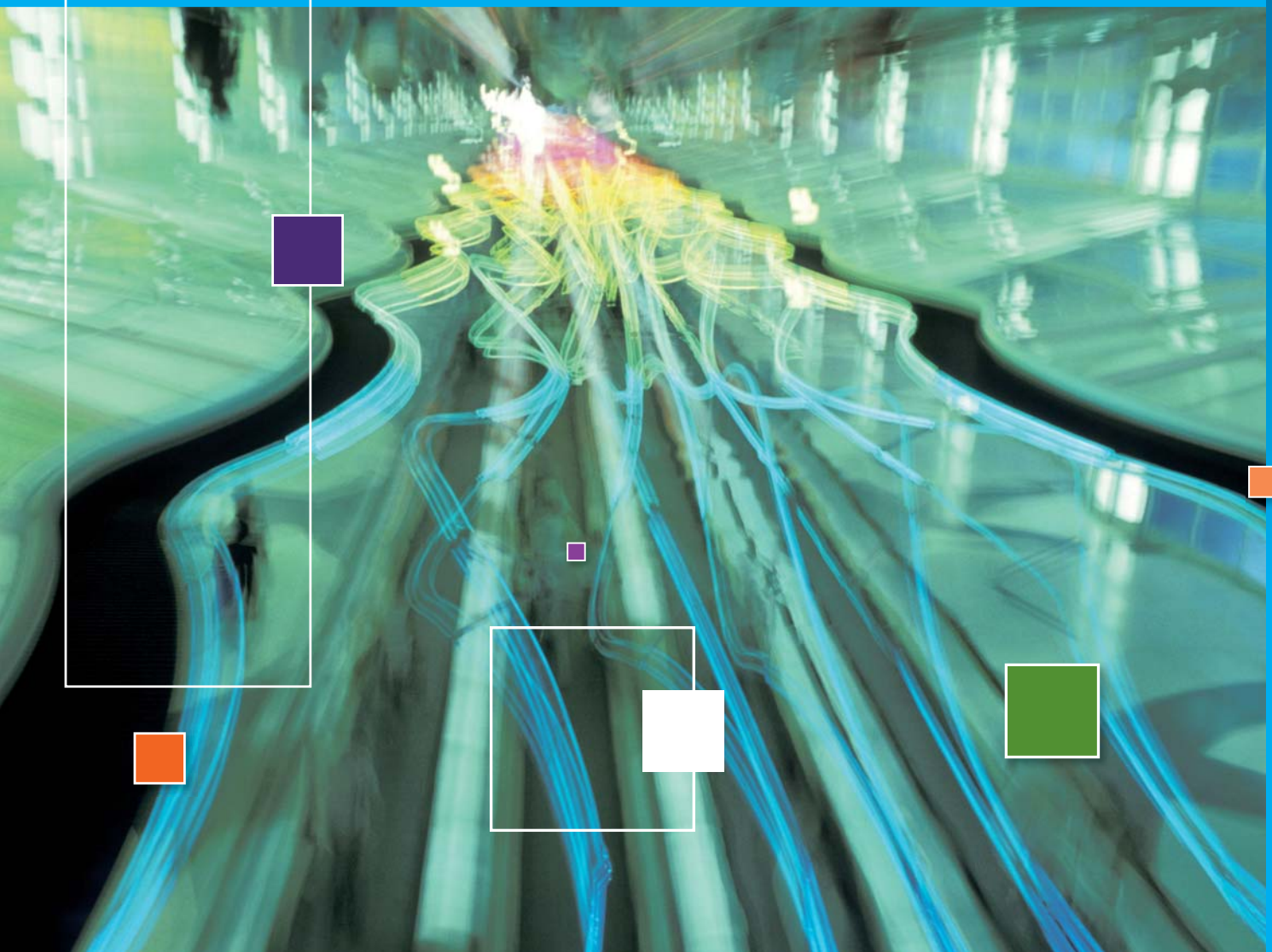
ANNEXES

EUROPEAN SECURITY RESEARCH & INNOVATION FORUM

ESRIF

ESRIF FINAL REPORT

PART 1



1. Introduction

The European Security Research and Innovation Forum (ESRIF) was established in September 2007, based on a joint initiative of the European Commission and the 27 EU Member States. Its plenary of 65 members from 32 countries includes independent representatives from industry, public and private end-users, research establishments and universities, as well as non-governmental organisations and EU bodies. ESRIF was supported by more than 600 experts, thus making it the only large-scale, high level initiative of its kind in Europe.

This report is the culmination of ESRIF's work. While not exhaustive –one cannot prepare for all eventualities – the document proposes a European Security Research and Innovation Agenda (ESRIA) over the next 20 years. The following chapters set out ESRIA's context, content and implementation and propose recommendations which will support the development of European security.

1.1 ESRIF's tasks

To map out such a security research and innovation agenda, ESRIF was tasked to address:

- Mid-term and long-term security perspectives (up to 20 years)
- European, national and regional perspectives, building on previous efforts (notably the 2004 and 2007 reports of the EU's Group of Personalities and the European Security Research Advisory Board, respectively)
- Enhanced co-ordination with other institutions involved in security research and innovation
- Societal and technological aspects of security research
- Promotion of innovation as the foundation for a European security market that exploits economies of scale at European level
- Guidance for all stakeholders who prepare security-relevant research programmes in Europe

1.2 ESRIF's approach

Given the need for long-term foresight, ESRIF devised a set of context scenarios with a 2030 time horizon to frame how current trends may combine to create alternative future 'scenes.' These scenarios embraced a range of risks, from natural to man-made incidents, and were used to test – and identify – how short- and mid-term risks and challenges may evolve into long term ones. Preparation is key to minimising their impact.

ESRIF took a holistic approach to security, taking the widest definition of security and examining how that can be achieved regarding society itself and the freedoms we want to maintain or enhance. This approach has produced what ESRIF considers to be an impetus for the future of security in Europe; a scientific technological and industrial base from which we can draw the necessary equipment, technology and best practice to deliver security as well as a rigorous social engagement assuring accountability for the use and acceptability of such solutions.

Many issues such as climate change, scarcity of raw materials, the impact of nano-technologies or the wider cyberspace environment generate new risks but seldom lead to the radical removal of old ones. This increasing evolutionary complexity

and interdependence magnify the impact of networks – and their breakdown – on society. This makes the effects of threats harder to forecast and understand.

ESRIF aims for a common understanding of security, research and innovation to support a more harmonised approach. In doing so, ESRIF proposes to enhance the role and ability of Europe's security manufacturing and service industries to invest in essential research and development activities. Supported by spending at national and European level, this investment will provide a strong basis for addressing future risks –without prescribing any one solution for a given challenge.

ESRIF role is not to define security policy: it strives to inform decision making at industrial, national and European levels. Its work required the engagement and contribution of stakeholders at all levels to reflect the interdependencies, diversity, multi-dimensional aspects and operational expertise of security in Europe – and which sets Europe apart from the rest of the globe.

1.3 The external dimension to Europe's civil security

ESRIF advocates that the external dimension of security should feature high on the agenda of any subsequent security research and innovation policy.

The European Union and its Member States are part of a highly interdependent complex world. Failed states, border disputes, environmentally induced migration, resource conflicts: all increasingly have intercontinental, if not global, repercussions. Europe cannot ignore these external risks and threats – or their potential impact – on its domestic security.

In future, the EU will operate in a more crowded and strained world, confronted with diverse conflicts, and technological challenges but also new opportunities.

The EU's obligation to cope with these external risk and threats is reflected in the growing involvement of its Member States and their militaries, police forces and civil protection institutions in peacekeeping and nation-building across the world during the last 10 years. Technological capabilities are key to the success of these "out of area" missions in conflict and human disaster environments. But this also requires a new mindset to enhance the cooperation of civil and military authorities who, in many instances, use similar organizations and equipment. Counter-narcotics activity is a typical police task that has both civil security and military implications.

This external dimension must effectively marshal European resources and policy.

2. ESRIF'S Vision: Key Messages

The EU today faces security challenges entirely different from those at the time of its inception. These range from money laundering and corruption to organised crime and violent terrorist acts to weapons of mass disruption to natural disasters and pandemics.

ESRIF is unequivocal that the European Security Research and Innovation Agenda must provide both a strategic concept and a practical process that defines and updates shared priorities to meet those challenges. However, this cannot be done in a vacuum.

Protecting the EU's population and infrastructure must resonate with good governance, common economic sense, and respect for fundamental rights and Europe's cultural values. For ESRIF, gaining a competitive advantage and leadership position in the global security market for Europe must reflect European values.

2.1 Societal Security

European security is inseparable from the social, cultural and political values that distinguish European life in all its diversity. Security research and innovation must address the long-term vulnerability of these values via European economic, cultural, political, and technological systems.

Humans are at the core of security processes: They endure and respond to natural disasters. They perpetrate or are victimised by organied crime, trafficking and terrorism.

Because security is inextricably bound to a society's daily political, economic and cultural values, technological innovation cannot fully contribute to security unless it focuses on the human being.

Security from a social perspective has three major characteristics:

- It is about *people* – both as the source and the object of insecurity
- It is about *society* – in the knowledge that some threats will target people's identity, culture, and way of life
- It is about *values* – and which proactive and reactive measures can protect Europeans while reflecting their values and way of life

Research and innovation in security demands a framework of legal and ethical guidelines – a "legitimacy perimeter" – to ensure social acceptance and trust, alongside effective political leadership and communication. These will open markets for trusted new solutions.

2.2 Societal Resilience

Given the unpredictability of man-made and natural threats, security research and innovation should focus on strengthening Europe's inherent resilience and ability to efficiently recover from crises by enhancing the cohesiveness and robustness of societal systems and their interface with security technologies.

Certain risks cannot be planned for or avoided. Resilient societies are those whose citizens, infrastructures and organisation can face shocks and recover from them. This ability to reduce vulnerability, mitigate effects and recover quickly requires resilience at all levels of society.

The cohesion of European society will depend heavily on the strength of its convictions and commitment to its institutions, culture and identity. In times of crisis this requires that individuals work together, based on joint preparation and mutual trust, confidence and support. Such interaction is crucial to societal robustness and resilience, but it is complex and needs to be better understood.

In ESRIF's view, a purely technical-systemic approach is not sufficient. Societal resilience is equally, if not more, important – and that calls for preparedness and prevention. Operational and service-organisational infrastructures also demand close attention. Understanding the specific drivers of resilience and how they differ in time and place is essential for security operators and, by extension, providers of security solutions.

2.3 Trust

Security implies nurturing trust among people, institutions and technologies. Under conditions of threat trust enhances transparency and social inclusion. It plays a decisive role at the interface between citizens and governments, social services and institutions, information agencies, ICT and other technological systems, and local and global markets.

Trust refers to overall judgement about what can be expected from both people and technologies. It is a core component of security.

The human dimensions of security as embodied by trust will play a central role in the way Europeans face the dangers of the unknown. Trust demands that authorities communicate transparently on security matters: it is critical to a secure Europe.

Yet trust is not a 'given." It flows from a determined combination of direct human contact, informal transmission of knowledge, experience and tradition, culture, reputation, solidarity, expertise and communication. It rests on transparency, fairness and justness, but also enhances efficiency. This concept transcends all of ESRIF's work – be it border security (e.g. document and data treatment or "trusted traveller" programmes), protection of critical infrastructures (e.g. financial services and ICT networks) or crisis management.

The public must be reassured that:

- A sufficient level of protection is in place against the main known threats
- Main infrastructures and services are resilient
  people and organisations in charge of security and crisis management are well prepared

2.4 Interoperability

Security organisations increasingly face technical, operational, and human interoperability issues at their geographical and organisational borders. A vigorous political will to share assets and standards across Europe will empower us all in jointly handling the security issues posed by a progressively more interlinked world.

Interoperability implies that the resources of different Member States and EU organisations operate together effectively to carry out security tasks and missions, as foreseen via common EU capability planning. However, increasing interoperability can also lead to higher vulnerabilities.

The European continent is a patchwork of languages, laws, cultures, and habits that change at nearly every border. Without a doubt, Europe represents the world's most dense interoperability challenge. Its problems include:

- Communications networks of similar technology but incompatible with each other
- Power grids whose linkages cause negative chain effects such as outages but which are not easily synchronized for restarting (see 2005 power outage in Europe)
- Divergent emergency response procedures and inadequate cross-border language skills such as those that hampered Europe's transnational fire-fighting efforts effort in 2007

Taken together, the multitude of Europe's problems with territorial, organisational and cultural non-interoperability along its member states' borders enables criminal and terrorist organisations to exploit the patchwork's inherent weaknesses.

Indeed, certain problems such as new forms of financial fraud or cyber-crime have simply grown beyond the ability of individual nation states to deal with them. Europe risks falling prey to the vulnerability of its own diversity.

Thus, for Europe to guard against these threats investments in a seamless approach to security are essential. We need to strike a balance between the patchwork's richness and the efficiency of working together as one continent. The key enabler for this to happen is acceptance at all levels of our societies of shared 'ownership' of the problem and responsibility for solving it.

For example, if rescue workers from different Member States are to work together effectively and efficiently, innovative approaches are needed for rapid cross-border exchanges of information. We need innovate ways to unite security personnel across Europe.

This demands similar policy and investment approaches (geographical, organisational, or otherwise) at the operational level across borders, from tools and methodologies to training. A first step is to inventory and prioritise those domains and topics where standards are needed to guarantee interoperability at equipment and system levels.

ESRIF firmly believes this requires major research investments and joint approaches in the security sector.

2.5 A systematic approach to capability development

The growing complexity of security demands increasing sophistication in strategic foresight and risk assessment, modular generic capabilities and solutions at the system-of-systems level.

By definition, a joined approach to security in Europe is a major undertaking. As the number of independent actors increases, so will the complexity of effective information-gathering and decision-making. This calls for a well-balanced portfolio of modular and broadly applicable capabilities for generic security problems such as substance detection or information fusion. But it will have to evolve over time.

Fortunately, many concepts and challenges are similar in the security and defence areas, and across various security disciplines (e.g. police forces and private security services). These will benefit from close and systematic cooperation in capability development.

The emerging capabilities must be integrated with legacy systems in terms of technology, culture and institutions to produce system-of-systems solutions, with the latter able to evolve over time in response to risks and user requirements. Thus, modelling, simulation and field experimentation are indispensible aids to capability development.

Achieving effective and efficient systemic capabilities requires guidance from strategic foresight, risk assessment and monitoring activities, including ways to evaluate best value for research money.

2.6 Industrial policy

Europe has a strong extensive industrial capability and knowledge base in the security field, but represents a fragmented market. Rectifying this would open the door to global leadership in the security market, and spawn an efficient European industry, making our society best security solutions available to the world. This ambition requires a clear political choice and a persuasive European industrial policy.

An institutional market such as security is generally driven by regulations, not market forces. In a marketplace as fragmented as Europe's, using legislative and regulative guidelines to "level the field" for all stakeholders would encourage more private stakeholders to enter the sector. Yet industry will not invest and commit resources without incentives and future demand that is reasonably predictable: these, too, should be the aim of any industrial policy.

A stringent and comprehensive industrial policy framework for the security sector is thus necessary to increase the security of Europe's citizens and the global competitiveness of its security industry.

Such a European industrial policy framework should seek to:

- Motivate strong and widespread R&D activities (both public and private)
- Ensure the rapid transfer of the best results of innovation to market
- Foster general interoperability of solutions
- Provide common guidelines for capabilities that are jointly developed by the supply- and demand-side participants

Moreover, Europe's security and defence sectors share a large number of requirements and missions – a commonality that will only increase in the future. Industrial exploitation of these synergies and interoperability between security and defence solutions should be encouraged, as history is full of successful bi-directional transfers of knowledge and solutions.

ESRIF endorses the idea of creating a Lead Market Initiative in security. In a globally diversifying market, Europe can be a key supplier of technologically cutting edge, qualitative and effective security solutions. However, such solutions can only be successful on the world market if they are interoperable, flexible, modular, upgradeable, hardened, affordable and effective. Moreover, they can only be developed if all stakeholders are involved early on in regulatory policy and R&D processes, where a future joint science board could be envisaged, for example.

In sum, a co-ordinated legal framework is desirable both at national and European level to achieve a common understanding of the principles governing the security market. A common harmonized regulatory framework for security technologies and security research and innovation in Europe would allow industry to better focus its new industrial developments in view of user needs and market requirements.

2.7 Innovation

To preserve its security, Europe must have strong in-house scientific, technological and industrial competences. It is important to capitalise on this knowledge through pooling and clustering to maximize synergy between different technologies, stakeholders and services and in establishing a systematic interaction between demand and supply to ensure that security solutions are effectively tailored to meet operational needs.

Innovation is about finding new paths in research and development, and bringing the results to markets. But organising knowledge base is not sufficient—we need strong interaction between supply and demand sides to produce the right solutions.

To support the take-up of R&D results, security research needs to be grounded in a comprehensive policy approach. This would embrace the definition of initial operational security requirements and end-user needs to operational testing of solutions and their procurement and deployment. Such a process approach calls for the sustained engagement and commitment of all stakeholders.

Yet fostering true R&D innovation also requires incentives for high-risk research investment in the knowledge that not all innovative efforts in such directions are successful. That same risk factor also explains why such investment is difficult to justify according to strict business criteria. ESRIF therefore advocates that a certain percentage of EU and Member State security research funds be reserved for high-risk risk investment that otherwise would not see the light of day.

2.8 Security by design

Securing the future will require that security be treated as integral part of any given system, process or operation from the point of conceptualisation onward. Current add-on security solutions no longer suffice, Europe needs a systemic approach to security.

New capability driven, standardisation concepts must be developed, focusing on the performance of security-related solutions rather than on the level of technical equipment specifications. This security-by-design approach will enrich the market and allow a broad range of industries to come up with compatible, interoperable and flexible solutions to meet customer needs.

Incorporating security in new systems, together with safety and environmental integrity, at the earliest stages of the design process has an ongoing and positive impact. Critical infrastructures and services will need innovative technical solutions and capabilities, and intense preparation of the operators to minimise the impact of incidents and ensure fast recovery. At nuclear and airport facilities, for example, high standards of security require that design takes full account of security requirements for both operational and crisis scenarios right from the start. Security-by-design affects other life-cyle aspects too. Legacy systems may need updating to new security levels. Maintenance and repairs must guarantee safe and secure systems for the public. Periodic testing is imperative, as is the continuous training of operators.

The security-by-design also directly concerns quality of emergency management, where personnel at all levels must be able to communicate efficiently with first responders and society at large. Raising public awareness about security and the nature of threats, and how to interact with emergency forces during crises are important goals.

The first analytical phase of a security lifecycle is greatly enhanced if detailed standards and guidelines regarding the product's applications are immediately available. It is common practice today to conclude the realisation phase (covering detailed design to manufacture) via verification of performance and design, so that a product can be certified early on. In this regard, some type of European security label could be a useful instrument for promoting a common "seal of quality" for security equipment, capabilities and solutions.

2.9 Awareness raising through education and training

Education and scenario-based training contribute significantly to the overall acknowledgement and recognition that security is a common responsibility of all stakeholders, especially, policymakers, regulators and citizens.

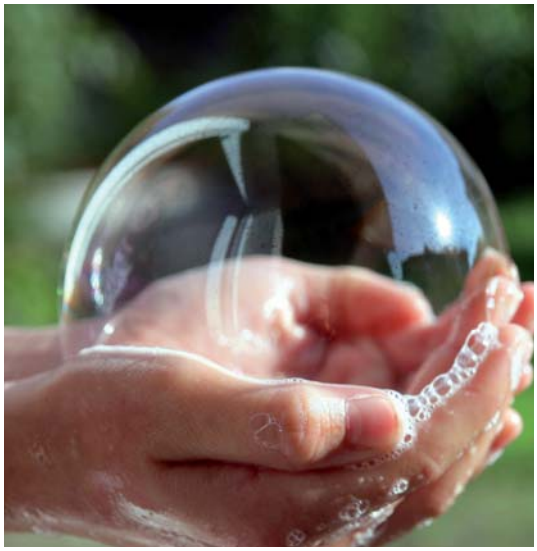
Education and training in the security sector is a common responsibility of all stakeholders: security officers, policy makers, law enforcement agencies, civic society, industry, research organisations, academia and the media.

To achieve resilience, specific programmes are needed to reach out to the wider public to raise awareness of threats, risks and vulnerabilities and to improve its understanding of policies and the technological solutions required for security. Priority should go to initiatives involving the media and the special role they play in communicating about security crises.

Security training across Europe is diversified and often under the direct control of local authorities or a specific public service. For effective interoperability, transnational initiatives in training and education for security functions and tasks should greatly increase experience and the exchange of best practices. Tying these initiatives to existing networks for professional training such as CEPOL – the European Police Academy – would ensure rapid progress in this important field.

The use of virtual reality, "gaming" and other simulation environments offers considerable training opportunities in the security field. Their use would increase informal learning, foster communities of practice and facilitate the translation of operational lessons learnt into learning environments (and vice versa). Similarly, scenarios would provide realistic contexts and environments for complex crisis management operations and offer an important means for delivering training solutions in the future.

3. European Security Research and Innovation Agenda (ESRIA)



ESRIF's task is to develop a strategic plan for security research and innovation over the next 20 years. After analysing the risks and challenges facing Europe during that period, ESRIF defined key messages to set the context for future research and innovation activities, and developed an agenda for it. The result is the European Security Research and Innovation Agenda or ESRIA.

ESRIF has chosen to structure ESRIA, which is at the heart of its work, in five clusters.

3.1 Methodology and visualisation

The ESRIA framework and structure shaped the core of ESRIF's work, as based on the contribution of ESRIF's 11 working groups regarding capabilities and technologies across the five clusters.

Capabilities – the ability to perform a specific task or operation – served as the primary foundation and were derived from a close analysis of the security risk and challenges.

The capabilities are catalogued according to their urgency:
- Immediate actions
- Actions required in the short-to-medium term
- Actions to be supported for the long term

Due to the huge number of capabilities generated by the working groups and the degree to which each varied in terms of granularity and width of description these are arranged in functional groups for ease of visualisation.

The technologies and processes identified are transversal and thus applicable to more than one capability. In the visualisation, they are represented in terms of "Technology Readiness" as:
- LOW – requiring basic/scientific research
- MEDIUM – requiring advanced/applied research
- HIGH – requiring immediate industrial implementation

They are also represented via a time-scale for their development. Three periods are identified : from the present to 2013 (in FP7); from 2013 to 2020 (in FP8) and, finally beyond 2020.

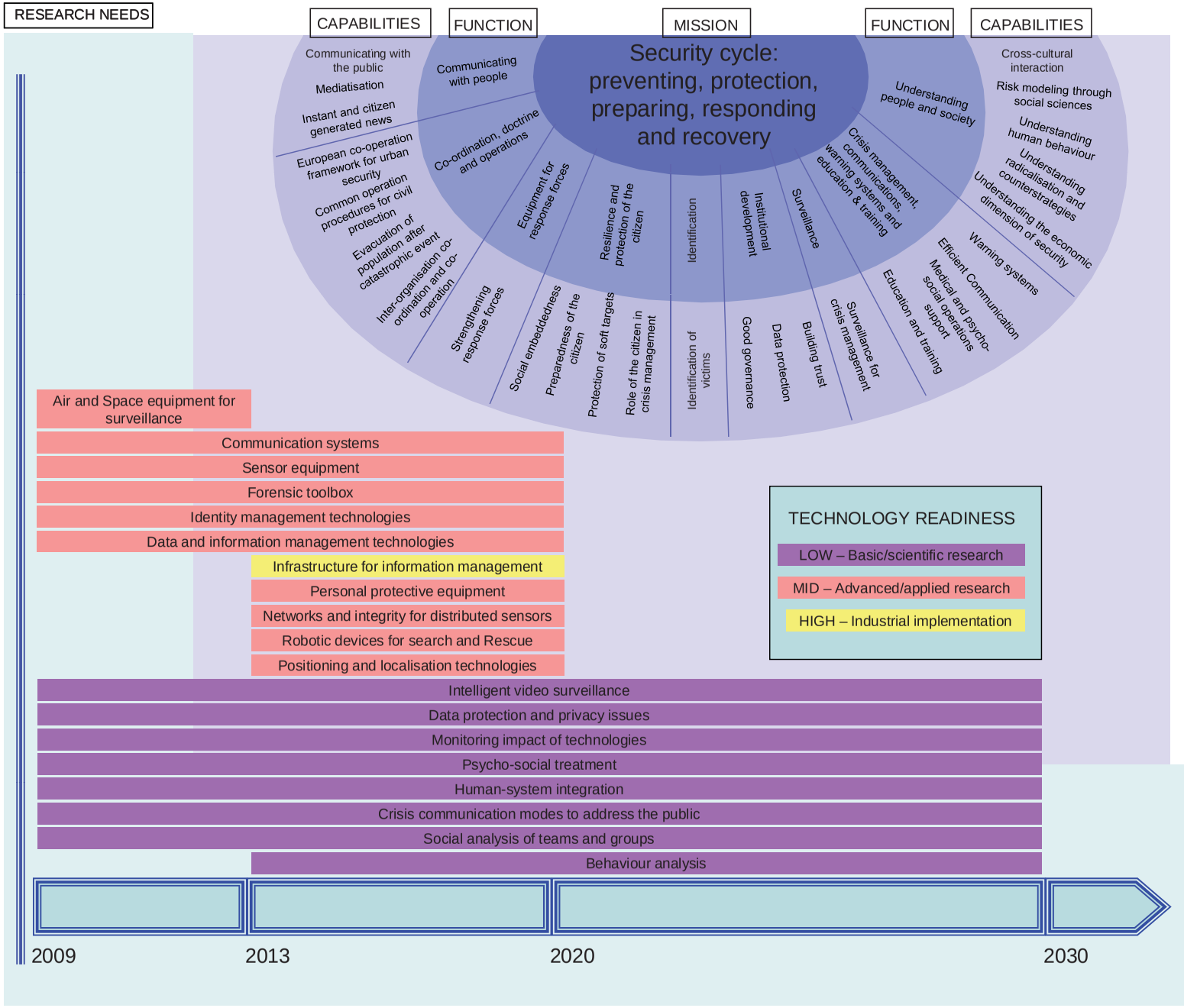
In addition any underlying documents can be found in Part II.

On the left side of the chart, a list of systemic needs is defined to indicate the drivers of innovation processes.

SYSTEMIC NEEDS

- Education / training for citizen
  - on security issues and available solutions
  - for crisis management operations
- Education / training for decision makers, regulators, security forces and media
- Models for field cooperation
- Scenario simulation tools (incl. virtual reality) for rapid assessment during crisis
- Modelling and simulation tools of residential areas and built infrastructure
- Tools for Common Operational Picture
- Cost / benefit assessment of prevention actions
- Information / warning methodologies
- Organisation Governance / Decision making
- Methods and infrastructure for information sharing
  - providing public with updates/ alerts/ warnings
  - private reporting about noticed unusual /suspicious activities
- Standardisation of rescuer identity, skills and credential for interoperable command and control cooperation , for a more efficient international cooperation
- Operational concept of social resilience
- Knowledge base of researchers for policy advice
- Building of trust in authorities, and systems, through education, training and other forms of long-term trust-building interactions

RESEARCH NEEDS



3.2 Securing people

Ideally in a secure society, citizens live in an environment of dignity and respect for their privacy rights and their possessions. Citizens exist within communities which have a well-developed social coherence, where the individual and groups are connected to their wider societal living environment. However, the same society has to cope with threats from criminal, terrorist and natural sources. In order to sustain its future, society must be prepared for such attacks and develop knowledge and tools to be resilient.

Securing people through preparation requires strengthening of several critical capabilities not least of which is protection of persons and residential areas, and the prevention of violent radicalisation and criminalisation. In a cross-cultural, -generational and -societal context, strengthening measures that prevent organised crime and radicalisation are a priority. Education has a key role in this process and not only within Europe.

Surveillance is increasingly a central element of security management and takes place through a number of means, from closed circuit television to various biometric tools. As these tools are developed, the impact on European values of the relation between surveillance and civil and human rights, the place of new technologies in society role, their role in security crises and their consequences for the individual remain poorly understood. Future research and innovation should carefully assess these societal questions and their links with Europe's security.

A special emphasis is given to security of Europe's cyber domain. The extraordinary development of internet technologies and applications during the last decade has triggered parallel development of new types of criminality. Organised crime is increasingly involved in such activity.

3.3 Civil Preparedness

Across Europe public services and their partners have the responsibility to prepare for security incidents, to manage them efficiently and to execute rapid and effective interventions to resolve incidents and thus enable the populace to return to normality. The public has its own role to play in this preparation, too. It is important that, in case of a crisis, people behave appropriately and in the most organised way. For that purpose communities need adequate information about the potential security incidents in their environment.

Citizens are contributing to the prevention and response to security incidents. Protection of high-density living or gathering areas for people versus those individuals with a higher risk profile: both challenges require well balanced preparatory measures (including personal protection, procedures and shelter areas). Rapid building-up of shared situational awareness of a security incident together with information sharing among all stakeholders is critical. Response organisations need a shared understanding of command-and-control (C2) structures to deliver prompt and effective responses. Education and training of decision makers, public services and citizens is mandatory. Organisation of exercises should be facilitated by the use of new techniques for modelling, simulation and serious gaming.

Testing and evaluation of new technologies by first responders is vital. There are not enough opportunities to exercise with technologies still in development. This is an innovation priority for the future so that new technological solutions can be optimised under real conditions in close co-operation between developers and users.

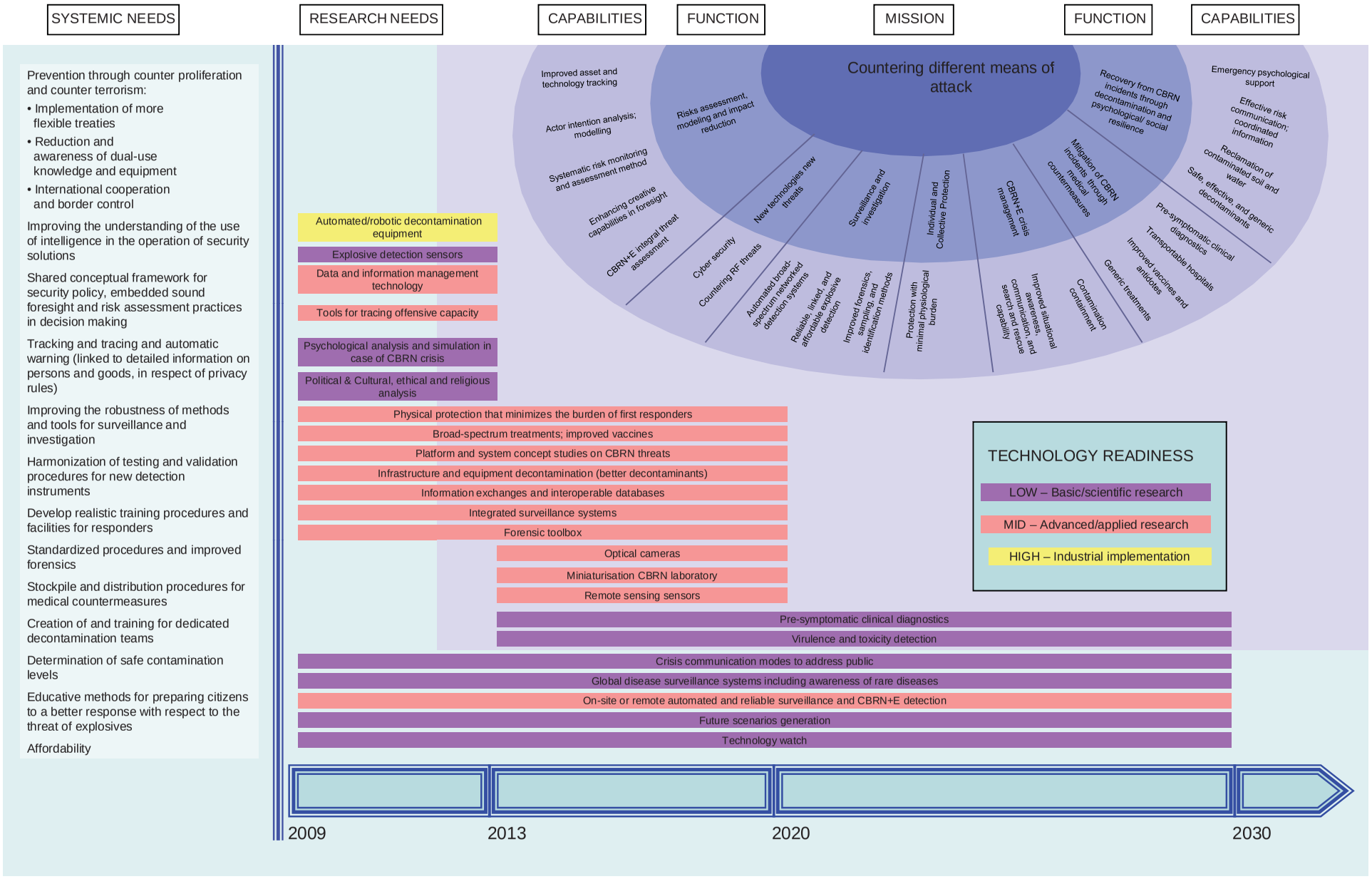
3.4 Crisis Management

Despite all efforts deployed to prevent incidents or accidents, crises will occur.So it is critical to rely on strong crisis management capabilities. The origins may be more diverse than before, but the requirements for an efficient management are getting stronger. Public expectations of first responders are on the rise. The public demands faster intervention, more efficient medical and psychological support, better information about situations and a quicker return to normal life, whatever the nature of the incident or accident.

Understanding the situation is a key priority for rescuers. They are now benefiting from man new technologies that increase their situational awareness. New sensors, for example, facilitate more accurate visualisation of a situation, whileC2 infrastructures now rely on the compilation of a growing amount of information. Research efforts must be pursued in this domain and for technologies that promote better treatment and management of victims.

How security incidents are perceived and understood by the public is crucial for their overall impact and resolution. Each individual has his own resilience capabilities that need to be enhanced and deployed in a crisis situation. Enabling the public to actively contribute to crisis solutions requires research as to how this can best be achieved. Media are also central to this perception. Existing research on media does not adequately account for the interplay between media and security, and in particular, the ability of media to significantly determine the outcome of such incidents. The Security Research and Innovation Agenda will provide a focus for addressing these topics.

Effective treatment of victims can require biographic and biometric information. In the same way, details of rescuer identity, skills and credentials are required to facilitate efficient, interoperable command-and-control cooperation. Therefore, general data protection standards need to be adapted to emergency circumstances. A number of crises have regional or international impact: their management involves multiple agencies. Coordination between these agencies raises specific issues about their differences in organisation, methods, language and culture. Interoperability at the communication level is key. Improving our understanding of the ability of such organisations to cooperate flexibly is a priority.


SYSTEMIC NEEDS
RESEARCH NEEDS
CAPABILITIES
FUNCTION
MISSION
FUNCTION
CAPABILITIES
Prevention through counter proliferation and counter terrorism:
• Implementation of more flexible treaties
• Reduction and awareness of dual-use knowledge and equipment
• International cooperation and border control
Improving the understanding of the use of intelligence in the operation of security solutions
Shared conceptual framework for security policy, embedded sound foresight and risk assessment practices in decision making
Tracking and tracing and automatic warning (linked to detailed information on persons and goods, in respect of privacy rules)
Improving the robustness of methods and tools for surveillance and investigation
Harmonization of testing and validation procedures for new detection instruments
Develop realistic training procedures and facilities for responders
Standardized procedures and improved forensics
Stockpile and distribution procedures for medical countermeasures
Creation of and training for dedicated decontamination teams
Determination of safe contamination levels
Educative methods for preparing citizens to a better response with respect to the threat of explosives
Affordability
Countering different means of attack
Improved asset and technology tracking
Actor intention analysis; modelling
Systematic risk monitoring and assessment method
Enhancing creative capabilities in foresight
CBRN+E integral threat assessment
Risks assessment, modeling and impact reduction
New technologies new threats
Cyber security
Countering RF threats
Surveillance and investigation
Automated broad-spectrum networked detection systems
Reliable, linked, and affordable explosive detection
Improved forensics; sampling, and identification methods
Individual and Collective Protection
Protection with minimal physiological burden
CBRN+E crisis management
Improved situational awareness, communication, and search and rescue capability
Mitigation of CBRN incidents through medical countermeasures
Contamination containment
Generic treatments
Improved vaccines and antidotes
Recovery from CBRN incidents through decontamination and psychological/ social resilience
Pre-symptomatic clinical diagnostics
Transportable hospitals
Safe, effective, and generic decontaminants
Reclamation of contaminated soil and water
Effective risk communication; coordinated information
Emergency psychological support
Automated/robotic decontamination equipment
Explosive detection sensors
Data and information management technology
Tools for tracing offensive capacity
Psychological analysis and simulation in case of CBRN crisis
Political & Cultural, ethical and religious analysis
Physical protection that minimizes the burden of first responders
Broad-spectrum treatments; improved vaccines
Platform and system concept studies on CBRN threats
Infrastructure and equipment decontamination (better decontaminants)
Information exchanges and interoperable databases
Integrated surveillance systems
Forensic toolbox
Optical cameras
Miniaturisation CBRN laboratory
Remote sensing sensors
Pre-symptomatic clinical diagnostics
Virulence and toxicity detection
Crisis communication modes to address public
Global disease surveillance systems including awareness of rare diseases
On-site or remote automated and reliable surveillance and CBRN+E detection
Future scenarios generation
Technology watch
TECHNOLOGY READINESS
LOW – Basic/scientific research
MID – Advanced/applied research
HIGH – Industrial implementation
2009
2013
2020
2030

3.5 Explosives

Explosives are unfortunately the vector most often used by terrorists. Preventing access to explosives, their precursors and the technology to manufacture them remains very difficult. Thus the capability to detect them before they can be activated is critical. Mitigating existing and new means of attack such as improvised explosive devices (IEDs) is a permanent challenge for society.

Sustained research efforts must be pursued in this domain regarding the detection of all types of explosives –unattended or man-carried –including remote detection capabilities. Detection equipment must be transportable and easy to use. New solutions allowing very fast intervention are needed to neutralise, even partially, unattended potential explosives. The development of new markers in manufacturing and the ability to track compounds that identify the source of their components would also be very beneficial for detection and investigation.

Coordination at European level, mutual use of methods and expertise to counteract violent means of attack and support for the development of improved harmonised regulation should be encouraged. The existing European Network of Explosive Ordinance Disposal Units could be an appropriate channel to support such action.

3.6 Chemical, Biological, Radiological, Nuclear

Chemical, biological, and radiological incidents, be they intentional or accidental, are major risks for Member States. The scale of these risks ranges from attacks by states to the use of small, improvised devices by terrorists. The spread of technical knowledge and capabilities that can enable dedicated individuals or groups to build CBRN devices is a major concern.

While the impact of a CBRN incident on society can vary dramatically, it is in any case likely to be immense. Prevention is crucial and should receive particular attention by equipping intelligence agencies and policy makers with better information analysis tools. Consequence management to overcome CBRN attacks and hoaxes is also of extreme importance. This requires development of more effective and reliable detection and identification capabilities, including detection networks, data fusion, distribution of signal output and decision support tools.

Another important capability gap involves safe containment and decontamination procedures that provide quick effect without harmful side-effects, not least of which is the environmental clean-up of these materials. Special focus must also be placed on understanding the metrics of the psychological and sociological consequences of CBRN incidents and thus how to design proper countermeasures (education, communication and recovery).

Although Europe has developed good standards for laboratory safety, the advent of dual-use technologies and the proliferation of know-how for the malicious use of biological agents have increased the need for socially-grounded approaches to bio-security. Moreover, the continuing threat of global pandemics –with its potentially devastating impact on the health, social and economic stability of European society – sharpens these security concerns.

3.7 New technologies, new threats

Having identified the sustained research requirements to deal with generally known means of attack, ESRIF recognises that while new technologies are of paramount importance for to improving security, they may also foster new or transformed threats. Formerly unaffordable and high-level technologies may become widely available for malicious use; e.g. high-power microwave or radio frequency jamming devices can be constructed using simple, off-the-shelf components while mobile devices are used to initiate or detonate homemade bombs.

Although certain future deliberate misuses of technologies can be foreseen, most cannot. There is no doubt that rapid evolution in ICT/cyber security and its misuse will continue and even accelerate. Some technologies already identified as candidates for

misuse are nano-technology, artificial intelligence and 'synthetic biology' (i.e., the use of DNA technology to 'engineer' living organisms). These threats will have to be continually monitored and countered.

Therefore it is very important that security research programmes maintain a strategic "technology watch", and foresight activities, regarding potential and real threats that may arise from technological development. This should include processes by which technologies interact with socio-economic developments at large.

SYSTEMIC NEEDS

Adaptive simulation and modelling tools development for crisis situations for CIs

Common procedures, protocols and interfaces enabling rapid re-onlining of affected CIs.

Sensibly Interoperable Systems

NEC concepts

Analysis of the standardisation needs in the various segments of the security market.

Analysis of the conditions allowing the definition and implementation of a European Security Label.

Analysis of the economical impact.

Promotion of dynamic standardisation.

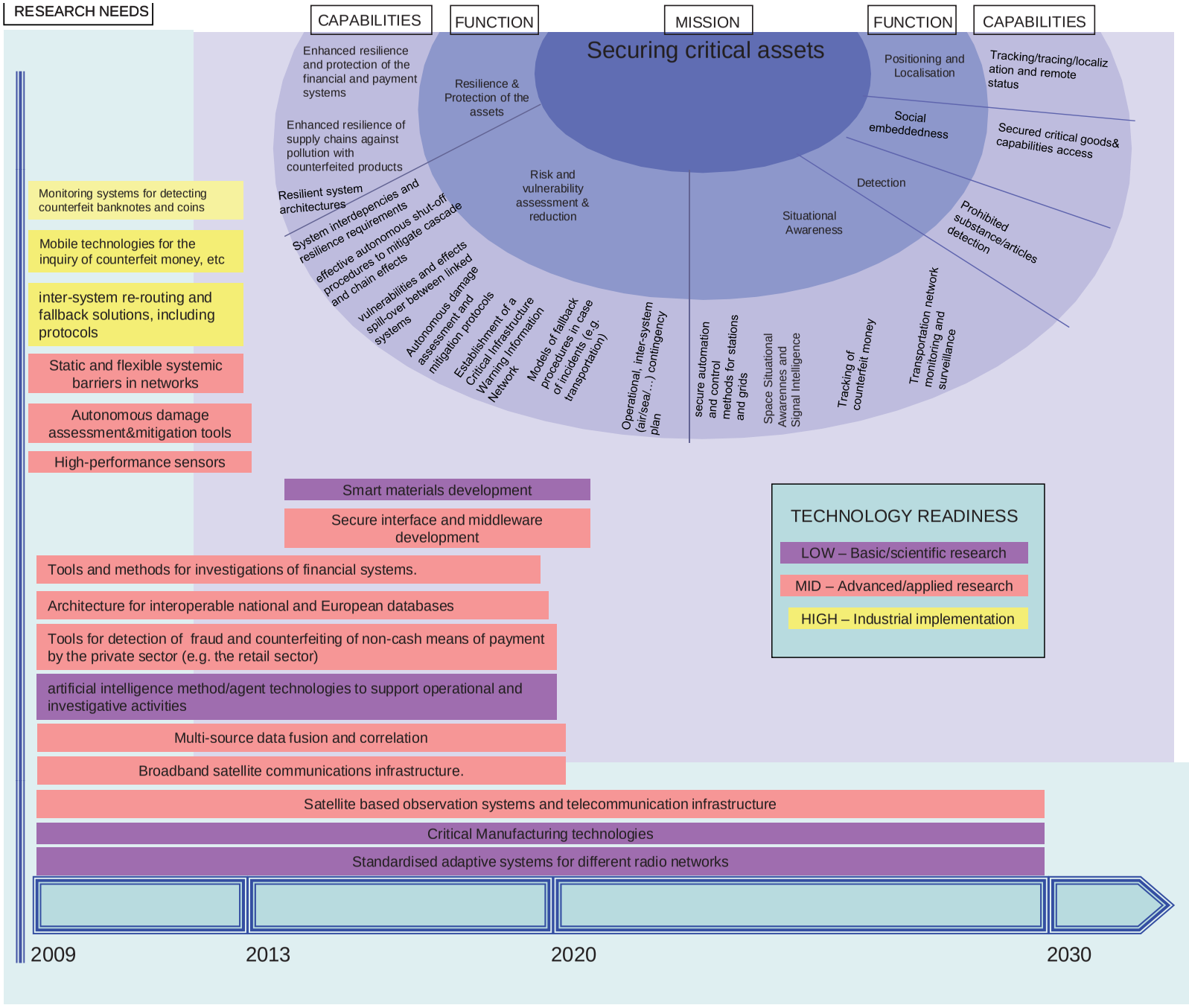
Elaboration of a common policy on the development and implementation of methods for financial investigations.

Methods for training of relevant personnel in the private and the public sector for fighting against organised financial crimes.

Rules and integrity standards for a higher transparency of financial systems.

Coherent international approaches for improved branding of products with better tracking and tracing of goods along supply chain.

RESEARCH NEEDS



3.8 Security of Critical Infrastructure

The security of Europe's critical infrastructure is naturally a focus of security research and innovation. Given that certain infrastructures provide essential services to society and economy –with some of them directly interfacing with the public such as water supply or ICT – their criticality is obvious. Other CI systems are less visible, but also essential to the functioning of societal elements such as space-based navigation, which offers more than just localisation tools. Many of these CI functions are technologically and operationally interconnected, of which their exact possibilities and potential risks need better understanding.

Therefore, as a general research topic for critical infrastructure security, these interconnections and interdependencies need to be thoroughly studied and analysed, with separate analysis results placed in a broader context and matched against similar studies. This will boost awareness of potential spill-over and chain effects that need to be prepared for. On this basis, reliable, effective and proactive countermeasures regarding existing and foreseeable systemic vulnerabilities and risks can be developed. If this is combined with advanced simulation and modelling tools – both for interconnected and stand-alone system operations, and impacts and malfunctions – then end-users and crisis management experts can be provided with powerful instruments for prevention and preparation. This should lead to higher systemic and societal resilience and security in general.

A future awareness group should analyse the potential future criticality of emerging and evolving technologies. This will enable end-users, researchers and manufacturers to jointly define security protocols and architectures early in the design process, which is in line with one of ESRIF's key messages. The proposal to expand the definition of critical infrastructures and analyse Europe's industrial landscape for critical manufacturing capabilities and capacities must be seen in this wider context as well.

3.8.1 Security of Natural Resources

Securing access to essential natural resources, strategic supplies and consumables or their substitutes is of high importance to European security. Many raw metals and salts are essential for the production of electronics, though most of these resources lie beyond the Western world. Access to adequate quantities of food and water is not likely to be an issue for Europe, but guaranteeing sanitary and tamper-free transport conditions for resources will be. ESRIF considers that the definition of critical infrastructures be expanded to include the supply of natural resources, with all research consequences connected to it.

This will require two main research approaches: Firstly, natural resources need to be defined and analyzed for their criticality to our societies and economies. This also refers to points of origin, inherent security issues and potential substitutes. The latter point transcends the topic of security and will require joint research efforts with other fields such as basic chemistry research. Beyond technical aspects, this is also a security policy issue, since it points to a definition of Europe's vital economic interests that need to be secured. In this regard, security research could help lay the groundwork for formulating a crucial aspect to European foreign policy.

Secondly, secure transportation of foodstuffs from source to consumer – from "farm to fork" – needs achieving. Seamless traceability before and along the supply chain is a key requirement here, limiting malicious attempts at tampering (e.g. contamination or fraud) and supporting monitoring functions for product recall in emergency cases. Special requirements also apply, such as broad detection capabilities and affordable networkable biosensors in certain supply networks such as water supplies. Not only will this require research into detection and identification of all known contaminants, but also the development of marketable sensors.

3.8.2 Energy

Europe is heavily reliant on its power generation and transmission grids to ensure that the power requirements of individuals, businesses and states are met. However, Europe is not self-sufficient in primary energy sources (gas, oil), so to reduce its dependency on other regions and to improve its resilience, investment in novel and/or more efficient energy generation methods is necessary. Energy security research will need to focus on innovative automation and control methods for power and energy generation, and for distribution grids. In particular, monitoring the integrity of a power system is an important element to ensure continuous energy supply.

ESRIF is acutely aware that as a result of the EU policy, a significant increase of renewable ("green") energy will be evident. With multiple locations of relatively solar energy and wind farms of different sizes comes the challenge of securing their infrastructure. In certain environments such as marine settings the challenges will be particularly difficult. Research can provide meaningful insights and solutions to these challenges.

Guaranteeing energy security inevitably implies securing energy supplies. Improving the security of the energy supply chain with technology and improved organisation will minimise additional security measures that may be required at a later stage. Similarly the decentralisation of power generation could increase resistance to disruptions and failures of energy supply networks, while reducing transmission losses and increasing efficiency in use of the overall system.

However, the large-scale integration of renewable energy sources into existing energy systems is challenging. Further research and development of new energy storage technologies is needed to manage the fluctuating and intermittent character of these energy sources. Besides development of renewable energy sources, an adequate electricity mix – including conventional power plants – is required to guarantee security of supply.

A secure European energy security is related to all other critical infrastructures and enhances the robustness of the European economy.

3.8.3 Transport

Transportation of goods and people will remain a critical area for security research for the next 20 years. Understanding the vulnerabilities of different modes of transport (i.e. rail/road/plane/ships, etc.) in the three environments of air-sea-land requires further research and alignment with existing research programmes. Future trends in transport must also be secured, while designing security into the fabric of transport infrastructures and means will require reliable output from research programmes.

Europe is heavily dependent on regional and global movements of goods and people; the high degree of interdependence between transport types focuses research requirements on systemic resilience. Comprehensive research into such interdependencies and the drafting of operational contingencies and their legal and regulatory implications is necessary here.

As with all spatially dispersed critical infrastructures, prevention measures need to be broad but also focussed on nodes (air-/seaports, railway stations, hubs). Therefore, the question of location, tracking and tracing remains a research priority, along with devising appropriate identifiers of attacks, sensors and networks and, finally, transmitters for incident information. This will necessitate co-operation not only within Europe, but with countries of close proximity and/or high relevance.

Tools that identify prohibited and dangerous articles swiftly and reliably need to be enhanced much further than the current generation of technology used today –not only in terms of speed and broad applicability (i.e. non-metallic detection) but also for remote detection, large throughput environments capability, etc. Aviation, for example, needs improved detection capability for explosives and other materials that can damage aircraft and airports.

3.9 Security economics

European security research should analyse in its programme all economic impacts of security aspects, investigate the economic causes and consequences of insecurity, and the direct and indirect costs of security policies and how they contribute to or hinder economic growth. ESRIF considers that analysis of the economics of terrorism, for example, -needs to be across-the-border due to globalisation.

Understanding how perceptions and fear of terrorism shape behaviour is also important in addressing its economic impact. Evaluating the cost-benefit relationship of security measures, even if difficult to assess, is important. Cost calculations should place specific emphasis on less visible impacts, including increased hidden costs, decreased efficiency and trans-boundary impacts such as the interaction between security behaviour and economic growth over time.

In addition, society needs basic market data to understand the security sector. Baseline data analysis may help to reveal the basic conditions and the sector's structure, conduct and performance. These are essential requirements to carry on any policy in this sector. Furthermore, market data about shared competencies with other transversal sectors such as ICT will improve our understanding of this market.

SYSTEMIC NEEDS

Develop **interoperability** requirements (architectural, technical, operational etc.), aiming at agreed processes and standards

Promote **risk analysis**, including scenario development and vulnerability modelling

Further harmonised security level of **identity documents**

Sharing and **pooling** of surveillance assets

Development of **education and training** for all stakeholders on threats and preventive measures, including use of simulation-supported training methods

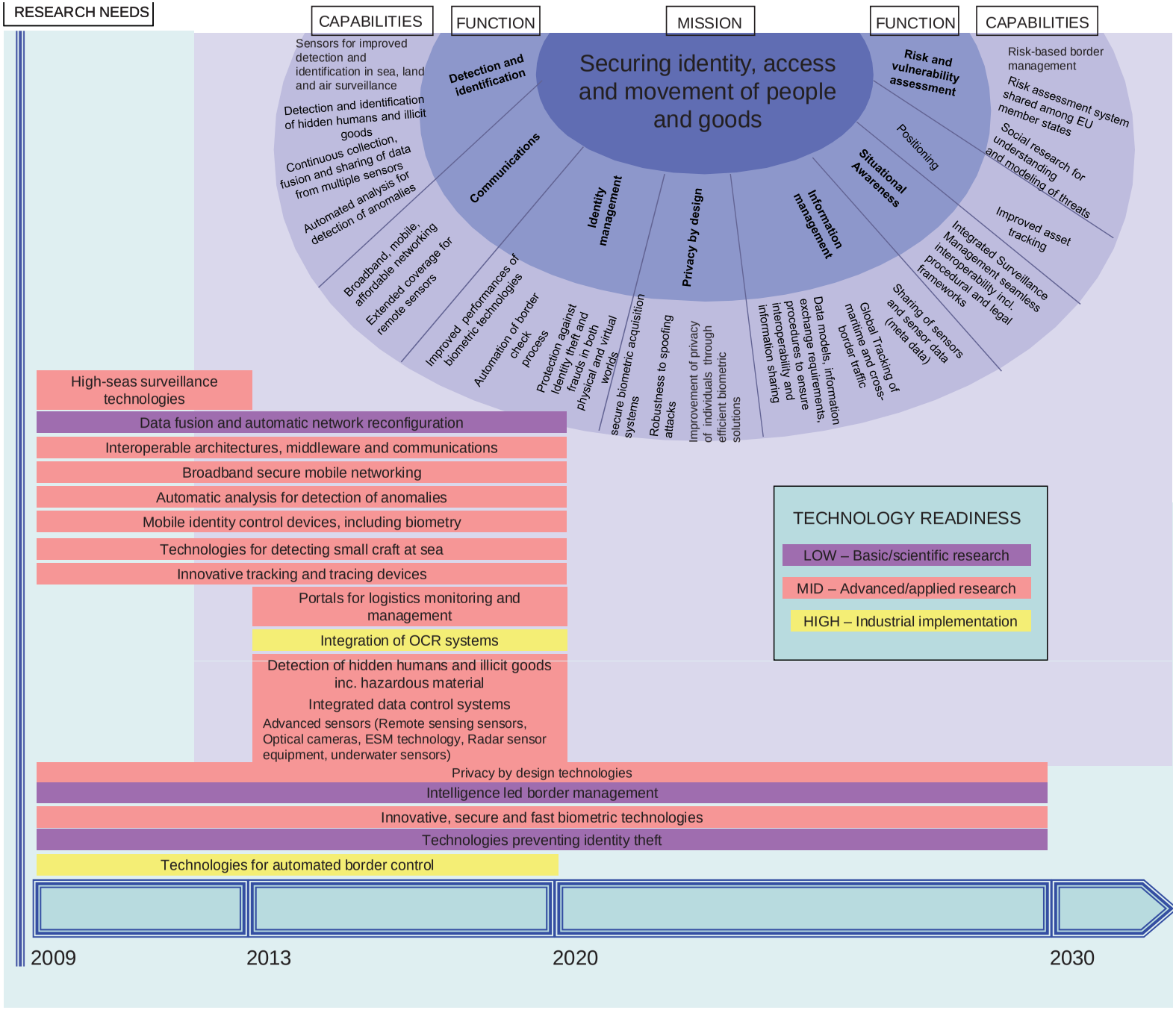
Development of a common information sharing environment for the EU maritime domain

Large scale deployment of advanced technical equipment supported by significant cost reduction and lower cost of ownership (reliability, easy to maintain and use)

Harmonised privacy protection for identity management, development of Privacy Enhancing Technologies (PET) solutions

Harmonised global border control, in order to manage the technical and legal complexity arising from the increasing number of electronic travel documents, develop standards required to ensure true interoperability of secure documents and systems, and by defining precise common rules of creation, distribution, update, exchange and revocation of certificates between the EU Member States

RESEARCH NEEDS



3.10 Border Security

The main focuses in the field of border security are the efficient and effective control of the flow of people and goods at border crossing points, and surveillance of border areas – land, sea or airspace – beyond those border crossing points. Detection of anomalies in large, regular flows and the use of mobile technologies in mobile environments such as trains and boats are important topics. For the usage of mobile devices it is important to implement secure data transfer technology. Proactive methods of processing ID checks and controls have to be developed.

Research is needed to improve current systems for checking people and scanning goods at border crossings in a secure, convenient and efficient manner. This includes biometrics for identification of people and sensors for screening goods. Furthermore, a holistic approach to border management, including an understanding of border activities within and beyond Europe, is needed to ensure efficient border management.

Another area where research is needed is sensor and information systems for detecting non-cooperative and non-registered vessels at sea, and for detecting anomalies in the traffic flow.

Interoperability is essential to make border security more efficient. Research must cover technical interoperability aspects between deployed systems, as well as interoperability at the organisational level, taking into account the diversity of cross-border cultures. Interoperability may also be enhanced through harmonised or common operational procedures for development, acquisition and training.

The ultimate output of research and innovation initiatives must be affordable and user-friendly equipment. Social science research for understanding and modelling various risks related to border security is also of crucial importance.

3.11 Identity management and protection

Citizens expect high levels of security from digital systems. The absence of written and visual proof has given rise to demand for high levels of identification and authentication of parties and transactions. Without adequate protection, personal data and individual credentials are vulnerable in a virtual world. ESRIF proposes to address research topics that enhance the accuracy of biometric devices by developing strong authentication processes and technologies, and that improve methods of secure online authentication of individuals, regardless of which digital identity element they use.

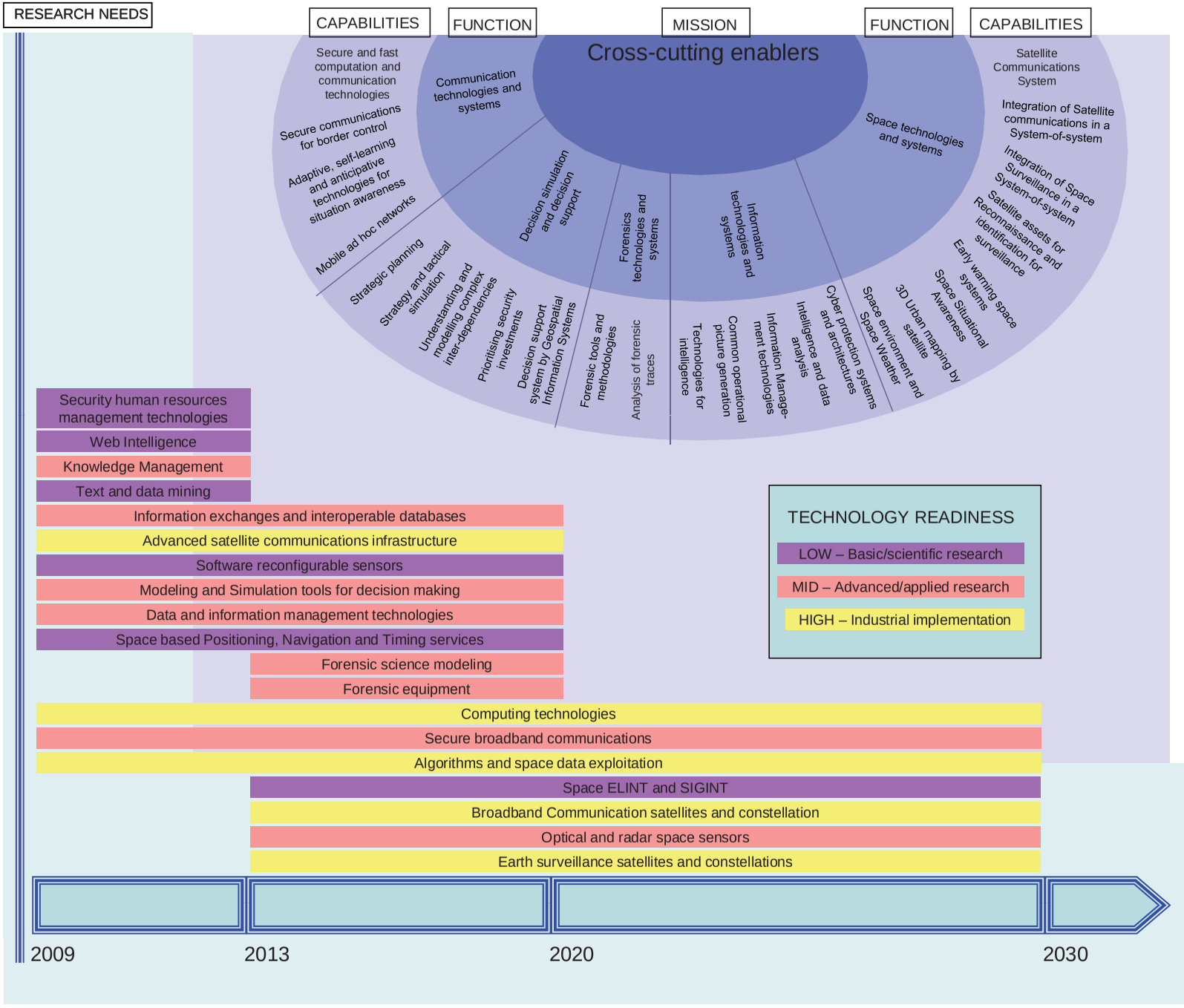
Digital identity is increasingly an integral part of an individual's identity. The particular set of data linked to "digital identity" should be protected using the results of robust research. ESRIF has identified research domains to counteract identity theft. The current lack of solutions costs companies, countries and citizens billions of euros in fraud and theft, and undermines global and financial security. Moreover, to combat fraud systems and technologies should perform mutual recognition between regional, national and/or European systems.

Correct identification of individuals within health systems, together with appropriate medical records, is always a priority. Systems need to be developed that support unavoidable exchanges of patient information on a national and transnational basis but which protect individual identity and privacy rights at the same time.

ESRIF advocates implementation of a 'privacy by design' data protection approach that should be part of an information system's architecture from the start. To ensure real effectiveness, this privacy-by-design" protection should combine general privacy controls, a separation of data of different streams, privacy management systems, and effective 'anonymisation' of personal data. Research in these areas must be pursued to ensure that effective solutions are available as soon as possible.

SYSTEMIC NEEDS
International applicable unique interfaces, protocols, connectors etc. for trusted exchange of sensitive information
Statistical methods, and tools, for objective interpretation. Standardized European protocols
Training and education methods for crime scene analysis
International standards for trace recovery
Resilient architectures design
Flexible technical and operational interoperability of security actors
Technical and operational interoperability
Access protocols to sensitive data as per access rights
Assessment of modern management concepts and tools and their possible use for innovating crisis management
Analysis of novel system of systems approaches like the NEC for civil security applications
Systematic and coherent capability analysis and development process which could be referred to on European and Member State level
Systematic evaluation of approaches leading to consolidation of methods to model complexity and interdependencies

RESEARCH NEEDS



3.12 Information and Communication Technology (ICT)

Information and Communication Technologies are crucially important for European security as they are critical infrastructures in themselves and also enablers upon which other services and sectors rely. ICT networks need research to increase systemic resilience, e.g. via intrusion detection, 'self-healing' networks or semi-intelligent data filtering.

At the same time, development of secure ICT-solutions, software and hardware, including mobile secured communications, will continue. Combined with increased robustness of electronic identities and more stringent authentication processes, the prevention of fraud and misuse will need to be studied. Virtualisation, encryption and authentication, communication algorithms, high performance computing, filtering, education and training activities, ICT's transcendence of borders: all are key research topics in this area.

An increasing number of citizens use ICT at home and at work and may be affected by security threats via the internet. Current ICT solutions provide a certain degree of anonymity for perpetrators of criminal acts. Stronger security will severely hamper the detection of criminal acts, but will also limit the freedom for individuals to use technology as it was intended. Research into legal frameworks is needed to support forensic and evidence gathering in this environment: current mechanisms are not interoperable and jurisdiction remains a challenge regarding the location of a perpetrator versus the location of his criminal act, for example.

3.13 Space

Space assets are today key enablers for a wide spectrum of applications. Space services, complemented by other services, notably airborne ones including UAVs, have increased importance, providing critical capabilities in addressing some of the societal challenges that Europe and the world face in the field of civil security, emergency response and crisis management. Consequently, ESRIF has identified the role of space as vital in different security-related technological domains.

Tools for environmental monitoring and security will contribute to provide an integrated infrastructure, combined with in situ data gathering to cover a broad range of services and applications in environmental monitoring, early warning and crisis management. Real-time monitoring of natural and man made disasters is a necessity. The capacity to monitor from space of weather phenomena and access their effects on power, gas and telecommunication infrastructures is imperative. Mechanisms for data exchange on abnormal critical climate events and on detection as well as autonomous reaction capability also require further research and development.

Satellite based surveillance, which benefits from improved observation and sensing capabilities, together with international cooperation between civil and military stakeholders, offers excellent opportunities. ESRIF also sees a need to continue research on new imaging/sensing capabilities from various platforms: microsatellites, sensors (optical, hyper spectral), and development of standard satellite platforms with autonomous capabilities to increase responsiveness. Future European and multilateral telecommunication projects will increase the capability in space of secure broadband communication systems to be deployed in a very short time to back up/substitute terrestrial communications infrastructure.

The gradual deployment of the EU's 'Galileo' constellation of navigation satellites will provide a wide range of added value services in support of security. Positioning and timing capabilities together with continuous and low-cost monitoring of infrastructures and natural phenomena (e.g. volcanic eruptions, land-slides, floods etc.) will provide a much needed service to users who require accurate information for Search and Rescue (SaR) teams.

Given the scale and cost of investment in space technology, it is equally important that we invest in security for the assets themselves to ensure proper access and operational capability any time, under any conditions. Advanced anti-jamming and encryption techniques, the hardening of systems and equipment against electronic attacks, autonomous protection tools, distributed capabilities (over a number of satellites): all are examples of security measures that can be implemented with effective research results.

3.14 Evidence and forensics

Due to the growth of international organised crime, forensics need strengthened capabilities regarding cybercrime, the misuse of financial and payment systems, counterfeiting of products, money laundering and the theft of valuable goods during transport. An effective European approach demands cross-border exchanges of law enforcement information together with a comprehensive accreditation network to investigate cross-border crime. This approach should include the creation of standardised protocols, in a formal and widely accepted structure, for relevant databases.

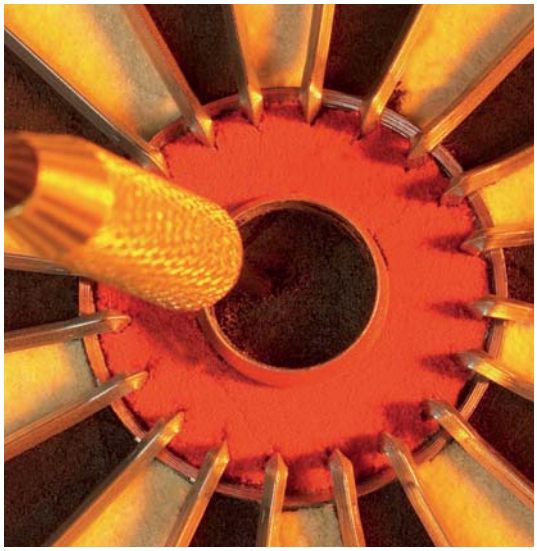
3.15 Informed Decision Making

One of the main challenges– but also an opportunity – for developing European solutions is in the area of human-system interaction. To facilitate the decision making processes, faster and more efficient tools should be designed for early warning of harmful events, for the detection of suspicious behaviour, for preventive detection of possible failures and for the simulation of unfolding events in order to evaluate the effects of potential decisions. In addition, the man-machine interface requires specific research to ensure that solutions are effectively designed for end-users, providing them with increased efficiency. This would include advanced visualisation techniques to provide a more complete picture to handle complex situations efficiently.

Data fusion, which deals with the sorting, filtering and combining of data and information from various sources, is a vital component in decision support systems and embraces legal and integrity aspects as well. To exploit all available information sources, research into system and data interoperability and visualisation is required. The changing security environment requires innovative management concepts based on novel approaches such as network-enabled capabilities, or NEC. This new conceptual model is based on autonomous decision-making units that need intelligent planning and decision support from the strategic to tactical level.

ESRIF asserts that end-users will make better decisions when these are based on a risk management approach. This is true for both day-to-day operation of security systems and, combined with added-value information, also for strategic decisions on investments, co-operation, task assignment and organisation. Particularly for the latter, a comprehensive risk management must contain elements of foresight to deal with risk scenarios that change over time, and must be able to handle conflicts between different aspects of security and the different players involved. Research is needed on the principles for future risk management and governance. It must encompass both the technical and ethical dimension to this challenge.

4. Implementing the ESRIA



Effective implementation of ESRIA is necessary to help create opportunities for more coherent research programming and funding which, in turn, will lead to better innovation and competitive market conditions. The implementation of ESRIA encompasses not only the management of ESRIA itself but also governing processes.

4.1 Governance

4.1.1 Integration of Human and Societal dynamics

ESRIF has integrated the human and societal dynamics of security as a main focus within the research and innovation agenda. Respect and consideration for civil liberties and rights was taken into consideration when developing the thematic concerns and addressing topics of Security Research. Within ESRIF we are adopting a more integrated approach. Beyond defining the security research and innovation agenda, we also respect data protection, privacy and other regulatory requirements, and address the more fundamental questions of trust, societal resilience and the ethical prism through which we assess our security solutions.

4.1.2 Engaging Stakeholders

Security research aims at being user-oriented and capability driven. This is only achievable through a clear articulation of demand, to improve the understanding of user needs, establish mechanisms for translating those needs into technical requirements and service specifications and to identify research efforts needed to fill gaps or strengthen capacities. To this end, appropriate interfaces and exchange mechanisms need to be established between the user, research and industrial communities. This will foster demand-oriented innovation cycles.

Among the primary drivers for demand focussed research and innovation are regulatory systems. ESRIF supports the development of mandatory consultation processes, as components of an overarching common capability-based planning process that involves all stakeholders, including those from supply and demand, as national or EU legislative or regulatory initiatives on security are developed. This approach engages all actors and supports effective planning and investment in their security research programmes. Partnerships between SMEs and integrating larger companies should also be facilitated and encouraged through implementation of these measures.

4.1.3 Security Governance at EU level

The pursuit of EU-wide governance in security research and innovation is a complex task: there remain significant differences between Members States' national policies concerning risk perception and approaches. Such differences are noticeable too in their security concepts and national governance models.

Ultimately, EU-wide governance in security research and innovation must be "user" and "capability" driven. The search for governance in this area must proceed in parallel with the development of a "European security culture". In those fields where the EU has adopted policies (i.e., border management or the protection of critical infrastructures) there is the opportunity and need to first develop complementary and interoperable capabilities, then shared ones and, ultimately, common ones.

4.1.4 Co-ordinated Approach

ESRIF has identified the need for transnational and national organisations to be set up in a way that supports coherent and consistent application of security measures. Building on existing organisations, such as FRONTEX and EUROPOL, bodies or networks should be established within the Member States to share such best practices and advice. These, in turn, would liaise with their equivalent organisations throughout Europe. This multilateral co-operation and co-ordination is necessary to assure the engagement of citizens and industry in the interests of achieving security objectives. ESRIF is convinced that the compatibility of security capabilities in Member States will be improved via this co-ordination.

For certain security concerns such as fraud or organised crime, enhanced co-ordination is crucial since such criminality is borderless. To be effective, prevention and deterrent mechanisms need proactive transnational co-ordination that is intelligence-led and which exploits effective and innovative decision support tools for detection and investigation. ESRIF does not underestimate the difficulty in achieving this goal. However, those who threaten our security have no such constraints, and Europe should not shrink from the difficulties but focus on the outcomes. For example, security background checks on certain categories of employees should be co-ordinated and structured to consistently deliver useful information.

4.1.5 Trans-European cooperation

ESRIF strongly supports developing a model based on a strategic and coordinated approach to trans-European cooperation. An example could be Trans-European Networks for Security (TEN-S) based on the model developed for other sectors, such as transport and energy. In these sectors this approach has resulted in key investments and procurements, linked directly to the objectives of the European Union itself, cohesion and Lisbon objectives in particular.

By adopting such a common model, Europe can draw on its collective strengths and knowledge. No single country is able to develop affordable trans-European interoperable solutions for common security issues.

The legal and financial conditions for these would also need to be further explored.

The resources available for research and technological development must be harnessed to respond fully to users' expectations. Such a process may be supported by setting up an Internal Security Fund.

4.2. Enabling conditions

4.2.1 Innovation – A Priority for ESRIF

A specific target for ESRIF is to go beyond research to address the challenges of demand-centred innovation, bridging the gap between research and the provision of innovative solutions to end users. Innovation creates market opportunities, promotes competitiveness and entrepreneurship, and guides research needs and their prioritisation.

ESRIF believes that security should be considered – and invested in – to develop a lead market. Innovation stimulates the creation of jobs, provides SMEs with new business opportunities and makes Europe a more secure place.

Initiatives should be taken to maximise the value of the research investments, promote a more harmonised procurement process, avoid duplication of effort and overcome fragmentation of market opportunities. In addition, a dialogue with insurance providers and other relevant entities is necessary to explore how certified innovative security solutions could reduce the cost of insurance premiums.

4.2.2 Exploiting knowledge synergies

ESRIF believes that the security domain could derive significant benefit from a systematic exploitation of research results from other domains. Therefore, adequate mechanisms should be put in place to assist in the technology watch of other domains, and future security research programmes should promote the adaptation of existing solutions to security specific requirements. At the same time, interaction between ESRIA and strategic research agendas in other areas such as the defence sector should also be addressed.

Cross-fertilisation is required not only at the level of research and related application domains, however. Investments in security often bring other advantages such as better visibility on internal operational processes or more efficient logistic chains. As such, investment in security becomes an investment in multi-purpose solutions. ESRIF believes it would be beneficial to encourage research initiatives that would foster this positive interaction with other operational security functions and tasks.

4.2.3 Standards, Validation and Certification

Standards, validation and certification processes have multiple roles: they facilitate interoperability of equipment, products, processes, and allow substitution of equipment. In Europe's fragmented security market, they can contribute to building more harmonisation to improve our region's position on the world market. Thus, ESRIF strongly supports all efforts to identify necessary new standards and their development. ESRIF has also analysed the concept of a "Security Label" that could support effective regulatory enforcement and has identified several sectors, whereby such processes could further enhance the confidence of citizens in their security.

Capability-driven standardisation is an important enabler of innovation. It can make an important contribution to the development of a sustainable industrial policy, unlock the potential of innovative markets and strengthen the position of Europe's economy through more efficient capitalisation of its knowledge base. Capability driven standardisation is also a priority in preventing identity theft and enabling interoperability at European borders.

For operators, competitiveness is a constant challenge and most of Europe's security providers are fully exposed to the global commercial environment. Europe needs to ensure that market conditions are such that competition is enabled not only in a European context but also in terms of the global market. Limiting liability for security providers and operators in sectors subject to security regulation could further enhance market conditions.

Detection, protection, and decontamination equipment, and medical countermeasures marketed for use against CBRN incidents must be properly certified. CBRN expert centres should be strengthened to validate manufacturers' claims and to oversee and standardise the calibration of equipment, shelf-life extensions and training. These expert centres could also validate identification of CBRN and hoax materials.

4.2.4 Developing common rules and procedures

ESRIF has identified several practical ways for supporting transnational co-operation by implementing common rules and procedures. For example, data policies for space situational awareness systems provide a common platform to fully exploit its functionality. Common methods and best practices in the area of forensic analysis or even biometrics will greatly enhance the effectiveness of detection and investigation. To enable citizens to operate in a virtual and digitalised world, development of strong common methodologies for protecting ID credentials and prevent ID theft or fraud constitute a main domain of research for the future. Adopting common criteria and approaches for security information management-and-response will greatly assist in co-ordinating and implementing effective security measures.

To assess performance of new technologies, products, services and processes, generate trust in their performance, and allow their benchmarking, it is important to strengthen systematic testing, evaluation and validation of security products, which is underdeveloped today. Europe has strong testing and evaluation capabilities across its Member States and ESRIF believes that pooling and networking these capabilities would be of merit for the security domain. Initiatives should be taken to evaluate best practices in experimental facilities, e.g. field labs by cooperation among end-users, industrial suppliers and research institutions.

From a market perspective, Europe's legislative framework for the security market(s) needs to be harmonised. This is not a call for a state-governed market, but for a common European framework regulation to foster a European market. The problem of transnational,

discordant legislation affects competition across Europe which, in turn, directly impedes competitiveness and innovation. Addressing these discordances in a co-ordinated way would enable industry –large companies and SMEs – to better evaluate their business cases regarding the future market opportunities and their own private R&D potential, thus catalysing dormant R&D assets.

4.3 Operating ESRIA

4.3.1 Funding the implementation of the ESRIA

Funding the implementation of ESRIA should continue and increase, as appropriate in keeping with the overarching goals of making Europe a more secure place. Therefore security research and innovation programmes should provide Europe with a high level of knowledge. Europe needs to benchmark itself in terms of security spending and determine an appropriate budgeting mechanism in line with its goals.

ESRIF also considers that systematic capability planning for better and more targeted investment is an ongoing priority, and that this capability planning should be linked with other entities vested with promoting and developing security.

4.3.2 Managing the Implementation of ESRIA

ESRIF has agreed that a formal implementation process is required if ESRIA is to provide the foundation for security research and innovation in Europe. ESRIF is not in the position to interfere with political decisions, such as proposing a concrete body to be set up. This should be the task for the post-ESRIF period. However some criteria are listed up in the following that might be of help:

- Ensure stakeholder (e.g., end user, supplier and civil society) representation and engagement
- Monitor coherence between all actors involved in security research
- Maintain structured dialogue with Europe's technological and industrial base
- Build on existing co ordination activities (regional, national or inter governmental) in areas, such as crisis management
- Monitor coherence in implementation between capabilities and R&T work
- Assess good and adequate use of European subventions, as well as reasonable balance between public funding and own investments from the industrial sector
- Review ESRIA at regular intervals regarding benchmarked forecasts provided by security experts
- Maintain a holistic and comprehensive perspective that includes root cause analysis, international engagement and the societal dimension

4.4 Conclusion

Ultimately, ESRIF considers that the development and implementation of a strategic plan for security research and innovation –together with an appropriate review mechanism – should produce a more coherent, organised and permanently functioning system for delivering security to Europe's citizens. ESRIF has developed ESRIA in the context of key messages but recognises that to achieve its goals, follow up implementing procedures are compulsory.

5. Recommendations

ESRIF strongly recommends that the EU and its Member States launch new measures to enhance the security of its citizens. These should also aim to create amenable conditions for European excellence in research and innovation, and thus advance Europe's security. The below sets out policy and operational recommendations for achieving stronger security research and innovation results:

5.1 Common European Capabilities

The EU must draw on its collective strengths and knowledge by developing common capability via enhanced transnational co-operation.

1. This calls for *close consultation across Europe* among supply, demand and end-user stakeholders across the planning, execution and review cycles of security research policy. The demand side in particular – governments and end-users – needs organisational re-alignment to both shape and respond to security innovation.

2. *Resources and incentives* are essential to developing common capability. ESRIF recommends, notably with a view to the implementation of ESRIA, that the EU maintains the current rate of growth of its security research programmes – with the aim of reaching an annual budget of one billion euros as proposed in 2004 by the Group of Personalities. National programmes should reflect this degree of ambition. Regarding the necessary research and industrial synergies, technical compatibility and interoperability of new security solutions, a significant effort is required to ensure the coherence of national and EU efforts through enhanced coordination.

3. Research programmes should be complemented by additional implementation programmes. Success on the global market strongly depends on EU market procurement references. Pre-commercial procurement of innovative solutions should be exploited as a mechanism to bring research results closer to the market.

5.2 New Policy Initiatives

The above should be supported by stronger articulation of demand, and delivery of the most appropriate solutions by the supply side.

4. New initiatives and programmes should include:

- Creation of knowledge centres such as CBRN expert groups to guide research

- Preparations to meet foreseeable needs for pan-European network-enabled capabilities and complex systems in early warning and response readiness that deal with natural and man made incidents
- Expanded critical infrastructure protection programmes
- Evaluating the applicability and efficacy of the numerous initiatives available to the EU and its Members States such as: a Lead Market initiative, Trans European Networks for Security, the creation of an Internal Security Fund or a "European Security Label"
- The early engagement of all stakeholders and transparency of the regulatory environment, including standards to stimulate private sector investments in security research. If upcoming regulations are understood early on, a return on security investments can be foreseen and investments can thus be expected to take place

5.3 Integrated Approach to Security

Effective civil security must embrace interoperability, standardisation, certification, validation, communication with the public, education & training, exchange of best practices, consultations on privacy issues and other factors that cut across public and private spheres and provide synergies between civil security and defence research fields.

5. A holistic approach must include:

- Efforts to ensure that the social, cultural, legal and political aspects of security research and development are taken into account. Research programmes should reflect relevant ESRIF key messages, and thus promote overall "societal coherence"
- The promotion of a *security by design* approach in any newly developed complex system or product, ensuring that security is addressed at the point of conception, as it has been the case for *safety by design*
- Programmes to raise societal awareness of security threats, risks and vulnerabilities – and the security and safety impact of emerging critical technologies

5.4 The Global Dimension

The EU's civil security is a collective responsibility touching government, societal organisations, industry and individual citizens. It cannot stand in isolation from the world.

6. The globally inter-related nature of security calls for:

- A strong and independent technological and scientific base for the EU to safeguard the interests of its citizens and ensure that its industry is able to provide products and services in a competitive manner
- Giving high priority to security's external dimension and closer home affairs/defence consultation. Research and innovation programmes should support peacekeeping, humanitarian and crisis management tasks, including joint initiatives with other regions and international organisations, notably as regard the development of global standards

5.5 Security Research: The Future

The proposed European Security Research and Innovation Agenda – ESRIA – should be seen as a living document.

7. For ESRIA *to evolve* with Europe's internal and external threat environments:

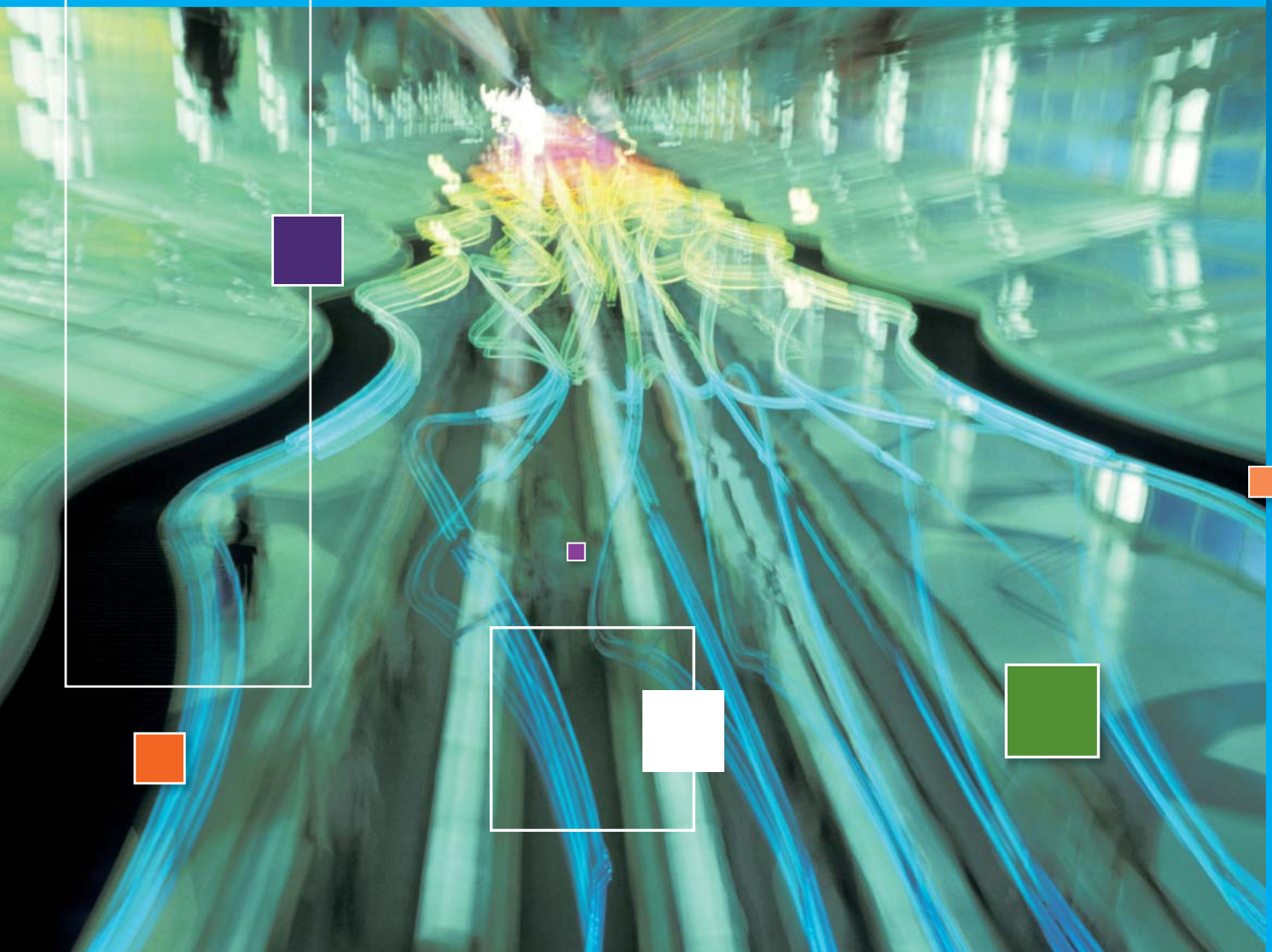
- A transparent mechanism involving all stakeholders should be set up to implement ESRIA in a balanced and rigorous manner
- ESRIA should be revisited and evaluated on a regular basis with special attention to evaluating any measures flowing from ESRIF key messages

EUROPEAN SECURITY RESEARCH & INNOVATION FORUM

ESRIF

ESRIF FINAL REPORT

PART 2



Introduction

Introduction

Part II of ESRIFs final report consists of the detailed findings of ESRIFs eleven working groups.

Background to ESRIF

EU-level civil security research started in 2004 when the European Commission launched its three-year **Preparatory Action for Security Research (PASR)** with a budget of €45 million for 2004-2006. A number of national security research programmes were also launched during this period. PASR's purpose was to test the idea of using EU funding for security R&T projects. This paved the way for today's fully fledged European civil security research theme in the EU's 7th **Framework Programme for research (FP7)** for 2007-2013, which was allocated a budget of € 1.4 billion.

The preparation of both PASR and the FP7 Security theme was supported by high-level strategy groups: the 2004 **Group of Personalities (GoP) for Security Research** and the **European Security Research Advisory Board (ESRAB)** whose strategic report in 2006 helped shape the scope and implementation of these programmes.

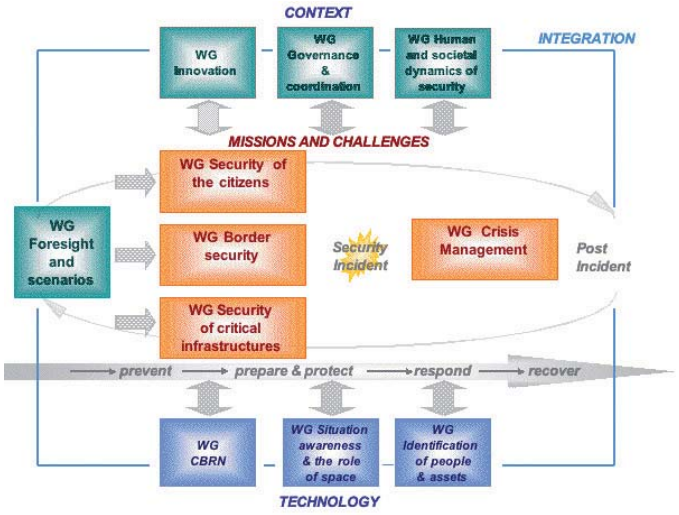
As described in the Introduction to Part I of the Final Report, **ESRIF** was then established in September 2007, on the basis of a joint initiative of the European Commission and EU Member States and FP7 Associated States. It has been an informal group, set up jointly and co-owned by its stakeholders from the demand and supply side of security technologies/solutions as well as from civil society and with a mandate to develop a 'European (Joint) Security Research and Innovation Agenda' for Europe (ESRIA): a strategic roadmap for security research and related measures to bring greater coherence and efficiency to the sector, while promoting innovation[1].

Internal Organisation

ESRIFs 65 members divided their tasks into specialised areas that were addressed by 11 working groups (WGs). WG5, for example, focused on foresight and scenarios, and provided methodological guidance as well as the long-term scenario background perspective that was crucial to ESRIF's work. Other WGs were set up to focus on security missions (WGs 1-4), specific challenges requiring separate investigation (WGs 6-8) or "horizontal" issues.

In addition, a "Transverse" Committee was created to interlink all WGs and identify common key factors across different fields. The Transverse Committee dealt with issues such as security economics, mediatisation & communication, as well as ethics.

ESRIF's working groups were organised as follows:



1 See ESRIFs Terms of reference – in annex I

"Missions" and thematic areas :

1. **Security of the citizens**
2. **Security of critical infrastructures**
3. **Border security**
4. **Crisis management**
5. **Foresight and scenarios**
6. **CBRN**
7. **Situation awareness and the role of space**
8. **Identification of people and assets**

Horizontal (cross-cutting) issues :

9. **Innovation issues**
10. **Governance and coordination**
11. **Human and societal dynamics of security**

Co-ordinating with each other, the WGs' work was simultaneous. Each group had a leader and a rapporteur to guide the process.

Methodology

ESRIF's work approach and roadmap can be summarised as follows:

- The **first year** was dedicated to assessing existing security policy decisions, strategies and plans at European and national level, as well as recent studies and projects such as those of PASR, FP6 and FP7. Exploiting its experts' knowledge base, ESRIF identified the mid-term threats and risks for Europe's security and the resulting challenges.

- During the **second year** the required capabilities and capability gaps in European security policy needed to counter the above threats were identified. Finally, a set of comprehensive recommendations for research and policy measures in the innovation domain were drawn up indicating priority areas.

Not only did ESRIF draw on the work of the GoP and ESRAB, but also on contributions from other fora to avoid duplication of efforts and to maximise consistency with the results of previous and ongoing research programmes.

In order to explicitly account for long term developments ESRIF engaged in a scenario planning exercise where a set of alternative future worlds were developed to contextualise the midterm findings on threats, risks and challenges identified by ESRIF Working Groups. This "robustness check" demonstrated a tendency for societal risk to grow over time, which underscores the need for security innovation to avoid excessive costs.

The ESRIA road map

In Part I of the final report the ESRIA roadmap was visualised. The foundation of ESRIA is based on the table described below (and attached in annex II).

A common framework guided the construction of the roadmap, based on the answers to the critical «why-what-how-when» questions that define and explain the research plan, including in some cases the investment indication.

The following information is inserted into the Road Map table on each item:

1. **Running number**
2. **WG number**
1. **WHAT? Research capability**
2. **WHY? Reasoning**
3. **HOW? Plot of the future development in scientific or technical field**
4. **Key link elements (Reference to Part I Paragraph where the research need is mentioned)**
5. **WHEN? Timeline (short -20019/13; mid- 2013/2020; long-term beyond 2020)**
6. **Weight/Cost estimation (only on a voluntary basis)**
7. **Cluster number**

The working groups aligned themselves with the five clusters (decribed in chapter 3 of Part I), according to a structure based

on research capabilities and technological needs.

The WHY defines the domain of the roadmap, which is based on the ESRIF vision and key messages, the end users needs and Europe's competitive positions.

The roadmap connects and balances the drivers of research capabilities (WHAT - end-users pull) and technology innovation (HOW - technology push).

Due to the huge number of research capabilities (WHAT) generated by the WGs (95) and the extent to which they varied in terms of granularity, a virtual reference for grouping the capabilities was established, called function. This is an artificial expedient to help the readability of the roadmap in the visualisation that does not form part of the Roadmap table. The function arranges capabilities that are associated to similar technological or scientific solutions.

There are approximately 350 scientific and technological lines (HOW). Moreover in the visualisation (Part I) a technology readiness level (TRL) was associated to all of them to assess the maturity of each specific technology and the evolution of technologies that will achieve the objectives over time is also shown.

The time-based (WHEN) Roadmap shows the urgency of the research capability.

ESRIA roadmaps and table also include linkages to show how the elements of the roadmap are driven by systemic or innovation needs.

Contributions by the eleven Working Groups

In the following 11 chapters, each Working Group explains in more details its work and findings.

While using the earlier described methodology, the working groups have - in as far as possible - divided their respective chapters into the following sections:

- Introduction
- Threats, risks and challenges (or "Challenges" for non-mission groups)
- Capabilities and gaps (or "Needs" for non-mission groups)
- Priorities (for research and innovation)
- Conclusion
  List of references and annexes to the chapters are found in Annex 3.
  Relevant reference and background materials are included in the attached CD-ROM.

1. Working Group: Security of the Citizens

1.1 Introduction

1.1.1 Scope

The security of Europe's citizens is deliberately threatened by a variety of violent and destructive acts of man, most notably terrorism and organized crime. The targets of these threats vary widely: threats can be aimed at the security of our borders, our infrastructures, our population, or government. They can materialize through a variety of means, such as financial manipulations, CBRNE-weapons, corruption, and so on.

ESRIF deals with these threats, how to prevent them from happening, how to be prepared for them and how to deal with their destructive effects. Within this context, Working Group 1 considered those threats where citizens are threatened by acts of man aimed at wide targets, rather than individuals.

1.1.2 Fit to context of ESRIF

Nowadays the security of citizens is primarily pursued by the elimination of malignant elements and by the efficient and effective response to manifesting threats. ESRIF Working Group 1 chose a broader approach with a specific attention to social coherence of the society. This includes, for example, the desire for an early response to detection of tensions between population groups with significant differences in welfare, ethnicity or religion. In this perspective, trust between citizens and societal structures is a key factor for prevention of feelings of uneasiness and seeds of unrest. A resilient society, in event of security incidents, requires appropriate behaviour from well prepared citizens and the efficient, flexible and proportional reaction of security organisations. Sharing of situation awareness and coordination of preventive and responsive actions are, in this context, key elements.

Innovation of systems on a multinational scale is essential for reaching higher security levels for citizens in Europe. Modelling of social interactions, information-exchange systems, mobility of people and goods and of organisations responsible for executing security tasks is necessary to lay the foundation of broadly acceptable policy options and new technical provisions. Requirements from the perspective of laws, guidelines, privacy, business and interoperability have to be accommodated. The implementation of new systems often requires modifying the responsibilities of the involved stakeholders. This results in the need for adequate education and training for security workers, but also for example service providers and not least for citizens.

1.1.3 Developing a strategy

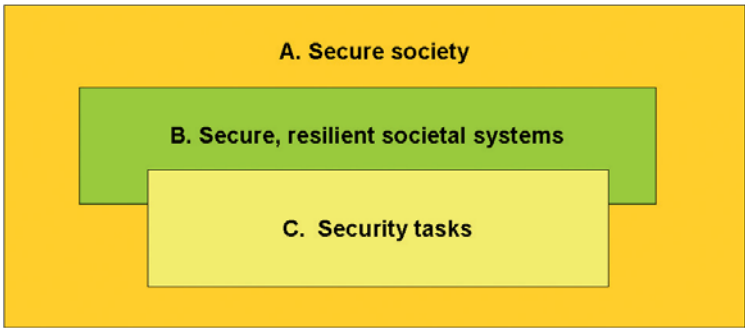
From the start of ESRIF, the following nine topics were selected for a more in depth study by Working Group 1:

1. **Terrorism and organised crime**
2. **Protection of soft targets**
3. **Urban security**
4. **Civil protection**
5. **Cybercrime, on-line investigations**
6. **Public-private trusted information exchange models**
7. **Financial threats**
8. **Explosives**
9. **Forensics**

For each of these nine topics we have identified a range of threats and challenges based on existing policy documents at EU and national level, and on the expertise available in the group. Subsequently we analysed these threats and challenges on a number of selected aspects, defined the desirable capabilities to tackle them in the future, analysed the current capabilities, and determined the existing capability gaps that have to be addressed. Based on these results we formulated a list of prioritised research needs for Europe.

1.1.4 Integration to a strategy

The scope covered by WG1 was considerably large, and the group identified many topics of interest. When combining the results of the nine subgroups, a significant number of common issues and related recommendations emerged. For the purpose of coherent reporting, the topics needed some restructuring and the following scheme was developed:



The first layer, the "Secure society " (A) relates to the environment where the citizens live with mutual respect and where their rights, privacy and possessions are protected. Such a society has a high resilience against natural and hostile disturbances.

The second layer, "Secure, resilient societal systems" (B) relates to what is necessary to secure the basic needs of the population and of the private and public institutions.

The third layer "Security tasks" (C) relates to reducing security risks and to adequately acting in case of security incidents, whatever their scales.

Guaranteeing the security at these various levels is the concern of different stakeholders. Although cooperation and shared actions are essential, the main responsibility for the three fields is usually covered by different players:

A. A secure society is the primary concern of authorities at a local, regional, national and European scale,
B. Secure, resilient societal systems require mostly the care of private sectors or public-private partnerships,
C. For efficient performing, societal security tasks are most of the time under the responsibility of public organisations.

1.1.5 Economic dimension

Enhancing the security of the citizen has a significant economic dimension at each of the three distinguished levels of the previous paragraph:

- **At the level of a secure society, the investments in security devices to fully protect citizens, houses and buildings could represent a substantial business potential.**
- **At the level of secure, resilient societal systems there is a need for a large number of capital-intensive systems**. The competitiveness of the operators is in many cases determined by an efficient and effective incorporation of the security requirements; as examples the transport and the utility sectors can be mentioned. In some sectors, compliance with security is a matter of to be or not to be; the financial sector is the extreme illustration of such a sector.
- **At the level of security tasks there are two relevant sectors:**
  - Industrial suppliers of equipment, information systems, fire engines, etc. This sector is split up into a very large number of SME's and some multinationals. To improve the competitiveness of the European enterprises the market should be made more transparent and better structured.

- Security service providers. In this sector an enormous scaling up of enterprises takes place. Nowadays there are several firms with more than 100.000 employees. At the same time a number of authorities are privatising some of their security tasks, while private players are also increasing the hiring of surveillance services. An important challenge is to enhance the competitive power of these firms by new supportive technological systems.

In the next paragraph the issues in the three distinguished fields of security are further analysed. For each threat, required capabilities, systemic needs and research needs are dealt with subsequently.

1.2 Required capabilities and research needs

1.2.1 A secure society

1.2.1.1 Threats and challenges

Societal coherence is an essential prerequisite for a secure society. However, a society fulfilling the ambitions and ideologies of all individuals and groups of citizens is a utopia. There is always a societal trade off of different desires and views in order to reach broadly shared, common social, cultural and political values. The dissatisfaction of certain individuals or groups can become a kernel for societal disturbances. In addition, intended and non-intended infringements of the law and neglecting of societal values are causing damage. Essential phenomena in this context are:

1. **Aggressive violent acts of individuals**
   Here, threats of a different nature can be mentioned: threats of a mainly social nature (such as acts of desperate people, acts on environment threatening pollution or vandalism (hooliganism)) and threats of a more political nature such as hostile, discriminating acts towards minority and vulnerable groups (religious, ethnical, sexual, political groups, females, elderly, children and persons with specific needs). An extreme category consists of violent acts: (suicide-) attacks, taking of hostages and kidnapping.

2. **Terroristic acts by organised groups and networks**
   Terrorists do not restrict themselves to well protected targets, such as embassies, VIP's, critical infrastructure etc. During the last decade an increasing number of so called soft targets were attacked. They intend to cause casualties in easily accessible places where civilians are brought together in confined areas on a routine basis (Madrid/London public transport attacks, Mumbai hotel attacks, or road side bombs in Iraq). Due to the rapid distribution of information and the spreading of news by mass media, the intended feelings of anxiety and unease in large parts of the population are provoked. Terroristic activities are directed to deteriorate society by creating panic as an ultimate challenge. An example of a scenario with a real risk for causing panic is a large-scale CBRN attack on a major city with rapid spread of contamination.

3. **Organised criminal activities**
   The dimensions of organised criminal activities exceed significantly the local scale associated with regular crimes. Europe is confronted with growing organised crime concerning drug trafficking, trafficking in human beings, environmental crimes, racketeering and counterfeiting. The scale of involved networks is still increasing. Organised criminal activities are directed to gain materialistic advantages or power.

4. **Radicalisation of groups of the population**
   In certain groups of the population with specific characteristics (e.g. ethnic origin, religion, students, poverty) feelings of alienation and exclusion can arise. If these feelings are ignored there is a risk of provoking undesired processes and worsening the dissatisfaction in organised groups or networks. A subsequent stage could be the mobilisation potential actors for defending the denied rights. Ultimately, violent actions remain a possibility. Among others, a manifested problem is the periodic violent uprisings of young second-, third-, etc. generation immigrants.

1.2.1.2 Required capabilities

Authorities at all levels have to take care of the security in society. In order to cope with the above indicated threats they have to provide for a number of capabilities:

- **Mobilisation of citizens for enhancement of societal security**

  Citizens have to be prepared for security incidents and to behave optimally to avoid personal harm. A significant challenge is to strengthen their behaviour in case of security incidents and calamities. Citizens have an enormous capacity for observation of signals indicating the risk of a potential security incident, they are usually the best position for the very first response to the incident and they can contribute to the emergency response immediately after it has occurred (see Working Groups 2 and 4).
- **Protection of soft targets**

  Soft targets are all those places where people routinely reside, gather or recreate while not in transit or where the public is admitted, as well as some forms of public transportation, whether they require exceptional security plans (major events) or not (fixed targets). The primary goal of any initiative devoted to protecting soft targets should always be the protection of people. The scope of this action is to introduce proactive and coordinated measures in collaboration with the private sector to strengthen the protection of soft targets, the ultimate aim of which is to guarantee normal life. In particular, certain categories of travelling groups, including pilgrims, immigrants and displaced persons, require heightened protective measures, especially in terms of receiving coordinated response measures and security warnings. Targets that require special attention are VIP's and major events.
- **Resilience of society for calamities**

  After large scale disasters or security calamities the transport infrastructure for the rapid evacuation of people from dangerous areas has been downsized in a number of cases. An infrastructure with a good balance of transport corridors and shelter areas for large number of people can greatly reduce the number of potential victims.
- **Warning systems and new interventions concerning terrorist acts by organised groups and networks**
- **Prevention and suppression of organised criminal activities**
- **Creation of cross-cultural, cross-generational and cross-societal links**

  In order to increase the resilience of society and its resistance towards violence, human links of solidarity should be created across cities between communities, between rich and poor, between the highly educated and the undereducated. The methodology used should value the potential represented by local communities and newcomers, and the resource that culture represents. Such methodology should furthermore be oriented towards the development of practical solutions and allow all members of society to participate.

1.2.1.3 Systemic needs

The well-balanced functioning of a secure society requires more than capabilities. The society should provide suited arrangements and infrastructure for effective responses to undesired behaviour, acts and developments. Essential systemic needs concern:

- **Legislation**

  The Hague Programme highlighted the need to develop an EU intelligence-led law enforcement mechanism to enable decision makers to define European law enforcement strategies based on thorough assessments. Availability of and access to information, production of European criminal intelligence and enhanced trust between law enforcement authorities at European and international level, constitute its core elements.
- **A common European structure for cooperation between actors involved in urban security**

  Definition of the goals and the implementation of security at urban level require involvement of all actors of security and prevention – local and regional authorities, police, judiciary, administration, health and social workers, including the youth and popular and immigrant classes. A common European structure is needed for cooperation in new developments comprising the various aspects of Urban Security (including social and societal pre-conditions, youth frustration, unemployment and criminal behaviour, urban violence, the role of police, feelings of insecurity, radicalization and terrorism).
- **Civil rights**
  - Protecting Privacy : Social, legal and ethical issues of surveillance
  - Personal responsibility for own security
- **Economic stimulation by enhancing societal security**
  - Standardisation
  - European network of validated test facilities for the specific application field of security products and systems
  - Approaches for creating critical mass for new products and services

1.2.1.4 Research needs

Research is needed for:

- Development of know how required for building up of needed capabilities
- Designing of systemic improvements for the well balanced functioning of a secure society

In table 1 the research needs for a secure society are specified.

TOPIC	RESEARCH NEEDS
CAPABILITIES	
MOBILISATION OF CITIZENS FOR ENHANCEMENT OF SOCIETAL SECURITY WITH RESPECT TO INCIDENTS	Behavioural analysis (collective and individual) for risk perception / emergency, information / *warning methodologies* (incl. minorities), *Organisation Governance* / Decision making, human behaviour in stress situation, education of population to security issues. Mobilizing the citizens to behave in an appropriate way for reducing their own risks and - if necessary - contributing to the emergency response, including caring for minorities and weaker individuals. The availability of reliable messages clearly indicating what has to be done is essential. On the other hand, during a crisis situation, the people in the crisis area stand for a gigantic reservoir of information, but the challenge is to effectively exploit this reservoir. New possibilities for communication via mobile devices can be seen as the nucleus for new ways of crowd sourcing. Effective communication in two directions require a systematic approach to meet the real information needs without overloading the human capacities; a netcentric information infrastructure with user specific modules and interfaces has to be developed; training and education of public bodies, first responders and citizens is required for effectiveness. How people have to react in the event of a CBRNE incident or terrorist attack is an option for a scenario to be considered.
PROTECTION OF SOFT TARGETS	Models for field cooperation around specific targets concerning systematic risk assessment and review of security measures. Development of the desired security awareness is an important aspect. Methods and infrastructure for Information sharing; this comprises providing the public with updates/ alerts/ warnings, private reporting about noticed unusual /suspicious activities. Major events can be valuable as laboratories to implement and test specific security measures, as well as to elaborate best practices that are also transferable as routine protective measures for fixed targets.
RESILIENCE OF SOCIETY FOR CALAMITIES	Modelling and simulation of residential areas and built infrastructure for better coping with different virtual scenarios for calamities of a significant size. Moreover, the composing of adequate sets of measures for appropriate levels of security requires the use of these types of instruments for evaluation purposes. After a natural or industrial catastrophe, urban acts of violence or a terrorist attack, cities may recover economically and can be rebuilt. At the same time the recovery of the victims requires more attention, because the usual short-term psychological support on a large scale is not sufficient. Development of longer-term support for the victims of such events is necessary. An option to be studied is the creation of an internationally recognized victim status which should provide them with legal, social, and short- and long-term psychological support to help them recover from the events.

WARNING SYSTEMS AND NEW INTERVENTIONS CONCERNING TERRORIST ACTS BY ORGANISED GROUPS AND NETWORKS	Development and verification of models for social dynamics of groups with high levels of dissatisfaction. Stabilizing and destabilizing triggers have to be traced. Special attention to the direct and indirect signals of unsatisfied groups to the society in several stages of a radicalisation process could create the basis for new early warning systems and interventions.
PREVENTION AND SUPPRESSION OF ORGANISED CRIMINAL ACTIVITIES	Development of models for the social processes contributing to the originating of personal criminal intentions and alignment with other persons with criminal intentions. Special attention to the direct and indirect signals of growing criminal intentions could create the basis for new early warning options and proper interventions.
PREVENTION OF RADICALISATION BY CAPACITY BUILDING	To acknowledge the divisions of society and the discrimination which some groups face on a daily basis – and to develop, or effectively apply existing, anti-discriminatory laws and measures. To develop, implement and support positive education, employment, careers, housing, family measures towards first-, second-, third-generation, etc. immigrants without provoking extremism in the rest of society (See Working Group 11 report on radicalisation)
CREATION OF CROSS-CULTURAL, CROSS-GENERATIONAL, CROSS-SOCIETAL LINKS	Analysis of mechanisms with respect to solidarities between citizens from various parts of town and of society, and making social and societal barriers more porous. This analysis should result in a methodology for the development of practical measures, e.g. concerning the integration of newcomers by presentation of the local cultural values and activities allowing all members of society to participate.
SYSTEMIC NEEDS	
LEGISLATION	Thorough assessments for development of European law enforcement strategies.
A COMMON EUROPEAN STRUCTURE FOR COOPERATION BETWEEN ACTORS INVOLVED IN URBAN SECURITY	A common, adaptive, general, legal, conceptual, practical European framework should be developed to insure effective, cost-efficient, integrated, coordinated and synergetic horizontal (across public agencies, private services and civil organizations) and vertical (between various levels of government, from local to regional, through national and European) cooperation of all actors in Urban Security, including the inhabitants and those that are part of the "problems" – fostering dialogue, mutual understanding, close cooperation and recognition. The following elements of this framework should be developed: ▶ A cartography of national and European Urban Security Risk zones and a European network of Local Urban Security Observatories ▶ Methods for monitoring of the subjective feelings of citizens in residential areas ▶ Models describing the dependency of urban security from a spectrum of parameters (e.g. population characteristics, local distribution of welfare, concentration of unoccupied houses, presence of shops, levels of illumination, intensity of surveillance by authorities, organized public panels for surveillance, special instructions and education for citizens concerning security) ▶ An architecture for supporting the development of security policy by specific authorities with optimal involvement of societal stakeholders (including citizens). This architecture should make available information systems, models, simulation features and approaches applied elsewhere ▶ Facilities for Concept Development and Experimentation for supporting the participation of stakeholders in the design of solutions for specific challenges

CIVIL RIGHTS	To enhance privacy, specific technologies should be developed for the encryption of sensitive information elements in complex information systems. Citizens are becoming more pro-active concerning their own security. This trend triggersthe development of a legal framework with more responsibilities for citizens, including possibilities to manifest this enhanced responsibility; as an example, one can mention: new domotic tools, education, hired surveillance services etc. Clarify the divisions of society and the discrimination which some groups face on a daily basis in order to be able to develop and effectively apply anti-discriminatory laws and measures.
ECONOMIC STIMULATION OF ENHANCEMENT OF SOCIETAL SECURITY	Development of Public – Private Partnerships (involving intelligence, law enforcement, emergency responders and site/building/venue/ group managers/owners), to prevent, protect and respond/recover from the materialized threats. PPPs, which could be initiated on a voluntary basis for a private sector facility (open to the public and included into a vulnerable targets list). Development of attractive business case for potential partners in PPP's for security

1.2.2 Secure, resilient societal systems

1.2.2.1 Threats and challenges

Within our society a number of systems for the maintenance of critical societal functions can be distinguished: energy, water, information and Communication Technologiies (ICT), finance, food, health, transport, etc. In the last few decades the size of these systems and their interconnectivity has increased tremendously. Due to the growth of societal systems, significant gains in efficiency and effectiveness were realised. However the shadow side of this development is a substantial augmentation of the vulnerability to disturbances. Natural, criminal and terrorist incidents are now able to cause a much larger impact as would have been possible in the past.

Working Group 2 deals with the proper system development for protecting these critical societal functions. On a complementary basis, our Working group analyses the corresponding interfaces with the society.

In this context the following significant threats can be mentioned:

1. **Pollution of supply chains with counterfeited products**
   Criminals gain significant, growing revenues by counterfeiting goods and substances. Due to the improved production capabilities of organized crime counterfeited products are now frequently difficult to discriminate from the original ones. Examples of sensitive categories of products are medicine, electronic devices and software.

2. **Misuse and disruption of ICT-infrastructure by cybercrime**
   Cyber criminality, including attacks against information systems have increased spectacularly in recent years. Quickly developing technology provides more and new opportunities for criminals in an environment which can more easily guarantee anonymity. New types of cyber attacks of previously unknown large and dangerous scale have been observed. Nowadays, cyber-criminals seem to be more motivated by a desire to gain financially than to cause electronic vandalism. They design malicious codes to use infected machines to accomplish their objectives, such as stealing credit card numbers, sending spam or providing an «unguarded» entry into the organization's network. Botnets present a particular threat due to the wide variety of activities for which they are increasingly used, such as to mount denial of service attacks, host 'phishing' websites for identity theft[1] , financial fraud, and distribute malware[2].

1 In the case of phishing scams, the scammer (cyber criminal, the person attempting to steal the confidential information) is attempting to acquire sensitive information such as usernames, credit card numbers, or bank account credentials. Source: Symantec Report on the Underground Economy, July 07-June 08, p.82.

2 Symantec Report on the Underground Economy, July 07–June 08, p. 19. See also footnotes 13 & 14.

The threats of cyber criminality comprise a broad range: from direct threats to individuals (e.g. online child sexual abuse) to threats to the national security of entire countries (large scale attacks on information systems) and occasionally a global impact cannot be excluded.

Some of these threats are listed hereafter:

- Cyber and physical attacks against IP distribution centres resulting in the paralysis of the Internet
- Dissemination of fear, recruiting, propaganda, fund raising – cyber terrorism
- Interfering, gaining remote control of systems that are strategic for state security and air transport (e.g. water, energy supply networks; communication, aircraft)
- Dissemination of child sexual abuse materials
- Internet as a medium for anonymous exchange of information on criminal activity
- Data mining (open sources and hacking) Internet resources to find potential targets for terrorist attacks and/or information on them
- Anonymous access to the Internet leading to e.g. cyber stalking or identity thefts

3. Organised abuse of financial or payment systems

According to the Communication from the Commission to the Council and the European Parliament on the prevention of and the fight against Organised Crime in the financial sector dated 16/4/2004 COM(2004)262, organised financial crime is taken to mean activities of organised crime groups which abuse financial or payment systems with a view to financial gain, a definition which is wide enough to embrace certain recent scandals in the corporate sector. This category comprises a number of important financial threats, from money-laundering to payment systems fraud, to direct attacks against the critical financial infrastructure of private banks and/or public authorities involved in handling and exchanging financial information. Organised financial crime can potentially result in a broad societal impact due to lost revenues, loss of reputation and degradation of public standards. High levels of such crime can discourage the creation of new enterprises, deter potential investors and distort competition.

As categories of financial crime one can distinguish:

- Counterfeit banknotes and coins. Modern digital equipment offers growing possibilities for reproduction of banknotes including some of the specific machine-readable features incorporated in Euro banknotes
- Fraud and counterfeiting of non-cash means of payment (principally credit and debit cards and cheque payments)
- Tax fraud. Especially VAT fraud is a major concern for the Member States and the European Community, because this fraud jeopardises legitimate trade in certain economic sectors and hampers the functioning of the internal market
- Ilegal transactions related to e.g. export of armaments and weapons, trade of drugs, money laundering, underground banking

1.2.2.2 Required capabilities

Private players and (inter-)national authorities at all levels have to take care of public security. In order to cope with the above indicated threats they have to provide for a number of capabilities:

- **Enhanced resilience of supply chains against pollution with counterfeited products**

  Improved branding of products or of sealed packages of products can contribute to better and easier possibilities of authentication in different stages of the supply chain. Also the development of tracking and tracing of goods during transport is relevant in this context. Standardization of the approach for special product categories seems needed for successful application. Furthermore the investigation for tracing counterfeited products should be made more professional. (See Working Group 2 on food and agriculture tracking and tracing).

- **Enhanced resilience and protection of ICT-infrastructure**

  Protecting the cyberspace from serious abuses is an important challenge for the years ahead. New protective technological measures and cooperation between law enforcement agencies cannot lag behind modern forms of crime. Our citizens expect an adequate response from authorities. An adequate strategy includes a combination of exploring new avenues and better use of existing instruments to ensure an optimal use of all available resources at EU level. The elimination of redundant duplications and a better and more intensive

co-operation on a national and international scale is also urgently needed. Working Group 2 has developed proposals for the prevention and protection of ICT-infrastructure. In addition to their recommendation Working Group 1 requests attention for more specific capabilities concerning detection of and response to misuse of cyberspace as early as possible:

- network capability to trace illegal activities in cyberspace back to its origin
- detection and blocking of websites potentially harming citizens and issues of common interest
- increased protection around sensitive information through the development of new security protocols
- influencing the behaviour of cyberspace users to reduce their vulnerability against actions with hostile intents

- **Enhanced resilience and protection of the financial and payment systems**

  To combat organised financial crime, transparency and integrity standards for financial systems in public administrations and in private entities are very important. Improved rules can prevent and discourage financial crime in general and also contribute to more effective tracing of organised financial crime. Close cooperation of the authorities with non-governmental sector representatives is essential for creating a broad acceptance of the new rules.

  Investigations of financial systems provide one of the options to learn more about activities and patterns of behaviour of organised crime groups and provide effective added value to investigations in Member States. The fight against organised financial crime would be enhanced through the elaboration of a common policy on the development and implementation of methods for financial investigations.

  Relevant personnel in the private and the public sector should be better trained and equipped for discerning of and fighting against organised financial crimes.

1.2.2.3 Systemic needs

Well protected societal systems requires more than capabilities. The society should provide suited arrangements and infrastructure for effective prevention and abatement of undesired behaviour, acts and developments. In general the protections of societal systems require an improved legal basis for tracking and tracing of misuse and the subsequent needed interventions. But there are also more specific needs:

- **National and European platforms for harmonizing the abatement of misuse of Internet**

  A legal basis (borders) to control the misuse of the Internet system. The international dimensions of cybercrime and the ongoing globalisation of ICT-infrastructure require new laws and guidelines simultaneously matching to new, adequate detection methodologies for misuse of ICT-systems and to the societal need for protection of privacy. An effective approach with harmonised procedures for interventions is asking for a structure with platforms on a national and European scale and a global scale. (See also Working Group 2 report for ICT protection).

- **Infrastructure for joint European investigations for abatement of counterfeiting**

  Development of standard and harmonized procedures to support investigations in multiple Member States for the abatement of counterfeit products. Enlargement of national and European databases and alignment for interoperability. Cross border cooperation with special investigative enforcement teams.

- **Creation of a European Body for the Financial Fraud Prevention**

  To ensure a more efficient and effective prevention of financial fraud an overall vision within the EC is required. Development of that vision urges to the creation of a European Body for Financial Fraud Prevention. For realising implementation of the vision each Member state should set up or modify the national prevention structure in alignment with the commonly determined vision. The national entities should act as a counter part to the European Body when new developments and initiatives exceed European borders. This European Body should also play a role in facilitating the cooperation between the financial and other business sectors and law enforcement authorities at the level of the EU and of the Member States. Other potential roles are the identification of best practices, encouragement of implementation of new approaches and promotion of sector-wide internal controls.

1.2.2.4 Research needs

Research is needed for the:

- Development of know how required for building up the needed capabilities
- Designing of systemic improvements for a well balanced functioning of critical societal systems

In table 2 the research needs for secure, resilient societal systems are specified.

TOPIC	RESEARCH NEEDS
CAPABILITIES	
ENHANCED RESILIENCE OF SUPPLY CHAINS AGAINST POLLUTION WITH COUNTERFEIT PRODUCTS	Systematic studies of the potential risks concerning the counterfeiting of products and possibilities to prevent or to hinder criminal activities in this field. Examples of sensitive categories of products are medicine, electronic devices and software. Coherent approaches for improved branding of products - or of sealed packages of products with better and easier possibilities of authentication in different stages in the supply chain. Also the development of tracking and tracing of goods during transport is relevant in this context. For special product categories the requirements for successful application should be investigated including the possibilities for standardization.
RESILIENCE AND PROTECTION OF ICT-INFRASTRUCTURE	Development of new approaches for investigation of the use of the Internet. By monitoring and observing the behaviour of users a search engine for detecting suspicious behaviour patterns should be developed. As an essential element, improved systems for automatic translation can be mentioned. Development of the network capability to trace illegal activity in cyberspace back to its origin. In addition, enhanced detection methodologies and blocking/filtering technologies have to be developed and promoted. Development of methods and procedures to detect web sites which should be blocked across the EU. Development of international applicable unique interfaces, protocols, connectors, etc. for the trusted exchange of sensitive information. Development of tools to reduce the vulnerability of users of cyberspace, a.o. : - new anti-virus programmes extended with online investigation modules for the identification of senders of messages, detecting of potentially hostile intent and warnings for malicious sites; the distribution of more free updates of these protecting programmes should raise the effectiveness, - methods for alerting the users to the potential risks of their ICT-behaviour through the efficient and effective development of new enhanced identification processes and investigative tools.
ENHANCED RESILIENCE AND PROTECTION OF THE FINANCIAL AND PAYMENT SYSTEMS	Development of monitoring systems for detecting counterfeit banknotes and coins. Development of tools for detection of fraud and counterfeiting of non-cash means of payment by the private sector (e.g. the retail sector). Development of design rules and integrity standards for a higher transparency of financial systems in public administrations and in private entities. Close cooperation of the authorities with non-governmental sector representatives is essential for creating a broad acceptance of the new rules and standards. Development of tools and methods for investigations of financial systems. Discerning of activities and patterns of behaviour of organised crime groups should be improved. Methods for training relevant personnel in the private and public sectors for detecting and fighting organised financial crimes.

SYSTEMIC NEEDS	
LEGAL BASIS FOR THE PROTECTION OF SOCIETAL SYSTEMS	Development of new internationally applicable legal instruments for tracking and tracing the misuse of societal systems and the subsequent needed interventions to abate the misuse. These legal instruments should simultaneously fit to the technological possibilities for protecting societal systems and to the societal need for protection of privacy. An effective approach with harmonised procedures is asking for a structure with platforms on a national and European scale as well as a global scale. Prioritized domains for initiatives at a European scale are: - the supply chains - the ICT-infrastructure/ Internet system - financial and payment systems
INFRASTRUCTURE FOR JOINT EUROPEAN INVESTIGATIONS FOR THE ABATEMENT OF COUNTERFEITING	Development of standard and harmonized procedures to support investigations in multiple Member States for the abatement of counterfeiting of products. Development of architecture for interoperable national and European databases. Development of competences and interfaces for investigative enforcement teams.
NATIONAL AND EUROPEAN PLATFORMS FOR HARMONIZING THE ABATEMENT OF MISUSE OF THE INTERNET	Development of a European structure for coordination and joint actions concerning the misuse of the Internet. Harmonisation of detection methodologies and of interventions needs to be strengthened and aligned with initiatives for updating legislation.
EUROPEAN BODY FOR FINANCIAL FRAUD PREVENTION	Development of an organisational structure which makes it possible **1.** To build a system to gather, share and analyse information on suspicious transactions of credit and debit cards and cheque payments **2.** To create a "National Prevention Structure" in every member state. By this Organization, member states would have a single comprehensive structure that would ensure a more efficient and effective prevention of fraud **3.** To define common roles and procedures to track money transfers. **4.** Creating an IT system for the authorisation and financial transaction of weapons and armaments **5.** Exchange information about the interconnected infrastructure status, useful for monitoring the overall financial network; **6**. Intercept events related to detected security breaches that can be used for defining countermeasures and for preventive actions to be implemented; **7**. Exchange information with other governmental agencies in order to create a network of interconnected regulator entities. Exchanging information in real-time greatly enhances agencies' possibilities to steer the market in order to improve overall security and transparency; **8.** Evaluate the financial infrastructure's overall security and dependability for monitoring purposes.

1.2.3 Efficient and effective execution of security tasks

1.2.3.1 Threats and challenges

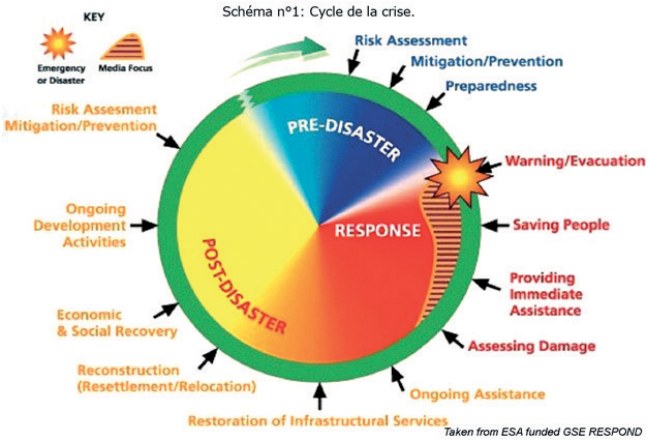
For taking care of public security and adequately acting with respect to incidents and risks, a number of – mostly public – organisations are in charge: police, criminal investigation institutes, fire brigades, ambulance service organisations etc. Of course these organisations have to execute their tasks efficiently and effectively. Among a wide spectrum of security and/or safety incidents they have to deal with the threats already specified at the level of society (paragraph 2.1) and at the level of societal systems (paragraph 2.2). Within the context of ESRIF we now focus on these threats.

1.2.3.2 Required capabilities

Special attention is needed for capabilities requiring larger scale cooperation or the harmonisation of ways of operation. These concern:

1. Civil protection in event of calamities and disasters

It is important to underline that even if the threats may appear very different in nature between natural or man-made disasters and violent acts of man, the effects on civil protection activity are very similar. This explains why capabilities herewith described have several commonalities with the general evolution of Civil Protection in the European Union and its Member States.



Capabilities are hereafter described according to the three general phases of a crisis as presented in the figure: pre-disaster, response and post-disaster.

During the **pre-disaster** phase, the European Commission is responsible for supporting and supplementing efforts at national, regional and local level with regard to disaster prevention, the preparedness of those responsible for civil protection and the intervention in the event of disaster. Key capabilities in preparedness are therefore:

- Organisation (at national and community level, including the legislative framework)
- Development of comprehensive scenarios (with related likelihood and consequences)
- Education, simulation and training (for first responders, semi-professional volunteers and population)
- Knowledge-sharing (information sharing, analysis of multi-hazards)
- Cost / benefit assessment on prevention actions.

During response (crisis) phase, timely and reliable information is the key to successful co-operation in civil protection matters. The players at stake are not only civil protection authorities but the public at large, which at any given moment could fall victim to a disaster. Contributing to raising awareness in view of increasing the level of self-protection of European citizens (including minority groups e.g. immigrants) is therefore part of the whole co-operation strategy adopted by the EU and Member States. At the same time, proper distribution of information during emergencies is also a necessity. Without information-sharing the whole co-operation structure would simply collapse. The challenge is targeting the initial actions already undertaken by the Commission to an operational system allowing actual communication between involved entities. Key capabilities in crisis are therefore:

- Relief and assistance to wounded members of the population
- Information and warning to the general public (including minorities)
- Rapid assessment (when reality does not fit with pre-defined scenarios)
- Awareness of potential hostile causes of crises and the need for recovery of traces for forensic and criminal investigations
- Communications between actors in hostile/deteriorated environment
- Coordinated action on place (language barriers, cross-border methodologies)
- Effectiveness of tools
- Knowledge from preparedness

During the post-disaster phase, after the emergency relief operation is over, work starts on further information-sharing and sustainable recovery, with emphasis on strengthening civil society for the benefit, safety and security of the citizens. In the case of major operations, it is fundamental to organise lessons-learnt sessions that greatly contribute to capitalise knowledge and to identify best-practices in preparation to other emergencies.
(See Working Group 4 report for in depth analysis of the post-disaster phase)

2. Investigation with respect to crime and terrorism

Public Private Trusted Information Exchange Models are needed for an improved exchange and sharing information across law enforcement and intelligence agencies with private organizations and companies, with the objective of contrasting the threat coming from terrorist and organized crime activities.

This is a result of the awareness that terrorist and organized criminal activities are not random and impossible to track. Terrorists must plan and prepare before the execution of an attack by selecting a target, recruiting and training executors, purchasing goods, acquiring financial support and travelling to the country where the target is located, disseminating propaganda and revendication material. In performing these activities they leave, voluntarily and/or involuntarily, traces in huge quantities and in dispersed ways, inside different public and private organizations or freely on the web, even if they attempt to hide or disguise their identities.

By analyzing the data coming from the communications and activity patterns among potential terrorists and their contacts it is possible to prevent attacks or crimes from occurring. Sharing the information about terrorists that is available to law enforcement and intelligence agencies as well as to private companies (in their databases or available freely in, e.g., web and press), and linking this data together, can help avoid their actions and disrupt their networks. Gathering and sharing information that identifies likely suspects is a critical issue here.

Surveillance of public areas and specific locations is essential for early responses to signals indicating the risk of incidents and an adequate intervention in the event of real security obstructions. Integrated control centres with well organised support information/intelligence have to provide the coordination of operating activities and must be able to function as crisis centres. These control centres should be extensively equipped with automatic analysis systems and decision-making assistance systems and systems for synchronization and reliable interaction between different control- and crisis centres.

Mobile technologies for the examination of counterfeit money, bankcards and documents. This would include implementation of artificial intelligence methods and agent technologies to support operational and investigative activities and evidence procedures.

Generalise the possibility of *rapid and secure transmission of data high flow* (video, its, images, etc.) between the servers of data of the police forces. Systematise using fixed or mobile system for the detection of displaced vehicles used by organised crime or terrorist organisations.

3. Forensics

Forensic science is the application of a broad range of scientific disciplines (e.g. biometrics, molecular biology, analytical science, informatics…) to matters of legal significance. The forensic science process is complex, involving police, scientific and legal/judicial personnel. Its application relies on an effective relationship between lawyers, police, scientists and other forensic specialists, and is interdependent and crosses professional, organisational and jurisdictional boundaries.

Furthermore, forensic science operates in a rapidly changing environment. New developments in technology such as DNA analysis have altered the role of forensic science and the contribution that it makes to police investigations and criminal prosecution. The net contribution of forensic science to criminal justice systems continues to rise and operational loads have typically doubled in the last five years. The use of technology in criminal investigations is clearly on the steep part of the growth curve. At the same time, due to the increased possibilities of this technology, the application of forensic science has become much wider than for the evaluation of evidence in court alone. Besides its 'traditional' application in the fight against crime, forensic science offers huge possibilities in information guided policing, crime prevention and security.

Although the use of forensic science for the purpose of generating evidence in court will remain an important application area, the possibilities for its use in the investigation phase is seen as one of the most promising areas in effectively and efficiently solving crime and enhancing security. At the same time the new possibilities presented by this technology pose new requirements to the necessary research. Where needed this ranges from fundamental to applied research, last but not least followed by the development of concrete products, tools and services that can be used in the forensic process.

4. Counteracting explosives

Recent history has shown that most terrorist attacks were performed using stolen and/or home made explosives. The dramatic effect of sometimes multiple and timed explosions on infrastructure and people has made explosives one of the most widely used terrorist means. Also in many criminal activities (either on national or international scale), the use of explosives is becoming a dominant means of the criminal activities (forced entry, protection of "illegal" production sites, means to create mass disturbance, etc). Counteracting explosives is a security task deserving increased attention, due to the size of the threat and the required thorough and highly specialised expertise.

In order to effectively counter the explosives threat, one has to think in terms of: Prepare, Prevent, Protect and Respond. The earlier intervention occurs, the better (intelligence, regulatory measures, localization of production sites ...), however the last chain of defence (detection, physical protection) will remain of utmost importance and clear improvements are needed in this context.

Preparation comprises continuous assessment of actual threats concerning explosives and the arising of new threats. Another point of attention is raising the public awareness of the threat of unattended and man carried explosives. Through education and information, citizens are able to improve the observation of suspicious human behaviour or unattended goods; instructions for adequate warning of the public security services have to be communicated.

Prevention should be focussed on reducing the relative "ease of access" to explosives through either criminal activity (theft or illegal purchases) or the production of explosives using freely available precursors, which make them the "weapon of choice" for terrorists. The availability of detailed production info through terrorist training groups and/or via easily available internet data makes the threat even more serious. All types of illicit use of precursors require different countermeasures, some of which are only partly available in current times or are only available by using very intrusive methods that are unacceptable to the general public. Nevertheless, extended regulation concerning precursors for so called Home Made Explosives (HME's) and improved control during transport and storage of explosives and precursors for explosives have to be realised.

Protection of vulnerable locations, buildings and events has to be further improved by quick and reliable detection and control systems. These systems should be connected to detailed information on persons and goods without infringing privacy rules. There is also a need for quickly deployable protective solutions. Furthermore, development of tools supporting balanced decision making on countermeasures to take, would be needed in order to optimize the protective chain (incl. impacts to the society).

Responses to incidents involving explosives require the rapid analysis of a whole spectrum of potentially present explosives. This can only be realised with a thorough understanding of explosives and explosive properties as well as an easy access to this data for those who need it (police, forensics, etc); furthermore, the full life cycle of explosives should be addressed.

1.2.3.3 Systemic needs

The systemic needs are specific for selected security tasks:

1. Civil protection

Alignment of operational procedures and applied information and communication systems should be very beneficial for cooperation in the field. There is a need for the development (and sharing) of *cross border methodologies* for joint intervention, standardised *emergency management multilingual dictionaries* and joint innovation for development of common counteraction *methodologies for new threats* (e.g. pandemics). In this field it is also very important *to consider the operational use* of (new) technology by First Responders, highlighting issues such as suitability and adaptability to operational context and procedures.

2. Investigation with respect to crime and terrorism

In the much diversified, low structured European Market, a wide spectrum of industrial suppliers offer an overwhelming amount of systems and components for surveillance of public areas and specific locations. There is a strong need for a European approach in this domain. This comprises improvement *of procedures for the design and procurement of new surveillance-systems,* facilitation of European suppliers of installations and systems with testing environments for proving and improving the quality of their products, for the reduction of market failure by an improved interaction between suppliers and clients.

The European Council stressed in The Hague Programme that strengthening freedom, security and justice requires an innovative approach to the cross-border exchange of law enforcement information. This requires an infrastructure with compatible and standardized databases and harmonized procedures. Moreover innovative service-delivery models for using information held within and outside governments are needed.

Special investigation techniques have proven effective in police, customs and judicial investigations of cross-border OC. The 2000 Mutual Legal Assistance (MLA) Convention and 2001 Protocol provide for these techniques, although neither instrument has yet entered into force, hence the separate Framework Decision (FD) on the use of Joint Investigation Teams (JIT). Further work is needed to improve the use of JITs and other special investigation techniques and to implement these on a European scale.

3. Forensics

The effective application of forensic science depends on the logically correct reasoning (based on empirical data and statistics), integrating the different phases in the forensic process, which encompasses the complete path from scenario-based trace recovery to reporting the evaluation of the evidence. This must occur within a comprehensive accreditation framework.

4. Counteracting explosives

The data on threats linked to explosives and the options for detection, identification and elimination of explosives in a number of possible situations should be made more accessible for those who need it (police, forensic, etc). Extension of the already existing activities at a European level is necessary. One of the challenges in arranging of mutual use of validated facilities[3]. These activities should also result in widely accepted regulations concerning restrictions to the use of precursors for HME's and improved control during transport and storage of explosives and their precursors.

1.2.3.4 Research needs

Research is needed for the:

- Development of know how required for building up of needed capabilities;
- Designing of systemic improvements for the efficient and effective execution of security tasks.

In table 3 the research needs for efficient and effective execution of security tasks are specified.

TOPIC	RESEARCH NEEDS
CAPABILITIES	
CIVIL PROTECTION	Protection of first responders against hostile treatment by the public Development of information systems for shortening of the reaction time, improve coordination between local team and coordination centres, enable quick exchange of information from different organizations (also from different countries). This requires efficient availability of the Common Operational Picture including provision of *scenario simulation* tools (incl. Virtual reality) for: ▶ Rapid assessment during crisis (incremental evaluation of threats and consequences)

3 On European level a significant effort is being done on the topic (e.g. ESETF, 2006-2007 timeframe, follow-on working groups). Knowledge generated, and the network of experts formed, have been widely used with this ESRIF working group.

	▶ Exercise, training, cost/benefit assessment of prevention actions ▶ Knowledge capitalisation tools (such as event / intervention data bases, "business" intelligence / process optimisation tools) An important issue is the connectivity with the systems of other responding organisations. The interoperability issue concerns investigation systems, risk assessment systems use of data from external on-line data information sources (including from public peers).
	Development of communication systems for crisis management operations with *integrated portable equipment* (radio, sat, ad hoc networks,…) and means to provide *alert / warning / information to general public* (media, dedicated equipment, …). Also in this context the *interoperability* issue is important.
	Development and improvement of electronic devices for surveillance tasks: on board satellites (e.g. GMES, UAV, …), autonomous / wireless / disposable / miniaturised sensors, bio- and environmental sensors, Next generation video protection / threat identification systems, robotic devices for S&R, as well as tools for the Localisation in closed / hostile environment. Intelligent collaboration of heterogeneous sensors is a major challenge.
INVESTIGATION WITH RESPECT TO CRIME AND TERRORISM	Development of retrieval capabilities for analysing the data and information available in a variety of proprietary or open sources but contained in unstructured, multilingual texts. Special challenges are: ▶ Dealing with out-of-date and erroneous data ▶ Structured data mining ▶ Video mining ▶ Social network analysis ▶ Machine translation technologies
	Development of **innovative systems for surveillance of public areas and specific locations.** This concerns components (including optronic sensors, radar sensors, beacons, electronic tagging systems and mobile sustained and improved automatic identification systems) as well as high capacity discrete surveillance systems (satellite, air, terrestrial and tactical surveillance) and integrated control centres applying automated surveillance systems with tracking and tracing features using advanced recognition techniques and adaptive multi-sensor systems. A special challenge is the development of systems allowing their direct use by security agents on the street.
	Development of **Mobile technologies** for the examination counterfeit money, bankcards and documents. This would include artificial intelligence methods and agent technologies to support operational and investigative activities and evidence procedures.
FORENSICS	Objective, probabilistic interpretation: logical and correct reasoning (criminalistics) for all forensic disciplines: ▶ Development of statistical methods and implementation in tools for objective interpretation ▶ Development of formal structures for databases (empirical science) and the development of databases ▶ Development of international standards ▶ Development of models for effective application and evaluation of forensic science use in a complex multi-jurisdictional environment

	Improve trace recovery, improve recording and reconstruction of the crime scene: ▶ Development of screening methods for detection and (first) analysis (e.g. lab-on-a-chip) which need to be portable, robust, high speed, sensitive and simple to use. This requires miniaturisation of technology in order to be able to bring 'the lab to the traces' instead of bringing 'the traces to the lab'. ▶ Development of systems for the recording, and software for the visualization of the crime ▶ Development of software for the reconstruction of the crime-scene and to visualize scenarios ▶ Development of decision making and risk handling models to manage real time application of outputs from analysis ▶ International standards for trace recovery ▶ Development of appropriate training and education methods ▶ Facilities for innovation in so-called field labs, in which clustering of actors and pooling of expertise takes place
COUNTERACTING EXPLOSIVES	Development of methods for influencing citizens to a better response with respect to the threat of explosives by education, information and instructions **(preparation).**
	Development of an adequate information system concerning explosives and their precursors in order to restrict the actual possibilities to make HME's **(prevention)**.
	Development of fast and reliable detection and control systems concerning explosives at vulnerable locations, buildings and events. Tracking and tracing and automatic warnings are attractive features. These systems should be connected to detailed information on persons and goods without infringing privacy rules. Development of quickly deployable protective solutions and tools for supporting balanced decision making on countermeasures to take **(protection)**.
	Development of fast analysis techniques for a whole spectrum of explosives, to allow an adequate **response** to incidents with explosives or related suspicions. The validation of and the access to this data for those who need it (police, forensics, etc) has to be well organised.
SYSTEMIC NEEDS	
CIVIL PROTECTION	EU wide Governance and Coordination of First responders (e.g. EU Commissioner for Crisis Management, European Agency for Civil Protection, for Security, …), to give a truly European dimension to civil protection policies, thus easing interactions between MS and also facilitating the development of a true market for European industry by reaching the critical mass.
	Joint facilities for: ▶ Accelerating effective innovation in cooperation with industry and research institutions ▶ Education / training / exercise and risk capitalisation for first responders (e.g. European Academy for First Responders) and population, to familiarise with the use of technology, make extensive use of lessons learned in past events, raise awareness and promptness to react.
	Development of the infrastructure for the cross-border exchange of law enforcement information. The action plan implementing The Hague Programme will further develop the Commission's initiatives to implement the principle of availability for the exchange of law enforcement information, common standards for access to databases and interoperability of national and EU databases. National and EU databases should progressively use the same standards and compatible technologies to ensure the selective exchange of law enforcement data while taking into account the appropriate inter-linkages.

	A special challenge is to design a higher level system where data coming from different public and private organizations may be exchanged, merged and fused, without risking law infringements, assuring civil rights are preserved (this may be solved also thanks to new laws which allow private organizations to provide the public sector with information without infringing civil liberties and data privacy or other laws).
FORENSICS	Design of a comprehensive accreditation network for an effective international response to cross-border incidents and crime. This concerns incidents with respect to terrorism, drugs trafficking, cybercrime, human trafficking, paedophilia, environmental crime, etc.) : ▶ Develop standardized methods and best practices ▶ Development of standardised and formal structures for databases to be used for more objective interpretation. Statistical research is also required in order to discover the limitations of various methods and their error rates ▶ Organisational models for collaboration of forensic scientists with appropriate industrial partners in an entrepreneurial manner in order to improve the competitive and independent position of the EU
COUNTERACTING EXPLOSIVES	Development of an extended European platform for Explosives with connections to knowledge centres, research facilities and the relevant Security organisation. Objectives: ▶ Accessible information systems with data on actual and new threats with explosives and the options for detection, identification and elimination of explosives in a number of possible situations ▶ Standardisation and - if necessary - certification of techniques concerning explosives ▶ Arrangement of mutual use of validated facilities ▶ Coordination of the formulation of widely accepted regulations concerning restrictions on the use of precursors for HME's and improved control during transport and storage of explosives and their precursors

1.3 Conclusions

1.3.1 Clusters of needed capabilities

A systematic analysis of the threats concerning the security of the citizen has revealed the need of capabilities at different levels. Clustering the indicated capabilities in the previous paragraphs results in the following list:

A. Society as a whole

- Citizens should be better prepared for security incidents, more intensively involved in the security issues related to their environment and should actively contribute to the security effort in the event of a crisis
- Society should be more resilient against security threats of a social origin by improving social coherence/ trust and by improved capability for early warnings and response to weak signals of potential tensions
- Authorities should strengthen the set of legislative instruments for preventive and responsive measures at the required national or international level

B. Societal systems

- Supply chains should be better protected against counterfeiting
- Information infrastructure should be better accessible for diversified users via secure user-specific interfaces
- ICT-infrastructure, financial and payment-systems should be better protected
- European cooperation for enhancement of resilience of societal systems should be strengthened

C. Security tasks

- Civil protection should develop a more powerful information infrastructure aligned with the involvement of all the participating actors during operations

- Law enforcement and intelligence agencies should improve their capabilities with respect to Public Private Trusted Information Exchange.
- New forensic sciences should be applied to non-traditional options for fighting against crime.
- Counteracting explosives should develop an information infrastructure that is accessible to all who need this confidential information, with as a special option to support the brigades on route.
- Security personnel should be better trained and educated by setting up an infrastructure for making use of lessons learnt in other parts of Europe.

exchange of new, successful approaches and development of new improved approaches for the threats and incidents to be dealt with.

1.3.2 Research priorities (for the ESRIA)

ESRIF working group 1 selected the following research needs as priorities for the ESRIA:

- Methods to improve the social coherence of the society. Trust between citizens and societal structures is a key factor for prevention of feelings of uneasiness and of seeds for rumbling processes. Mutual respect of population groups with significant differences in welfare or in ethnic and religious backgrounds needs attention. A resilient society requires, in case of security incidents, the alert acting of well prepared citizens, as well as efficient, flexible and proportional acting organisations for intelligence, sharing of situation awareness and coordination of preventive and responsive actions.
- Analysis of mechanisms with respect to lack of solidarity between citizens from various parts of society and making social and societal barriers more porous. This analysis should result in a methodology for the development of methods for an early detection of tensions between population groups and subsequent practical measure to diminish risks.
- Analysis of the relevant socio-economic factors for the development of organised crime and the creation of barriers for further related progress.
- Advanced and virtual methods for education and instruction of citizens, public bodies, first responders and other security services in order to reach a more effective response to security and safety threats. These methods should challenge the participants' imagination by using modelling, simulation and serious gaming.
- Technologies for improving the effectiveness and/or the efficiency of physical measures for the protection of persons, infrastructure and living areas.
- Systems for the surveillance of public areas and specific locations by automatic analysis of observations combined with databases containing intelligence information.
- Fast and reliable detection and control systems concerning explosives at vulnerable locations, buildings and events
- Methods and information infrastructure for supporting interventions and communication to communities, and individuals, in case of (large scale) incidents. This includes systems processing sensor data, real-time observations and information in a well structured way. Other topics are environmental alert systems, detection sensors for UAV's, balloons and satellites. Special attention is needed for alerting the right people with the proper information and instructions without overloading human beings with information.
- Information systems with multiple interfaces, suited for consulting by different categories of users in the event of suspicious activity. A special feature should allow their use by mobile surveillance and intervention brigades.
- Development of better aligned doctrines, equipment and procedures for interventions in several categories of characteristic incidents. Education and training of decision makers, public services and citizens, through exercises in realistic environments around validated scenarios, should be facilitated by new techniques for modelling, simulation and gaming. The virtual extensions of the real environment offer a promising challenge.
- Artificial analysis methods and agent technologies to support investigations in relevant sectors of society. A special issue is the development of methods for retrieval and analysis of data and information available in unstructured, multilingual texts in an enormous variety of proprietary and open sources.
- Tracing of illegal activities and analysis of patterns of behaviour of organised crime groups in cyberspace, with special attention to financial and payment systems.
- Internationalisation of information and communication infrastructure for dealing with security issues. The legislative framework, the technical architecture and the standardisation of tools, databases and protocols should make it possible to set up specific ICT-systems which can be used under different levels of security restrictions. These systems should be

accessible for many users with different user profiles, interoperable with a whole spectrum of data sources and information systems, provide a variety of options for modelling and simulation and user specific interfaces and should enable the support of the security services while they are on patrol.

2. Working Group: Security of Critical Infrastructures

2.1 Introduction

With the creation of ESRIF in September 2007, WG2 «Security of Critical Infrastructures» was established as the single largest Working Group in terms of constituency (>120 nominal members) and scope (11 topics). This called for streamlined handling, clear lines of responsibility and tight leadership despite mostly remote-coordinated work.

From the outset, the Working Group adopted the European Commission's definition of Critical Infrastructures (CI) as outlined by the EPCIP (European Programme for Critical Infrastructure Protection). This served to provide a common basis for the topic experts, who came from numerous countries where such definitions varied:

EC definition of Critical Infrastructures:

1. Those **assets, systems or parts thereof** which are **critical for the maintenance of critical societal functions**, including the supply chain, health, safety, security, economic or social well-being of people, and the **disruption or destruction of which** would have a **significant impact** in a Member State as a result of the failure to maintain those functions. Or
2. any other (hazardous) assets, systems or parts thereof the disruption or destruction of which would, as a direct consequence, have **a significant impact on the maintenance of critical societal functions.**

On December 8th 2008, with the European Council Directive 2008/114/EC, this definition was changed:

An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

The aim of streamlined handling was then achieved by aggregating several topics into three dedicated subgroups (Transportation, Information and Communication Technologies (ICT) and Distributed Networks) and covering the remaining topics using panel meetings. The latter approach was also taken for cooperative topics with other WGs, such as Security of Space Infrastructures (with WG7 «Situational Awareness and the Role of Space») and Protection from EMP (with WG 6 «CBRN»).

Thus structured, WG2 analysed in excess of 60 policy and strategy papers referring to Critical Infrastructure Protection (CIP), cross-referenced with numerous national and European-level initiatives and networked with all other WGs either directly/bilaterally or via Integration Team and Transverse Committee meetings. Some experts were called in where needed, e.g. to participate in panels that did not already enjoy intensive coverage from participating experts, so that by February 2009, all the topics covered by WG2 (and others) were covered and systematised by use of a matrix. This was achieved through strong interaction between the WGs, particularly with «adjacent» mission groups («Security of the Citizens» and «Crisis Management») and relevant technology and context WGs.

In earlier stages of work, the risk and challenges analysis was finished in summer 2008, leading to the capabilities and gaps analysis that provided the raw data for research recommendations. The systematic analysis and refinement of that raw data was completed in March/April 2009, enabling the more detailed deduction of key messages and recommendations.

WG2 Scope of topics	**WG2 Subgroups**
1. Energy (generation, transmission, storage, oil/gas power production and transport) **2.** Nuclear Industry **3.** ICT **4.** Water **5.** Food **6.** Agriculture **7.** Health **8.** Financial **9.** Transport **10.** Chemical Industry **11.** Space	▶ Transportation (air/sea/land, including site security) ▶ ICT (incl. finance) ▶ Distributed Networks (power, water etc.) **WG2 Panels** ▶ Space infrastructure (with WG7) ▶ Health infrastructure ▶ Food infrastructure ▶ Agricultural infrastructure ▶ Protection from EMP/HPM (with WG6) ▶ Finance infrastructure (recap in light of crisis)

2.2 Risks and Challenges

The second step in our work was the definition of key risk factors and challenges that affect the protection of critical infrastructures in the mid and long term. Even though the objective was to identify novel risk factors and challenges, the WG could not omit those that are already known and which will continue to prevail in the long-term perspective that ESRIF takes.

From the perspective of WG2, two aggregated risks and five challenges seem particularly relevant.

Terrorism, crime and violent actions are some of the key drivers of risks to citizens and critical infrastructures. These attacks can be staged not only from the outside, but also from inside a system itself. The socio-psychological effects – panic, distrust, loss of public order - of a successful attack (broadly defined: destruction, disruption, spoofing, hijacking, etc.) on any critical infrastructure contributes to the attractiveness for attacks that these infrastructures possess.

Natural disasters and emergencies are another area of risk commonly addressed in the analysed papers. These incorporate earthquakes, droughts, floods, storms and pandemics caused by natural mutation. All critical infrastructures will be affected in different ways, partially, directly or indirectly and with a degree of interdependence between such infrastructures that often leads to spill-over effects. In light of the expected climate change effects, regionally specific risk aspects apply (e.g. thawing of permafrost in mountainous regions and in arctic areas) and there are specific concerns with regards to eco-system degradation (e.g. the extinction of native species, the invasion by non-native species or the emergence of diseases that were previously unknown in Europe).

The first challenge to be addressed is the **emergence of new or increasingly dangerous potential threat vectors.** New means of an attack can be developed technically (i.e. EMP improvisation, hacking methodologies and tools) or might naturally occur (i.e. pathogen mutation) which in turn can destabilise critical infrastructures directly or indirectly; all critical infrastructures are vulnerable.

This is further compounded by the fact that **critical infrastructures will increasingly be technical in nature or be controlled by ever more complex technologies.** These being mostly civilian and COTS (commercial off-the-shelf) in nature, a high degree of systemic vulnerability is evident, with interoperability cutting both ways: While functionally being a distinct advantage, interoperability will need to hinder cascading or chain effects. Naturally, critical infrastructures that are heavily dependent upon technology are most affected, e.g. ICT-, power supply-, mass transportation- and space infrastructures.

Weaknesses inherent to existing systems can be expected to remain in the coming years. Non-standardisation and limited interoperability will remain an obstacle to the early resumption of normal operations. The underlying ICT infrastructures are as vulnerable as critical infrastructure operations, especially to terrorist or malevolent/nuisance attacks. Indeed, the inappropriate handling of such systems by operators can also be a root cause of incidents. The mere existence of such a system may pose an obstacle to the introduction of better suited systems. Similarly, there is often an absence of adequate legal frameworks for critical infrastructure security and a real need to look at property rights and the complexity of ownership with regard to State and private operators. Thus, some critical infrastructures are weakening due to age and exposure, while service demand is increasing. It is to be expected that out-dated systems, especially process control systems, will at best receive patchwork upgrades that lead to new inherent weaknesses. From past experience, it can safely be extrapolated that power and water supply systems, as well as first-generation ICT and transportation infrastructures, tend to be more vulnerable.

Lastly, the **emergence of entirely new critical infrastructures**, or the evolution into new qualities of criticality for existing infrastructure, must be expected. These developments might be policy-driven or based upon prior technological developments. The particular vulnerabilities and failure conditions will have to be examined up front, as new systems are more likely to offer new means of service disruption or misappropriation. For WG2, biodiversity itself is a Critical Infrastructure, given the impact that interference or loss (man-made or natural) would have on food, water and health. These challenges will be reflected specifically in the recommendations section of WG2.

All of these risk factors and challenges will probably remain stable even through diverse possible futures; cross-checking with WG5 («Foresight & Scenarios») has shown that a) many other WGs have identified similar aggregated risk patterns and challenges and that b) changes in scenarios lead only to different «flavours» of the same risk or challenge, such as what is being considered «critical» in a benevolent or an antagonistic future. All overarching and most detailed recommendations still remain the same. What is deemed to be critical still needs to be protected and secured and the provision of services still needs to be ensured.

But there remains one major uncertainty: The analysis assumes that Europe and the world at large at least remain somewhat similar to what is seen today. An incident, however unlikely, with global cataclysmic dimensions or radical and completely unanticipated changes in Europe's political structure and environment, can nullify, change or strengthen assumptions. It is this unknown that constitutes the absolute necessity for perpetual re-evaluation of ESRIF's assumptions, findings and recommendations in light of developments.

2.3 Capabilities, Gaps and Research Needs

In its analysis, WG2 extrapolated and derived key capabilities from the long-term scenarios provided by WG5 (Foresight and Scenarios) and from which CI security would benefit from in the future. Again, some of these capabilities may not be new, but Europe needs to either attain these capabilities in the first place or improve their performance. In some cases, it is a matter of developing a common approach to something that is being or will be done, but in a fragmented way; in other cases, it necessitates thinking in new ways.

2.3.1 Water Supply

Water supply security also heavily stresses prevention and protection, with reactive measures requiring rapid detection and identification of all possible agents (that is Chemical/Biological/Radiological/Nuclear, CBRN), and subsequent alerting of operators and public health officials. Preventive water treatment is generally reliable and at high levels already (>99% elimination quota), with disinfectants being added after treatment in some countries, acting as a «carry-on» prevention. Therefore, remaining or new contaminations after treatment need to be detected and identified rapidly via spatially dispersed but networked biosensors within the supply pipes. Speed is of the essence here: If an incident is detected early enough, emergency procedures can easily and vastly limit damaging effects. Lastly, these need to be coupled to adaptive prediction models of contaminant dispersion in order to facilitate rapid alerting and shutdown procedures.

The assumptions of future risks in this regard specifically refer to materials/system deterioration due to the lack of investment leading to contamination, or individuals actively introducing agents into the water stream. In these cases, an obvious gap appears: The current detection model works using germs that, if present, indicate the presence of others as well. If these «indicator germs» are not present, the system will appear clean even though it may carry vast amounts of agents. CBRN sensors are not in use at all. Broad-range, networkable and dispersible CBRN-, particularly bio-detectors are nonexistent. Identification is still too costly, time-consuming and not necessarily readily available. Flow and prediction models exist, but are dependent upon such sensor data in order to truly help when time counts. Lastly, rapid links into the public health system of the affected area exist only in some places.

Research Needs: Water Supply

	RESEARCH NEEDS
DETECTION	▶ Spatially dispersed, networked and affordable full spectrum contamination sensors (CBRN, especially biosensors) ▶ Miniaturisation and cost-reduction of sensors
IDENTIFICATION AND VERIFICATION	▶ Rapid, on-site incident verification methodologies and tools ▶ Rapid, reliable and on-site identification tools
DECONTAMINATION	▶ Rapid, effective localised and large area decontamination procedures and tools
INCIDENT RESPONSE, MODELLING AND	▶ Linkage of flow-modelling tools into fast adaptive prediction models for control rooms
CONTROL	▶ Direct links to public health communities affected, along with hierarchical reports (to e.g. WHO)
EDUCATION AND TRAINING	▶ Similar preparedness levels of employees for low-level and high-impact scenarios ▶ Emergency preparedness and cooperation methods and tools for the public, operators, health and crisis management experts

2.3.2 Health Services

Health infrastructure provides an essential tool for effects mitigation of course, but it is subject to risks and challenges, so the perspective goes beyond what such an infrastructure should consist of and provide to include how it can be secured. Particular challenges for health systems are access to and administration of medicines in remote environments such as maritime and the complexities and challenges related to mass casualty incidents in these environments.

The already widespread practice of counterfeiting medicine and medical equipment will require assurance of origin, supply integrity and legal sales, in other words seamless tracing from factory to pharmacy/hospital and that being done via «trusted suppliers» who adhere to stringent rules. Naturally, such suppliers will need to be somehow subject to European rules, and be available to EU citizens upon necessity (e.g. jump-starting mass-production of vaccines or of specific drugs), and therefore a political action to keep core medical production capabilities in Europe is in order. These core production capabilities must cover the whole treatment chain, from diagnosis to treatment and ancillary equipment (e.g. syringes, masks, bandages etc.). Pharmaceutical effectiveness will also require constant research into new or better diagnosis tools, treatments and drugs (i.e. antibiotics). What applies to water and food security (see below) also applies to health services: Scanning, detection and identification of agents/contaminants will need to be readily available, as will access rights in hospitals, whose security must also be considered. Similarly, the information associated with health operations – insurance data, patient history, simulation

data – will need to be secured, requiring attention to site and ICT security as well. Lastly, it is also within the remit of health services to assist in the detection of illegal sources of knowledge on CBRN agents.

With health infrastructure being only rarely considered as part of security, a lot of the above mentioned future capabilities are lacking or incomplete. Counterfeit medical supplies can be easily accessed via the internet with little regulation in the way and no trust-network being established beyond informal arrangements. Thus, end to end authentication of product sources is very limited. Emergency stockpiles of vaccines are available, but jump-starting mass production of vaccines is difficult, as Europe loses its pharmaceutical manufacturing base to worldwide relocation. This naturally also affects the R&D capabilities with regards to new and more effective treatments.

Research Needs: Health Services

	RESEARCH NEEDS
DETECTION, VERIFICATION AND HEALTHCARE COMMUNICATION	▶ Development of affordable, efficient and effective first diagnostic tools (i.e. agent sensors, infection markers and indicators) for public availability ▶ Assurance of privacy of patient data
ASSURANCE OF AUTHENTICITY AND GENERATION OF TRUST	▶ Seamless tracking and tracing of medical supplies from source to customer (hospitals, pharmacies, customers etc.) ▶ Definition of "trusted supplier" programmes and benefits derived
EMERGENCY TREATMENT CAPABILITIES	▶ Stocktaking of critical pharmaceutical manufacturing capacities and jump-start capabilities (i.e. rapid mass-production of vaccines) ▶ Constant research and development in/of vaccination and treatment capabilities for emerging and newly infectious diseases ▶ Delivering medicine in remote environments (e.g. Maritime) during mass casualty incidents
EDUCATION & TRAINING/ EMPOWERING THE PUBLIC	▶ Simulation and public exercises with new communication methods

2.3.3 Food and Agriculture Security

Food security, overlapping with agriculture, will have to focus heavily on prevention and protection of foodstuffs, with reactive capabilities being either recall of goods or in the remit of health services (i.e. vaccinations or culling). The crucial capability, therefore, will be the seamless tracing and guaranteeing of integrity «from farm to fork». The challenge stems from the very nature of the «farm to fork» chain, that includes family owned premises, small businesses, industrial processing plants or highly concentrated wholesale markets. Suppliers and handlers will therefore have to act according to certain, Europe-wide valid sets of good practices, laws and regulations (guaranteeing trust) to guarantee that food is not tampered with or spoiled, and implement systems enabling such tracing of goods. This, in turn, will facilitate easy control of recall action effectiveness, as returns can be measured against sales, batches localised and special public awareness actions can be taken. Foodstuffs marked as spoiled or contaminated need to be detected, cleaned or eliminated. Ideally, such tracing and procedural elimination on the part of producers and suppliers will be supplemented by affordable and readily available sensors that can alert consumers if food has spoiled or been contaminated.

Tracing capabilities are existent in the form of the barcode, but the actual monitoring is very limited and untimely. Bar-coding commences at the processing stage, not necessarily with the farm or source itself. Thus, while authentication and tracing capabilities exist, they need to become tighter and effectively seamless. Current technologies are only capable of this to a limited extent, and the awarding of the status of «trusted supplier» does not occur. Throughout the production and supply chain, biosensors and decontaminators are not currently

available or deployed. Procedurally and legally, differing levels of strictness of agricultural guidelines on farms apply, thus making cross-border comparability or actions impossible. This non-harmonised state enables gaps in quality control, beginning at the farm level and ending with customers, and opens up possibilities of fraud and other criminal activities.

Marine and agriculture food policy requires specific attention within security research programmes. Supply chain security is important but must be linked with innovative research into ways to secure the food source. In a recent UN Report, they estimate that food production must increase by 70% by 2040 and to achieve this we need new and better ways of producing food. Protecting habitats and biodiversity can provide a level of assurance if based on robust security research and enhancing our knowledge of effective means.

Research Needs: Food and Agriculture Security

	RESEARCH NEEDS
ASSURANCE OF AUTHENTICITY AND GENERATION OF TRUST	▶ Enhanced risk and vulnerabilities assessment methodologies ▶ Seamless tracking and tracing of livestock, foodstuff and agricultural products from source to end (i.e. shops/customers or processing stages) ▶ Continuous improvement and quality assurance in food processing facilities and machinery ▶ Development of comparable best practices, laws and regulations across Europe regarding food and agricultural safety and security ▶ Definition of "trusted supplier" programmes and benefits derived ▶ Evaluate applicability of European Security Label for food/agriculture domains
DETECTION, VERIFICATION AND RAPID REACTION IN CASE OF INCIDENT	▶ Development of affordable, effective and efficient biosensors ▶ Rapid recall issuing and monitoring capability
DISPERSED PREVENTION	▶ Development of affordable, effective and efficient biosensors as well as decontaminants for public availability ▶ Empowerment of the public through education (knowledge dispersal) and training (preparedness)

2.3.4 Transportation (air/sea/land)

The field of transportation, particularly of people, is a prime example of needing to prevent and protect first and foremost. To achieve this, comparable risk and vulnerability as well as effects assessments need to be developed where they are non-existent or of limited use and updated where necessary. Cross-border background checks will be ever more important to distinguish between trusted employees and passengers and those that pose potential risks – something that is not entirely practicable today.

Surveillance and screening systems in boarding/loading facilities will need to be able to spatially channel, accommodate and monitor huge crowds continuously and then rapidly focus to track potential suspects while not losing sight of the crowd; this requires adaptive networks of sensors, behaviour pattern analysis and cognitive computing networks. Coupled with biometric recognition systems these can be effective tools in the hands of security agencies. This also implies planning with foresight, meaning facility layout conception and even urban planning procedures need to bear in mind that, in an emergency, vast amounts of people will need to leave the area fast, under chaotic conditions. Hazardous materials will need to be detected early and reliably; such sensors will need to be contactless and appropriate to the environment. Having the capacity to deploy these at all mass transport

embarkation points will be important where the security risk requires it. During transportation, operators will want real-time and seamless localisation tools, as well as information on integrity and behaviour, particularly in the realm of maritime security. At its heart, this will need considerable computing power, correlating and transferring of data in real time, sifting and mining data stored and fed from the numerous information feeds. Only a complete, holistic and correct situational picture will provide proactive, preventive as well as protective and reactive capabilities that this critical infrastructure requires.

But the degree to which this holistic and integrated approach to security is implemented is wildly diverging: Airports feature a high level of security against the last attempted methods of attack,but they fail to plan adequately for other possible scenarios. The mid-2009 case of a member of the Saudi-Arabian royal house surviving a bomb attack, whose perpetrator seemingly carried the explosives inside his body, may have protective repercussions, particularly in airports – but also clearly demonstrates the need to remain vigilant to new forms of attack. These and other future developments need to be, if possible, anticipated, and «thinking like a terrorist» should be encouraged in security experts. Most railway stations have no security checks at all. Hazardous material detection is rudimentary at best, and sensors surveillance in general is, as yet, incapable of tracking and identifying; remote biometrics is still in a pre-usage development phase, as is behavioural pattern analysis. Evacuation route planning is the norm in facility layout design, but not in urban planning – this needs to change for city development and must be addressed for existing cities. On a larger scale, while coastal and Exclusive Economic Zone (EEZ) surveillance methods are getting close to real-time, the monitoring of international waters is incomplete and subject to irregular passes with Maritime Patrol Aircraft or surveillance satellites. Even if these assets existed, as with other Critical Infrastructures, the amount of data generated and stored already far exceeds computational and cognitive correlation/processing capabilities, leading to massive amounts of potentially crucial data being lost and forgotten. In addition to the technical aspects of attaining appropriate levels of maritime domain awareness (MDA) in shared international spaces, there are also the political and social issues of institutional integration and information sharing. We require security solutions that support decision making and assist security personnel in interpreting the information provided and some of these solutions need to be suited to the peculiarities associated with international shared space.

Research Needs: Transportation (Air/Sea/Land)

	RESEARCH NEEDS
RISK AND VULNERABILITIES ASSESSMENT METHODOLOGIES	▶ Systemic interdependence and interconnection awareness ▶ Advanced simulation and modelling tools ▶ Integration of emergency planning requirements into system, e.g. facility and urban planning, procedures ▶ Privacy protection / abuse prevention assurance methodologies
INSTITUTIONAL INTEGRATION, INFORMATION EXCHANGE AND RATIONAL DECISION MAKING FRAMEWORKS	▶ Systematic and systemic tools to enhance planning and cooperation ▶ Integration of institutional requirements in information exchange and decision making tools
RESILIENT ARCHITECTURES	▶ EMP-/HPM hardened system cores and emergency control functions
DESIGN, INCLUDING SECURE CONSTRUCTION AND PROTECTION	▶ Inter-system contingency/fallback planning procedures ▶ Smart materials for use in vehicles and facilities ▶ Good security practice in construction of node and hub facilities ▶ Continuous improvement of protective means, e.g. countermeasures

SEAMLESS TRACKING / TRACING/LOCALISATION OF VEHICLES, CRAFTS AND GOODS/ CONTAINERS	▶ Advanced manned/autonomous platforms (aerial/naval/ground-/space-based) ▶ Wide-area and localised surveillance of air/sea/land transportation networks ▶ Multi-sensor networks ▶ Data-fusion and cognitive correlation of intelligence/sensor feed ▶ Secure remote IDing of vehicles, crafts and goods/containers ▶ Remote health-monitoring/ status query capability
HIGH-PERFORMANCE SENSOR TECHNOLOGIES	▶ Remote, mobile and high-throughput capable hazmat sensors (CBRNE) in passenger and bulk-freight/goods environments ▶ Crowd monitoring and suspicious behaviour analysis tools ▶ Continuous enhancement of existing scanning technologies (e.g. radar, IR, visual etc.) and instruments
INFORMATION ASSURANCE	▶ Continuous improvement of encryption technologies
INCIDENT RESPONSE	▶ Advanced common situational/operational picture generation and dissemination ▶ Autonomous damage assessment and mitigation ▶ Autonomous incident detection and alarming ▶ Adaptive modelling and simulation tools for incident effect extrapolation, tied in to control room systems
FUTURE AWARENESS	▶ Assessment of future, possible transportation system characteristics and security requirements (i.e. sub-orbital flight etc.)

2.3.5 Power Generation, Transmission and Storage (incl. oil and gas supplies)

Power generation, transmission and storage will, due to their spatially dispersed nature, have to focus on reactive measures to increase resilience and assure service provision. Since we assume no large-scale investment in distribution and transmission lines to happen, while demand may still increase despite consumption-reduction initiatives, the immediate dispersal of overloads due to lines going down will be a necessity. This does not denigrate preventive measures, such as the absolutely necessary capability to «dynamically island» power distribution lines to avoid cascading effects or the need for better harmonisation procedures across frequency areas (under-/over frequency) in getting grids on-line again. Again, such a centralised system is only manageable with a powerful IT backbone infrastructure, requiring stringent measures in ICT security; this is particularly the case where internet access is facilitated by local power grids. Furthermore, the use of modern technologies and services (like smart grids based on public telecommunication channels, street/traffic light control over the internet, facilitating internet access by local power grids, etc.) requires special attention to very specific security aspects, particularly considering that these technologies often directly connect to the basic supply systems of European societies. The trend towards autonomous, decentralised power generation, even home-based micro-generation, can offset this, though, and would contribute to systemic resilience. This, in turn, can serve to reduce European dependency upon dwindling and potentially politically usable natural resources, such as coal and gas. Naturally, this will mean that efforts put into the development of substitutes and other power generation technologies have a security impact.

Larger power generation sites will still need to be protected, particularly nuclear processing sites. This goes beyond a set of «good practices», requiring a mix of state-of-the-art surveillance, verification and protective means, such as e.g. using smart materials in construction. With most of the European energy market in (semi-) private hands, thus being subject to a business paradigm that is not naturally inclined to include maximum security will require market models that go beyond those currently in existence as well as a consistent legal and regulatory framework throughout Europe. In general, for prevention and preparedness purposes, extensive multidisciplinary simulation and risk/vulnerability/effects assessment tools will be necessary.

Significant gaps were identified in the prevention of chain effects throughout an ageing infrastructure, the cascading of adverse effects into other critical infrastructures (e.g. affecting telecommunications via SCADA systems), and, most importantly,

the rapid on-lining of powered-down grid parts. This procedure is hampered by structural differences (frequency, ownership etc.) that need to be overcome in the future. The systemic digestion of load spikes is still problematic and requires a long-term solution. Therefore, incident mitigation shows huge gaps that need planned and thorough closing.

For natural gas and oil pipelines/refineries, different capabilities will be necessary. It is likely that these will be subject to government influence, so a major part of securing the provision of these resources will be the political stability and reliability of source and transit countries, thus being beyond the remit of ESRIF and the ESRIA. This is not the case however with the infrastructure itself: Again, sites require strong access control systems, but pipelines naturally are stretched over long distances between stopovers, often through remote areas, limiting protective capabilities and thereby requiring backup routes and up-to-date damage mitigation methodologies. The importance of Liquefied Natural Gas (LNG) sites and transportation will assumedly significantly increase in importance in the next twenty years. The extreme volatility of LNG, along with the large distances to be covered in transportation will require seamless localisation, monitoring and effective mobile protection mechanisms in international environments, and high standards of technical, material and procedural security on site. Renewable and sustainable energy sources and distribution networks will also need careful consideration in this regard.

The main gaps identified in this regard are surveillance means and proactive effect mitigation efforts. No spatially available surveillance means are in place, nor are integrity monitoring systems; effectively, many stretches of vital supply lines are completely invisible to operators, their only indication of something going wrong being the flow stopping. Once that happens, as fallback solutions are not readily available, the delivery of vital consumables can be endangered.

Research Needs: Power Generation, Transmission and Distribution (incl. oil and gas supplies)

	RESEARCH NEEDS
RISK AND VULNERABILITY ASSESSMENT METHODOLOGIES	▶ Systemic interdependence awareness (e.g. power transmission-ICT), sophisticated modelling and simulation models to analyse and understand dependency and cascading risk ▶ Critical generation resource dependencies and substitutes R&D ▶ Awareness of chain and cascade effect enablers and barriers ▶ Security requirement specifics of decentralised/dispersed power generation facilities ▶ Security requirement specifics of "green" power generation (e.g. off-shore/foreign solar farms and wind parks ▶ Security requirement specifics of micro-power generation and smart metering
RESILIENT ARCHITECTURES DESIGN	▶ "Dynamic islanding" of network segments, static and flexible barriers ▶ Hardened, resilient system control IT
SECURE CONSTRUCTION AND PROTECTION	▶ Smart materials in facilities and transportation means construction (i.e. pipelines, LNG storages and maritime transport) ▶ Enhanced, secure energy storage means and capabilities ▶ Advanced hard/soft site security and surveillance technologies ▶ Enhancement of access control technologies: identification, ID verification, tiered access authorisation
NETWORK SURVEILLANCE	▶ Wide-area and localised surveillance sensors and platforms in spatially spread power transmission networks and transportation means (esp. maritime LNG transport surveillance) ▶ In-system status feedbacks and health monitoring

INCIDENT RESPONSE/ EFFECTS MITIGATION	▶ Methods and tools to rapidly re-online diverse network parts across electrical power frequency borders (over-/under-frequency) ▶ Sophisticated modelling and simulation models of EU and MS energy grids to support incident response decisions ▶ Improved automation functions in system control, e.g. for autonomous, immediate re-routing
FUTURE AWARENESS	▶ Identification of new, secure power generation means

2.3.6 Information and Communication Technology, including Financial Systems

Without doubt, this area warrants the most attention, since societies and economies are becoming ever more dependent upon ICT to even attain basic functioning capabilities. The speed and complexity of current and future business processes are only enabled by the use of ICT, and even small-scale events can have dire consequences. Furthermore, the ICT industry is a globalised one, with a complex supply chain that spreads beyond Europe for the most part: traceability of equipment is almost impossible to achieve.

Therefore, future ICT systems, apart from growing in terms of processing capacity, will feature certain autonomous functions, limited self-healing, cognitive correlation and cyberspace pattern recognition capabilities. Security approaches will be less static, moving away from a «fortress» mentality towards a flexible policy of security enforcement. «Trusted nodes» will play a crucial role here, both from an end-user (society interface) and a professional operator perspective (professional interface). Verified and authenticated e-identities of both users and operators, leading to a certain trusted/suspect validation for sourced information, will constitute a great part of ICT security and access rights, thus the privacy implications of this term (e-identities) will have to be examined closely. Naturally, e-identity theft will continue to be a major problem in the future. As such, authentication means will need to be sophisticated, continuous, unique and assured. Managing data generated and stored will be an essential capability, as well as the immediate alerting of a system of a suspicious action or a detected attack. Overall and in order to achieve all that, computational power will have to increase exponentially as well, as will data correlation, mining, sifting and general management capabilities.

Whereas systemic flexibility, i.e. the adaptation of a system to local failures (re-routing etc.) is already quite high, the concept of sophisticated ICT-security is as yet rather amorphous: Protective layers are static («firewalls», mechanical disconnects etc.) and identities too easy to steal. The entire concept of e-identities still remains to be both defined and analysed as to their implications for ICT security; a chaos that gives rise to the relative ease of identity thefts currently experienced. Plus, and because of this, privacy is a relative term in cyberspace security. At a systemic level, the amount of data generated, stored and forgotten far exceeds computation and correlation powers, complicating the approach to systemic data usage for security purposes. Thus, the question of access to such data, even remote access via mobile terminals, is moot. However this will be crucial in the future, especially for security operatives that rely on Professional Mobile Radios for voice/data transmission. These, again, feature divergent hardening (from nonexistent hardening up to full immunity) against hardware and software infringements (i.e. EM/HPM pulses, hacking etc.). The issue of more sophisticated encryption technologies is an ongoing concern, as the means of attack increase and diversify. As the usage of commercial off-the-shelf (COTS) solutions increases, so too does the importance of making COTS more resilient.

Within the remit of critical infrastructures, the topic of ICT security is significant: So many of our societies' vital functions now depend upon ICT control (business processes, financial flows, operational control of systems, remote access to public services etc.) that it is almost inconceivable for society to operate without it. Therefore, the differing public research endeavours that relate to ICT functions – meaning also transportation, power transmission control, etc., should closely interact with specific ICT research programmes. ICT is a cross-cutting theme and must be treated as such.

Research Needs: Information and Communication Technology, including Financial Systems

	RESEARCH NEEDS
"HARD" ICT SECURITY	▶ Affordable hardening and immunisation of civilian critical cores/nodes and system elements against various kinds of interferences (i.e. mechanical tampering, EMP/HPM effects etc.
CYBERSPACE SITUATIONAL AWARENESS, PREVENTION AND PROTECTION	▶ Development of methods and procedures to detect suspicious web sites ▶ Continued development of anti-virus programmes extended with online investigation modules for identification of and attribution to senders of messages ▶ Development of international applicable unique interfaces, protocols, connectors etc. for trusted exchange of sensitive information ▶ Parameterisation methodologies for detection of suspicious cyberspace behaviour
SECURE IDENTITIES	▶ Continuing improvement of publicly available encryption/authentication methods ▶ Development of secure protocols and architectures that verify e-identity/-ies
CYBERSPACE FORENSICS	▶ Development of capabilities to trace illegal activity in cyberspace back to its origin. In addition, enhanced detection methodologies and blocking/filtering technologies ▶ Enhanced identification processes and investigative tools
EDUCATION AND TRAINING	▶ Methods for increasing user awareness on the potential risks of ICT-behaviour

2.3.7 Security of Sites (nuclear, chemical, biological, financial, research)

Securing sites linked to critical infrastructures will still represent points of emphasis due to the nexus character of these sites: They usually offer privileged access to a system, dispersal potential and maybe even varying control functions. The crucial issue therefore will continue to be limiting access to site and critical infrastructure functions and mitigating disturbance effects. Site security thus will need advanced protective materials (i.e. «smart» materials), real-time sensor data on people on-site, correlation with zone access rights, behavioural pattern analysis capabilities, tiered data access and control rights, etc. – in short, tight monitoring of who is on a site and what he/she is allowed to do, and correlating this to actual sensor feeds. Particular sites, like radiological or bio-labs, will continue to need state-of-the-art containment and decontamination facilities. Where possible, the area of surveillance, usually beginning at the perimeter and moving inwards, should be extended outwards to access routes. Here, behavioural pattern analysis could constitute a useful tool in providing advance warnings.

The already technically possible security level is relatively high, with almost all required capabilities existing at least in theory. But the degree of implementation varies vastly: Where tight regulation is in place (e.g. nuclear or bio-lab sites), standards are generally enforced and resulting in a comparably high level of security. Gaps identified are therefore in the area of security implementation, and have been identified for example in the area of hazardous materials detection (CBRNE) and data fusion capabilities in large scale sites.

Research Needs: Security of Sites

	RESEARCH NEEDS
DETECTION AND VERIFICATION OF INTRUSIONS AND INCIDENTS	▶ Continuous improvement of novel indicators, moving beyond classic sensor technologies, for situational awareness and alerting ▶ Extension of surveillance to access routes (while in line with privacy and individual rights protection) ▶ Psychological research to detect and potentially trigger-reveal malicious intent (i.e. via bio-/psychosomatic reaction triggers

"HARD" PROTECTION OF SITES	▶ Development of "smart materials" capable of reacting to tampering or passing on information to control rooms ▶ Development behaviour pattern analysis capability and abnormal behaviour detection ▶ Continuous improvement of containment technologies and automatic shutdown/ alerting/reactive capabilities (i.e. decontamination in case of bio-labs)
ACCESS LIMITATION	▶ Remote query of access-right authentication ▶ Continuous improvement of encryption and ID-based tiered access right awarding

2.3.8 Space Infrastructure Security

European civilian space infrastructure – mainly GALILEO, KOPERNIKUS and the numerous telecommunication satellites – will need to cope with increasing dangers in orbit (e.g. debris, material failure, ASAT interference etc.), on the ground (installation/site security) and on a system level (e.g. hacking, blinding, spoofing, etc.) and still be able to provide their intended services. That requires either manned space repair capability, or novel approaches to system architecture on orbital platforms. With control and data feeds being inherently ICT-based, these will have to be strongly encrypted if used in security contexts. Space platforms themselves would profit from direct proximity awareness and, on a larger scale, from a common European space situational awareness (SSA) capability.

There are numerous gaps in these capabilities, and some will probably never be truly closed, like the systemic vulnerability to direct ASAT measures or hacking, blinding and spoofing. Therefore, space based capabilities need to be able to cover loss of individual assets, and while reserve capabilities are in place to a limited degree, a concerted attack can cause severe damage. Space-based repair capability does not exist outside the USA. ICT is subject to continuous improvements in the means available to hackers and thus to a fast product lifecycle in security products, and while investment here occurs, gaps and vulnerabilities will always remain. The aim must therefore be to make the entire system more resilient to such incidents to ensure that the intended service is provided.

Research Needs: Space Infrastructure Security

	RESEARCH NEEDS
RISK AND VULNERABILITIES ASSESSMENT	▶ Assessment of civilian space asset risks, protective and reactive means with reference to existing and foreseeable threat vectors
SECURE CONTROL AND COMMUNICATION	▶ Progressive encryption improvement and rapid implementation ▶ Hardening and redundancy of command and control systems ▶ Advanced operations conducive to security (e.g. improved burst-communication)
SPACE ASSET SITUATIONAL AWARENESS	▶ Immediate asset proximity awareness capability ▶ Overall Space Situational Awareness (SSA) capability
RESILIENT ARCHITECTURES IN SPACE	▶ New service architectures and implementation in space ▶ Overcoming single point of failure and failure-loss vulnerabilities ▶ Loss-coverage methodologies
INDIVIDUAL ASSET PROTECTION, INCIDENT REACTION AND RECOVERY	▶ Semi-autonomous reactive procedures, intuitive controller interfaces ▶ Attack/incident detection and verification methodologies and tools ▶ Improved hardening/immunisation of assets against known and emerging disruption possibilities (e.g. blinding, spoofing, etc.) ▶ Structure and implementation of autonomous/remote space repair capabilities

STOCKTAKING	▶ Research into security applications of future European space systems (GALILEO and KOPERNIKUS)
FUTURE AWARENESS	▶ Evaluation of applied (e.g. micro-satellites) and general technology trends regarding space infrastructure security

2.3.9 Protection from EMP and HPM Effects

Future civilian critical infrastructures will be exposed to deliberate attempts at disruption/destruction by non-nuclear EMP (electro-magnetic pulse) or HPM (high power microwave) means; limited effects capabilities are easily manufactured today. This not only means conventional and novel hardening, but also systemic resilience features as well as methodologies and instruments for detection and verification of attacks capabilities. With the danger being perceived as abstract at best, a thorough risk assessment and database on the costs of such attacks should be created, as this will strongly underpin the necessary legislative incentives and enforcements of such hardening measures. Therefore, a regulatory and organisational framework should be implemented that also provides methodologies and procedures, designates responsibilities and offers help to affected parties. Particularly security and emergency services should use hardened equipment wherever possible. While this refers to non-nuclear EMP/HPM effects, the same protective and mitigation means are required for effects originating in nuclear detonations.

All of these capabilities represent gaps today and in the near future. Civilian infrastructures have for the most part no hardening, shielding or redundancy features at all. There are neither regulations nor organisations in place, detection means are non-existent. No assessment or evaluation methodologies are readily available, and threat awareness is mostly missing. The topic is generally unknown and/or unaddressed which together with budgetary constraints present particular challenges for the future.

Research Needs: Protection from EMP and HPM effects

	RESEARCH NEEDS
RISK AND VULNERABILITY ASSESSMENT	▶ Risk and vulnerability assessment methodologies ▶ Effects awareness over the EMP/HPM-effects spectrum
EFFECTS PROTECTION	▶ Affordable and available, hardened equipment/elements
INCIDENT VERIFICATION	▶ Affordable, hardened and professionally available detectors ▶ Verification methodologies and reference centres
SYSTEMIC RESILIENCE	▶ Hardening/immunisation of cores and nodes, redundant architectures for commercial systems
REGULATORY FRAMEWORKS, METHODOLOGIES	▶ Coverage of legal aspects: statement of incident, liabilities, crime status, insurance commitments etc. ▶ Vulnerability and effects assessment methodologies ▶ Basic and enhanced verification, mitigation and recovery methodologies
INCIDENT RESPONSE AND RECOVERY	▶ Toolset for re-establishment of system functionalities in large events ▶ Integration of hardened and/or low-tech fallback controls
EDUCATION AND TRAINING	▶ Risk and vulnerabilities awareness of responders and the public

2.4 Priority Research Needs

While the results of the subgroups and panels hint at a plethora of specific solutions to defined capability requirements and gaps, the work of WG2 gave rise to some key solution characteristics which are crucial to future critical infrastructures security. Due to their systemic, cross-cutting and general nature, WG2 has coined them «meta-recommendations» – they transcend almost all other, more specific recommendations, and many such specific recommendations will have a reference to these meta-recommendations.

«Meta-recommendations»

1. **COORDINATION: Critical infrastructure security relevant research should be coordinated nationally and internationally and focused on whole-system characteristics for all stakeholders, including** governmental and non-governmental organisations (companies, associations, operators/end users etc.) and citizens. "Security Governance" requires integration of the vertical and horizontal facets of CI policy, programmes and stakeholders. The European Commission is uniquely positioned to facilitate the international aspects of the interplay between systemic and application research, making the most use of synergies and added value thus gained.

2. **SECURITY BY DESIGN: In line with the corresponding ESRIF Key Message, security must be placed at the heart of any critical infrastructure development programme.** Currently, security more often than not is a "bolt-on" function of a system, added only at later stages, potentially reducing the operational effectiveness of a given system. Thus, political action is required to promote the security characteristics being integrated into the initial design process if possible. Since safety and security overlap, the same should apply to safety by design, as has been the case in some areas for decades. In short, security considerations should be institutionalised in CI development programmes.

3. **TREND AWARENESS:** Critical infrastructures are dynamic. Their structural makeup, role, level of «criticality» and nature evolve constantly with the society that they serve. Therefore, securing critical infrastructures needs **constant monitoring and the evaluation of evolving threats, the emergence of new critical infrastructures and technological progress.** In order to keep that pace, critical infrastructures are in absolute need of **constant and rapidly implemented innovations on** a technological, organisational and procedural level.

4. **RESILIENCE:** Critical infrastructures, by their nature, can only be protected from harm up to a certain level, but beyond that, risks have to be taken. **Therefore, critical infrastructures protection research should place emphasis on risk management, including prediction, prevention, ensuring service continuity and rapid recovery in the event of an incident.** Security characteristics therefore should be designed to increase systemic and inherent resilience.

   Such security characteristics are neither novel nor obsolete: **redundancy, hardening, modularity, upgradeability, immunisation, networking and islanding, technical and procedural interoperability and lastly standards.** In three words, what critical infrastructures in Europe need is a **culture of resilience.**

5. **SOCIETAL EMBEDDEDNESS:** Due to their direct interfacing with people, **the perception and acceptance of security measures** as well as the **generation of user** trust in service delivery will become ever more important. We need transparency and reciprocal understanding in order to ensure that the security of critical infrastructures do their part in increasing societal resilience.

These «meta-recommendations» in and of themselves constitute very cogent, long-term solutions to the problem of security being treated only as a minor thought. The change in critical infrastructure operations paradigm – currently cost-efficiency in service provision and ease of handling – can only be overcome in the long term, and it is security research that constitutes one of a set of instruments (the others being regulatory action and economic incentives) to attain that goal.

2.5 Point of Focus: New Critical Infrastructures

Tying closely into both the identified challenge «Emergence of new critical infrastructures» and meta-recommendation Nr. 3 «Trends Awareness», WG2 recommends a continuous focus on two key dimensions of critical infrastructures, namely a) new or more broadly defined critical infrastructures and b) their vulnerabilities, developments and potentials. What is to be considered critical for the functioning of European societies should be indentified and protected as early as possible. This will require a broader definition of critical infrastructures than the one currently being used by WG experts.

In this broader definition, **WG2 advocates that the biodiversity of Europe be included into the usually more technical definition and scope of critical infrastructures.** Biodiversity is here defined as the variation of life forms in a given ecosystem, including both animal and plant life. Flora and fauna represent a basic resource that European citizens rely on for food, basic processing materials and recreational purposes. Plus, the complex interdependencies of ecosystems are increasingly understood, as is the delicate balance such systems constitute: The elimination, weakening or relative strengthening of an element can completely and irrevocably damage an ecosystem and have direct and indirect effects upon European citizens, none less so than in the marine environment. This, therefore, will require that the specific vulnerabilities and characteristics of the European biosphere be monitored and the security implications of any loss or any invasion by a foreign species understood. This will also include understanding and detecting the effects of illegal toxic and other dumping, externalities from marine exploitation including deepwater trawling, oil and gas industry, etc.

Secondly, Europe needs to **secure access to vital natural and mineral resources, or their substitutes and alternatives**, both within and beyond Europe. Just what these are is unclear, as are the ways and means to circumvent possible critical shortages by means of substitutes and alternatives. This warrants thorough evaluation in times when other global powers are buying up critical resources across the globe, particularly in Africa. By extension, this means that the **European Union should take stock of current and missing critical manufacturing capabilities.** This requires answering the question as to what is necessary (e.g. vaccines, aerospace, ICT components etc.), to what degree does it exist in Europe under European sovereignty and, lastly, where are critical dependencies. This plays into the necessary definition of the European security sector, and will logically have direct consequences for European and Member States' industrial policies. Due to the crucial nature of this endeavour, a separate body of experts charged with undertaking such a task should be envisaged.

Thirdly, **Europe needs a trends and future awareness entity,** tasked with monitoring societal, technological, political and environmental trends and developments. Whatever the organisational form, security needs to be an integral part of such a group. From the perspective of WG2, from the outset it would help to identify potential future critical infrastructures, threats to them and ways to counter them. Naturally, the definition and scope of critical infrastructures of both the European Commission and the Member States should evolve in light of such findings.

Fourthly, an understanding of the evolving security dimension associated with emerging significant offshore investment in offshore renewable and alternative energy production. The multibillion euro developments associated with wind, wave and tidal farms will require particularly novel security solutions if the infrastructure is to be protected and the energy supply to be guaranteed.

Lastly, and in line with the findings of WG4 «Crisis Management», emergency response forces at the regional, national and European level, their professionals, structure and equipment, should be considered as a critical societal and governmental infrastructure in a wider sense of the term. Naturally, this places strong requirements on their operational and technical interoperability, on joint capabilities and consistency in procedures. Indeed, in some cases, joint European crisis management forces could be envisaged.

2.6 Systemic Research Needs

Apart from the overarching and critical research needs advocated by WG2, there are numerous and often very specific recommendations to enhance the security of European citizens. Some go beyond the limits of Research and Innovation and enter the field of policy recommendations; it seems natural for each and every research and innovation agenda that takes itself

seriously to address the political environment in which it is set and will evolve. Additionally, some recommendations are of particular relevance, as they need repeated investment and research and their relevance will never change, barring cataclysmic changes in the functioning of European societies. These tasks are referred to as «eternal tasks». For ease of understanding, the specific recommendations are grouped by function.

2.6.1 Basic Understanding

- We are only beginning to understand the potential positive and negative effects of climate change, and one cannot say for sure what will happen when or where. But whatever the case, vitally important infrastructure must deliver the service intended. Therefore, systemic **research into effects of changes in climate on the integrity (e.g. in the case of biodiversity) and operations (e.g. in the case of agriculture and fisheries) of** critical infrastructures is needed, perhaps in cooperation with other environmental research areas in future Framework Programmes.
- Facilitation without compromising security: Research needs to be done into **better proactive, preventive methodologies** in a variety of fields. Methods to do this are user discrimination through better pre-service background checks, **better and commonly accepted risk, and vulnerability and impact assessment methodologies.** This is both general as well as specific (e.g. EMP/HPM assessment).

2.6.2 Systemic and Mission-oriented Architectures

- WG2 fully endorses the «Security by Design» key message of ESRIF: Especially critical infrastructures are in need of such an approach, since many infrastructures are spatially dispersed and widespread. Therefore, **security solutions need to be omnipresent and immersed throughout the critical infrastructures system itself.** Linked to one or several command and control centres, features such as health monitoring of elements, automatic area shut-offs and re-routings should be developed and researched where necessary.
- No critical infrastructure is an island, most are interdependent. **There are systemic/service interactions and interdependencies between many critical infrastructures** (e.g. power to ICT to transport) as well as purely technical ones (e.g. power to telecommunications). Research and developments in one area therefore naturally have a spill-over effect into other critical infrastructure areas which need to be taken into account. Standardisation and harmonisation are cutting both ways in this regard: They aid interoperability gains, but enable negative chaining/cascading as well. **Research should therefore both target this interaction specifically,** as well as be a transversal issue in specific, CI-relevant research projects, with the **aim of maximising synergies while minimising vulnerabilities and potentially negative effects.** Moreover, new research, such as modelling and simulation, should cover the **area of inter-CI domains including dependencies.** Currently, most research is infrastructure-domain specific.
- This interdependence and interrelation research must lead to an **overarching awareness of even secondary cascades, positive and negative feedback-loops, etc.** The next step after gaining this awareness must then be the **identification of robust approaches** and solutions that ideally affect several critical infrastructures at the same time. Apart from increasing resilience across the board, this might lead to more cost-effectiveness as well.
- In many cases, the division between security and safety is blurry to nonexistent (i.e. in power plants and in the maritime environment). Similarly, many stakeholders do not distinguish these in operationally meaningful ways. Synergies thus should be exploited at system design stages already, in line with meta recommendation 2 («security by design») in order to maximise efficiency and effectiveness.
- **We need to do research into security applications– and the security itself – of future Europe-wide infrastructures, such as GALILEO and COPERNICUS** (see chapter WG7 on applications). The potential use of these e.g. in the direction of localisation/tracing/tracking of goods on land and sea (mostly), coupled with integrity data etc. is huge. **Space assets are uniquely vulnerable to damaging effects, due to their complete loss in case of failure or** attack. Therefore, critical applications need to **be made resilient**, e.g. by spreading an application over a large number of satellites, thus enabling compensation if one satellite is lost. «Adaptive Space» is only one solution, and more need to be researched.
- It should be anticipated that in twenty years' time, Europe will still be an economic powerhouse exporting and importing goods and services to/from all over the world. With this in mind, WG2 believes that **worldwide security of maritime transportation of people and goods will remain of utmost importance. Therefore, research should be conducted going well beyond maritime border surveillance,** and towards establishing seamless, real-time, wide-area surveillance (of vessels and goods) and intervention measures. In addition to the technical aspects of maritime domain awareness,

enhanced research efforts need to focus on the importance of, and the attainment of, institutional integration as an essential pre-requisite for information fusion both within the state and between states.

- **Power generation, transmission and distribution systems, operated mostly by private market actors, need to be made more resilient, this will become even more important as offshore wind, wave and tidal resources are exploited.** While parts of this are a short term question (investment), research should be done into sensible and hardened interoperability schemes countering cascading and chaining effects while enabling rapid re-establishment of service provision («dynamic islanding», self-healing systems, etc.), dependency-diversification (more and smaller sites and sources) and determinants of economical feasibility. This is in line with the crucial importance of power supply for Crisis Management, as outlined by WG4.

Regulation/Legislation

- **Clearly defined areas of responsibility and better and more effective interaction and cooperation** are needed between private CI operators and public regulatory and law enforcement agencies, especially across borders. This refers particularly to regulatory frameworks, which need clear delineations (for operational crisis management conclusions, see chapter WG4; for law enforcement agencies, see chapter WG1).
- The domain of Critical Infrastructure Protection is a strong and nationally regulated market of public and private actors. Investment is, whether partially or sector dependent, driven by legislative requirements rather than market forces. This has two implications: a) That similar **regulations should harmoniously apply throughout Europe** in order to achieve and guarantee comparable preparedness levels within this framework, and b) that new **ways of incentivising innovation** need to be found.
- The importation of goods and services from non-EU countries requires policy and regulatory frameworks. It should protect local environments, populations and industries in the countries of origin from exploitation in the service of economic gain.

2.6.3 Sensors, Tracing and ID Management

- The **broad application of sensors** from wide area maritime surveillance to very local tracking of suspicious individuals or screening massive amounts of passengers/goods for CBRNE threats, are an absolute necessity in Europe's societies and **their continued improvement should be considered an ongoing requirement.** These capabilities need to be developed (where missing), improved upon (where they exist) and networked for validation/triangulation, thus providing crucial added value to security end-users and operators. In combination with high computation power, cognitive correlation methodologies and multi-sensor networks, this will provide very real added value to security end-users and operators (for specific implications, see chapter WG3, 4, 7 and 8).
- This directly affects the aspect of **identification/authentication and access/control rights.** We need better background checks for use throughout Europe, a concept of secure e-ID, trusted providers, better encryption, etc. The area of mass transportation of **people and goods will ever more be in need of contactless/standoff scanners that are reliable, fast and broad in scope.** This refers to the scanning of people (biometrics, identification, data mining, international cooperation in data provision, etc.) as well as **hazardous materials, non-metallic materials and especially CBRNE detection** (e.g. innovative use of Roman spectroscopy or LIDAR - Light Detection and Ranging). New technologies (e.g. terahertz technologies) need to be continually envisaged, developed and evaluated in line with our understanding of evolving threats; improved, tested and spiralled into security use. WG2 would also propose that a fundamental review of the current regulatory regimes in the aviation and maritime industries be undertaken and research carried out to determine the effectiveness of measures as well as the appropriateness of current and emerging technologies in this area. In the context of societal resilience, trust, security and society, it would be useful to determine what, if any, measures could be removed and under which circumstances (see WG 6, 8).
- Water and food supplies, as well as **agriculture, maritime and health infrastructures are particularly vulnerable to bio-agent contamination**, be it man-made (deliberate or accidental) or natural in origin. We need **fast, reliable and widely applicable biosensors**, constantly available reactive health services, pharmaceuticals and well established crisis management capabilities across environments. Communication and, in particular, the role of the media require much research in this key area (see also chapters WG4, 6, 11).
- Food supplies and agricultural systems need to be put on a resilient preventive footing. This requires good regulation and biosensors (mentioned above), but also **traceability and tamper-proof seals throughout the supply chain.**

2.6.4 Information Technologies and Communications

- As outlined before, the **computation power** (in terms of speed and bandwidth, e.g. improvement upon quantum computer technologies, etc.) **and methodology** (i.e. correlation capability) needs to be continuously enhanced. At the moment, correlation/data mining methodologies are unable to keep the pace of data generation, thus hampering the benefit of higher computation speeds. Making sense of vast amounts of data – and getting the result to security forces in the field - will be key to successful security policy in the future. Plus, these systems and the internet, need to be protected from illegitimate access to data (i.e. hacking, code-breaking) by means of continuously improved encryption, and will be required on an ongoing basis.
- **Special Emphasis in security related research should be placed on ICT security**. Especially in CI, ICT infrastructure represents a core tool for communications and management; sometimes the CI is dependent on ICT infrastructure itself (CII). Indeed, our societies will continue to be extremely dependent upon technologies and computers in particular, engendering vulnerability to ICT disruption/data theft/hijacking/spoofing, etc. Europe therefore needs to make ICT systems more secure (i.e. multilayered ICT security).
- **Secure and effective data mining and correlation methodologies and technologies** need to be developed. The exponentially increasing amount of data available, plus more detailed information as sensors improve, urgently requires this capability – which is a clear gap today. We need investment in secure, high-performance and high-integrity computing in order to attain this capability.
- With the flow of vast amounts of information that are ideally filtered, layered and accessible comes the requirement for **new man-machine interfaces** that enable intuitive, rapid access to data. What is needed are interfaces that either optimise existing access and interfacing methodologies or explore novel ways and means, i.e. more effective use of visual control, voice control or direct mind-machine interfaces. The range of applications for this is immense, from systemic control and monitoring functions to command and control of security forces to cyberspace intervention and action.
- **This ICT security related research needs to reflect the enormous speed of ICT product lifecycles:** The average today is five years and the speed is accelerating. Research into solutions and migration efforts therefore need to be equally fast, flexible, non-bureaucratic and exploratory where no obvious solution exists. This also refers to ICT threats, which are equally rapid in evolution and require similar speeds in countermeasures. **We need a culture of experimentation** and WG2 strongly recommends a concentrated effort to monitor and extrapolate ICT developments for their positive and negative effects.
- The majority of ICT hardware commonly available is manufactured outside of Europe. A deterioration of political relations could easily result in this flow stopping, or hitherto unknown hardware manipulations being used against Europe. While this is a case **example for a critical manufacturing capability, the importance of equipping security-essential systems with absolutely trusted hardware and software**, should not be underestimated.

2.6.5 Command and Control

- Security agencies across Europe will depend even more on **rapid command and communication technologies.** Current and near-future solutions are interoperable to a limited extent as their bandwidth is too low and they are neither hardened nor completely secure against software hacking. This will reflect on network hard- and soft-wired security, protocols and control overrides. **Secure, broadband professional mobile radio or software defined radio solutions of the next generation should be developed** (e.g. cognitive radio technologies).
- Both public and private CI operators need to be fully aware of the state of their systems at any point in time. Therefore, the more specific recommendations regarding sensors, tracing and communications means need to be **integrated into state of the art command and control systems that are linked to related and neighbouring systems and security services** (e.g. police, crisis management, etc). This calls for technological as well as procedural and regulatory harmonisation.
- To better protect space assets against any kind of space-borne threat (e.g. space debris, ASAT threats, etc.), **a dedicated European Space Situational Awareness (SSA) capability should be developed.** This not only entails developing awareness, but also enhancing controlled and autonomous evasion capabilities. Since this requirement would surpass most national capabilities, a real European added value can be achieved.
- The importance of the attainment of institutional integration within states and between states as a prerequisite for functional command and control demands security research into its political and societal aspects.

2.6.6 Intervention

- **The evolution of CI and corresponding risks will partially affect response forces. In the case of physical CI, response forces** and their linkages mostly exist already. **In the case of ICT, intervention forces are rudimentary at best and security relies on soft- and hardware barriers.** The limits of these «static» lines of defence are evident and necessitate new solutions which warrant both basic as well as applied research into these counter-hacking/-spoofing strategies, methodologies and instruments.

2.6.7 Education and Training

- Given the importance of trust for CI security and operations and the knowledge that trust is generated by transparency and understanding, **preventive education and response training should expand not only to security experts and CI operators, but also to customers and the public at large** (for crisis situation training, see WG4 chapter). The theoretical and practical consequences of empowering European citizens as security stakeholders need foundation level as well as detailed, programmatic research.

2.6.8 Societal Embeddedness

- Critical infrastructures, perhaps more so than any other infrastructure, are **vulnerable to insider threats,** namely from personnel and third party individuals with access rights to certain key components that have radicalised and intend to use their know-how for adverse effects. **We therefore need more knowledge about radicalisation processes,** how to detect them and how to prevent resulting security breaches.

2.7 Conclusions

Security in the future remains a careful and very specific act of balancing prevention, protection and reaction/mitigation. In some cases, prevention and protection must be emphasised since the consequences of failure would be too dire to accept. In other cases, where prevention and protection are too difficult to implement, the emphasis must be on reactive mitigation of effects, that is, service must be delivered. In both cases, European critical infrastructures[1] that cross international borders need a higher level of resilience. If ESRIF advocates a «Culture of Resilience» that is understood to be comprehensive, then this is the result of realism and pragmatism: Crises will occur. Terrorists will exist and strike. Europe will experience floods, storms, droughts and epidemics.

If the work of ESRIF WG2 «Security of Critical Infrastructure» were to be broken down into a few words for national governments, they would be «prepare yourselves to ensure that nothing can completely put your system out of service». This is why WG2 strongly advocates the concept of resilience: That despite changes in assumptions, measures put in place will be effective (e.g. what helps against bioterrorist release of agents can very well help against a natural pandemic), power and water will be running to an acceptable standard (e.g. water will be potable), and basic communication will work effectively. Societal resilience is heavily dependent upon certain vital consumables and services being in place, and this is the contribution of WG2 «Security of Critical Infrastructures» to the endorsed concept of «societal resilience».

In the final analysis the security of critical infrastructure requires as full an appreciation of the potential impact of "negative externalities" as possible. Whether these are deliberate or accidentally generated, strategies, while ideally aiming to prevent the impacts, must also focus on mitigating the effects.

1 European critical infrastructure or 'ECI' refers to critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. EU COM(2008)114

3. Working Group: Border Security

3.1 Introduction

The objectives of border management are to prevent illicit cross border activities, while facilitating legitimate movements of persons and goods. According to the Schengen Borders Code, border control comprises checks on persons at border crossing points and surveillance between these border crossing points, as well as an analysis of the risks for internal security and analysis of the threats that may affect the security of the external borders of the European Union.

All studied scenarios show that in the long-term perspective, the task of border management to facilitate legitimate border crossings, while detecting and preventing illicit activities, will remain a critical capability, given the expected rising cross-border flows of people and goods.

Border control is likely to face increasing demands for efficiency, which implies a need for technical systems that are user-friendly and reliable in operational conditions. A general challenge is also to make the technical equipment affordable enough to be widely employed.

A further general challenge that applies to all scenarios is interoperability. Europe is developing a policy on Integrated Border Management that calls for integration between different national authorities related to border security, between the Member States, and finally between the Member States and neighbouring third countries.

These measures call for improved interoperability and standards, operational as well as technical, between the different units. The interoperability challenge concerns many technical systems, including communications and information systems.

In all situations, border guards will need capabilities to collect intelligence and produce a common situational picture to identify threats and carry out operations.

Required capabilities for border guards largely depend upon the operating environment. For this reason, WG3 activities were carried out by four task groups covering Border Checks and Land, Maritime, and Air Border Surveillance.

3.2 Threats, risks and challenges

Legitimate border crossings take place at border crossing points on land or at airports and seaports. Crossings of the land and maritime borders outside of the border crossing points should be detected and prevented.

Naturally, the threats, risks and challenges faced vary depending on the environment. Furthermore, the threats and risks constantly evolve, as criminal organisations adapt to the development of border control procedures and technologies. It can be assumed that some organised criminals have enough resources to deploy countermeasures to some border control systems.

In terms of future threats and scenarios, while the threat from terrorists might increase in scenarios with an increased level of conflict, other likely challenges depend more on economic conditions. Growing populations in the European neighbourhood, together with limited improvement in living conditions are likely to create a strong driver for illegal migration.

Under certain scenarios, Europe might face a humanitarian crisis at its external borders as a result of war or major disruptions in neighbouring areas. These situations, even if with low probability of occurrence, will require border guards to cooperate with other national authorities, possibly including the armed forces and humanitarian organizations, in order to provide support to persons in need of international protection, whilst maintaining control of the flow of people crossing the external border.

In the long term, the opportunities for organised crime might differ according to the character of the prevailing scenario. A more open and integrated global economy might offer new opportunities also for organised crime groups, while increased security measures might restrict them.

Border Checks at border crossing points

The challenges relevant to border checks at border crossing points are primarily to prohibit unwanted activities, while facilitating the large volume of legitimate border crossings. The challenges are mainly of the following types:

- People hidden in vehicles or in cargo
- People seeking access on the basis of false identity or false documents
- Overstayers
- People carrying infectious diseases

Closely linked to border control is customs control, which aims at the detection and prevention of illicit goods and substances. This category comprises, inter alia, weapons, drugs, CBRNE hazards, legal goods that are subject to duty, goods subject to import or export restrictions (e.g. antiquities, ivory, hard wood, and strategic products) and goods that fail to meet health and safety standards.

A common challenge for customs and border control authorities is to accommodate the ever-increasing flow of cargo and people crossing the external borders of the EU, without undue delay or with minimal intrusion, employing affordable technical and human resources.

External land borders

Whereas vehicles are normally employed for transport up to the border area, actual illegal border crossings take place on foot, seeking to exploit difficult terrain and poor visibility to avoid detection.

External maritime borders

The threats relevant to the maritime environment are primarily of two types:

- Risks and threats related to safety (which may have dramatic environmental and socio-economic consequences)
- Risks and threats related to security (unlawful activities: trafficking in human beings and narcotics, illegal migration, terrorism, piracy, etc.)

Many of the security threats involve the use of small craft, rubber boats, or even semi-submersibles. The challenge here is to detect and track these small objects and to distinguish them as possible threats..

Other maritime security threats involve illicit activities under the cover of regular shipping activity (e.g. on board of merchant and ferry vessels). Illegal migrants or illicit goods can be hidden amongst the cargo and can then be dispersed en route or when arriving at seaports.

Airspace

So far, the European Union has not yet seen aerial security threats to any significant extent. However, in other countries aircraft are commonly used for drug smuggling and other illegal activities. Security threats coming from the air could include:

- Low flying aircraft (general aviation)
- Renegade (rogue) aircraft
- Gliders
- LAVs (Lighter than Air Vehicles)
- UAVs (Unmanned Aerial Vehicles)

The above mentioned tools could be used as, or for:

- Weapons (e.g. September 11 attacks)
- Smuggling of illicit goods
- Illegal migration

As in the maritime case, a major challenge is to distinguish threats from regular activities and to organise the technical, operational and regulatory systems for the effective use of surveillance and patrolling assets.

3.3 Capabilities and Gaps

The threats, risks and challenges listed above result in requirements for a broad range of capabilities. Some of the most crucial and general capabilities are:

1. **Capabilities to manage increasing flows of people and goods**
2. **Capabilities to ensure surveillance, monitoring, detection (especially of abnormal behaviour), identification, tracking and interception**
3. **Capabilities to ensure interoperability and information-sharing (classified and unclassified) to increase response capabilities**

The requirement for interoperability is to a large extent driven by the lifting of internal border controls in the Schengen area, which makes external border control an issue of common interest at EU level, requiring close cooperation and coordination between different Member States and different organisations. Interoperability covers:

- interoperability of equipment and systems
- interoperability of communications
- interoperability of information and intelligence shared at national and EU level, including the «pre-frontier area»

These three levels of interoperability are necessary for efficient cooperation at EU level. However, currently interoperability is limited by:

- Lack of harmonised doctrines, concepts, operations, standards, agreements and governance structures
- Lack of a common language
- Different systems in service reduce mobility or drive training requirements
- Diverse format of information makes sharing difficult

The lack of interoperability is the result of several factors, e.g.:

1. **The plethora of agencies involved in border control, sometimes resulting in overlapping powers;**
2. **Uncoordinated approaches by different sectors, in particular in the maritime domain, often hindering effective exchange of information;**
3. **Reluctance to share intelligence between different sectors.**

There are several gaps which limit the affordability of many technical solutions e.g.:

- High initial acquisition costs leading to scarce or no availability
- High cost of ownership often determined by poor reliability
- Expensive infrastructure or communication networks required for remote operation
- Complex systems forcing high training costs
- No standardised equipment

The challenge to perform threat assessments requires:

- Improving exchange of information and intelligence between different law enforcement agencies within a Member State and between law enforcement agencies across Member States (overcoming sensitivities around intelligence sharing, protection of sources etc.)
- Improving processes to increase time available for border control authorities to prevent an identified threat without delaying traffic
- Creating a system of threat assessments that is shared in close-to-real time between the authorities involved in border security within a Member State as well as between border guards of different Member States and that can be kept up-to-date
- Creating feedback loops from border patrols to the threat assessors

Border Checks

The following classes of capabilities should be properly addressed:

- Capabilities to face rising volume of traffic of people and goods
- Capabilities to detect illicit substances and concealed people
- Capabilities to identify people and assets
- Capabilities to process information, including issues of interoperability and situational awareness
- Capabilities to perform threat assessments and profiling, including information sharing and learning systems

The challenge of facing the rising volume of traffic of people and goods requires capabilities for:

- Higher speeds of detection, identification, information processing and threat assessment of border check processes
- Positive profiling of low-risk frequent travellers
- Flexible, upgradeable (mobile) solutions
- User-friendly and affordable systems
- Automation of border control
- Incorporating a stand-off capability
- Harmonised standards in security and mobility chains (linked to customs control)
- Stakeholder management to create a secure supply chain (linked to customs control)
- Dealing with increased technical skills among groups that pose threats

The challenge of detecting concealed people and illicit substances requires mainly technological capabilities for achieving:

- Higher resolution of images
- Better identification of elemental, molecular, or biological composition (in order of increasing complexity) of the material
- Higher detection rates with a low false alarm rate and at higher speed (especially nuclear)
- Higher rates of detection, identification and defusing of explosive devices

There may be opportunities for improved processes e.g. at seaports (or) using transit time to increase scan time, but there are still a number of organisational and legal barriers to gain agreement on such processes with multiple seaports, countries, stakeholders etc.

The challenge of identifying people and assets requires:

- Means to assess the validity of travel documents
- Means to identify overstayers
- Methods and technologies to detect spoofing of biometric features. This holds especially for fingerprints.
- Standardisation and certification of equipment
- Mobile devices and high-speed wireless connections for ID checking (including biometrics) in buses, trains, etc.

Surveillance of External Land Borders

A permanent surveillance of all parts of the external land border is neither needed nor politically desirable. Border surveillance should thus be based on risk analysis and intelligence. This means that the focus for the surveillance of the external land borders is on border patrols using mobile equipment, while only selected parts of the land border should be surveyed by stationary systems.

There is currently a multitude of technical solutions for land border surveillance. However, the practical use of these systems is hampered by cost, reliability and interoperability. One of the main challenges identified is that the systems currently available are far too expensive. Furthermore, affordability and interoperability will therefore be key issues when developing the requirements for the necessary equipment, systems, doctrines, processes and standards to enhance land border security systems.

Such systems will have to work on a 24/7 basis and must be able, with a low false alarm rate, to send an early warning to command systems. Furthermore those systems will have to be easy to use for Border Guards with support & services adapted to the end-user requirements.

The chosen system should be adaptable and could be composed of different types of remote surveillance equipment such as fixed unattended ground sensors, or sensors placed on unmanned platforms (ground or aerial). Certain components could operate, at least partially, autonomously. Furthermore, extreme weather conditions would have to be taken into account.

Secure communication systems should be able to exchange all types of information (voice, data and video) at a rate that is compatible with the urgency of the different situations faced. Furthermore, tools for decision support should be available to Border Guards, integrating criminal intelligence (lessons learned) gathered by all stakeholders.

Surveillance of Maritime External Borders

The main overall challenges to ensuring interoperability and information sharing in the maritime domain are:

- Coordination and integration of different national authorities involved in maritime (border) surveillance at national and EU level
- Cooperation with neighbouring third countries

These two overarching challenges require capabilities and standards to be developed on a technical level as well as on tactical, operational and strategic levels.

More specifically, interoperability for maritime border surveillance requires specific capabilities for each of the following (in order of importance):

- Communications
- Common situational picture
- Information management (protocols)
- Operational processes

Currently, there are a series of shortfalls with regard to the security in the maritime domain:

- Open sea: partial coverage, no continuous and persistent surveillance
- Coastal waters: gaps in small targets detection
- Member State costal surveillance systems: adjacent, non integrated, limited coordination and information sharing
- Legal frameworks: limitation on interventions
- Fragmentation of involved organisations
- Limited interoperability between sectoral stakeholders and systems
- No common situational picture
- Lack of early warning and documented alarms
- Lack of cooperation with neighbouring third countries
- Delays in search and rescue operations (SAR)

These shortcomings result in:

- Loss of human life related to trafficking in human beings and illegal migration activities by sea
- Unlawful and criminal activities, organised crime at sea
- Limited global cost-effectiveness

The current capabilities concerning maritime interoperability and information-sharing present the following gaps:

- **Communications**
  - Limited interoperability inside and between countries, not because of lack of communication channels, but mainly because (1) no data exchange practices are performed between actors and (2) concerns about information ownership
  - In many Member States, the absence of a single "National Coordination Centre for Border Control/Surveillance" hampers interconnecting the different national authorities
- **Common situational pictures and dissemination tools**
  - Operational situational pictures fusing all available and relevant information are not produced in real time
  - Multi-sensor fusion is limited though various sensor solutions are implemented (including space-based sensors)
  - Multi information sources fusion (data bases, intelligence etc.) within the already existing situational picture is limited

Furthermore the various actors have different scopes and methods with regard to:

- Mandates and legal remits
- Methods of operation
- Theatre-related threats and priorities
- Access rights to information

Maritime surveillance requires specific capabilities for each of the following (in sequence):

- Monitoring
- Detection
- Identification
- Tracking
- Mission planning

Surveillance of airspace

The current capabilities in order to ensure detection of aircraft flying low and slow have several gaps. Those of higher priority are:

- **Situational picture**
  - Data mining on different databases
- **Detection**
  - Air Defence and Air Traffic Control radars have poor coverage at low altitudes, experience strong clutter at low altitude and are subject to terrain masking
- **Identification and tracking**
  - Current systems use basic identification and tracking algorithms, the results are not always available or reliable
- **Information processing (including for Interoperability and Situational Awareness)**
  - Air Defence/Air Traffic Control interoperability available only in few countries
  - Cross border interoperability not always possible
- **Systems and services**
  - Current Air Defence & National Air Traffic Control or Air Traffic Management systems have high overall costs. In some areas they are redundant, while in others there are holes in the coverage

Detection and management of renegade aircraft alerts is an area where NATO and Eurocontrol are currently collaborating. Technology demonstrators have been developed, like ERRIDS – European Regional RENEGADE Information Dissemination System and CIMACT – Civil/Military ATM/Air Defence Co-ordination Tool. However, much needs still to be done in order to bring all EU Member States up to the same level and ensure cross-border collaboration mechanisms.

3.4 Solutions

The key areas of interoperability and affordability can both be addressed to some extent through harmonisation and standardisation.

One way to address these issues is to invest in research and development with a focus on affordability, to effect an order of magnitude cost reduction in many surveillance equipment. Another solution is to utilize technology from adjacent markets such as mobile telecommunications where the volumes of production are very high, thus keeping the cost of processing down to a minimum. Harmonisation of requirements and standardisation across Member States would themselves automatically also greatly improve affordability.

Inefficient procurement processes lead to delays and higher acquisition costs. The EU as well as the Members States could improve their procurement processes by involving technical experts in the requirement specification and acquisition processes. Such technical experts, who of course have to be fully independent of the solutions providers, will advise on the best balance between the specifications/requirements of end-users and the technical performance of the solutions provided by the suppliers. Standardisation may be able to play a part in reducing such costs where equipment is required to be EU Security-approved, thus facilitating a quicker selection process.

In general, interoperability will require governance and standards to be agreed within Member States, among Member States and with third countries. A series of border control-relevant systems will be put in place or upgraded in the near future. To be interoperable there must be significant research into interface layers and common data models that will allow this diversity of systems to be truly interoperable.

Border Checks (including aspects of customs control)

Effective and efficient border checks of people and goods require a broad range of solutions. Some devices are better for checking people, others for cargo etc. A combination would bring considerable benefits, such as improved accuracy.

CBRNE detection is not yet satisfactory (e.g. the challenge of explosives as liquids). In particular, early warning systems with real-time monitoring are not yet available, and there is a need for solutions to be more affordable, flexible, reliable and user-friendly.

Identification of pathogens is at present not fast enough (requires growing a culture) or not sufficiently specific to detect dangerous substances with low false alarm rates.

Radioactive and Nuclear detection are advanced. NMR (nuclear-magnetic–resonance) is in operation to detect certain types of explosives, but the process is slow and is far from becoming a real-time system. Explosive detection technology is still under research using spectroscopic (terahertz, laser) and image methods and is not yet a technologically reliable. Stand-off detection capability is highly desirable.

Neutron radiography represents a very promising technology in the medium to long term. It is suitable for producing high quality images and can be used to detect elemental composition. In collaboration with gamma ray scanning it can produce good results.

X-ray scanners are in use to screen the content of a container detecting objects and people. The detection process is very slow and may be hazardous for humans inside the container. The challenge here is to reduce the screening time and to improve the image.

Terahertz technology is under research for screening at checkpoints to detect explosives and weapons or substances hidden under the clothes of persons.

Active Millimetre Wave Scanning technology for personal screening is in the testing phase at a few airports, but could face problems with passenger acceptance. Passive Millimetre Wave Scanning potentially resolves that issue but is still in the research phase.

Screening or Filtering has an important role to play – e.g. applying tests, intelligence or route tracking deviations to filter out items requiring further scanning or investigation.

The ability to automatically detect document forgeries needs further improvement: the computer aided analysis of IRU/V/visual images produced by document readers needs to be far more reliable, faster and flexible. It should be possible to configure "matching rules" for each document type specifically to check only what needs to be checked. It should be possible to configure new matching rules for newly found "regions of interest" in a certain document type, though this would require reliable, secure and timely communication with issuing authorities.

Video surveillance in security areas is usually almost fully-fledged. The ability to discern individuals in a crowd and track their paths would help aviation security as well as, for example, the identification of asylum seekers claiming to have lost their documents.

Systems for automated assessment of deviant behaviours might also be developed.

Systems for automated border control are already well-advanced in some Member States, usually at high-passenger volume airports, but need to be further developed in order to make border checks even more effective and cost-efficient.

The challenge of processing information, including the aspects of interoperability and situational awareness requires:

- Integrating outputs from multiple devices in order to create efficient data fusion
- Automatic screening, filtering and interpretation
- Combining human intervention with automatic processing
- Interoperability of equipment in automated processes
- Interoperability of information when using different languages

Surveillance of Maritime External Borders

A more integrated approach to maritime surveillance would help in mitigating current shortcomings by ensuring interoperability and information-sharing, an increased rate of detection, and identification of small craft and anomalies at sea. By sharing relevant information between the different sectors at Member State and EU level, which has to be done in full compliance with sovereign prerogatives of the Member States and information ownership requirements, a common information-sharing environment could improve the situational awareness of activities in the EU maritime domain.

Current capabilities in regard to detection, identification and tracking of small craft as well as detection of anomalies at sea have the following shortfalls:

- **Intelligence**
  - Data mining on a limited number of data bases
- **Satellite Earth Observation (EO) services**
  - Their use is not widespread. They are not tuned for these types of services and they have limited revisit rates
- **Platforms**
  - Limited availability and high costs of manned airborne and seaborne patrols for permanent surveillance
  - Surveillance networks and ship reporting systems could be better correlated to detect anomalies and identify threats
- **Information processing**
  - Databases
  - Integrated communications
  - Capability to access data bases

Maritime border surveillance is mainly characterised by:

- Extensive maritime areas, largely unmonitored in EEZs and beyond;
- A broad variety of adjacent activity sectors related to maritime surveillance (i.e. defence, transport, maritime safety, protection of marine environment and resources, fisheries control, customs, etc.) concerning both legitimate and unlawful activities.
- A large number of involved stakeholders who range from national and regional authorities (civil and military) to European and multinational agencies.

In this complex and multifaceted context there is a need to exchange information in order to benefit from monitoring capabilities of adjacent sectors (see above listed sectors) and meet the security challenges. This calls for developing a technical framework leading to a common information-sharing environment for the EU maritime domain, which allows authorities involved in border surveillance activities to considerably improve their situational awareness and increase their reaction capability both at national and EU levels.

This could be seen in context with:

- Pooling and sharing maritime surveillance assets currently available and expected to be available in the mid and long term (UAVs, new technology radars, wide swath satellites, etc.).
- Maintain situational awareness of activities (legitimate and unlawful) developing on the high seas, coastal waters and ports;
- Deliver operational security services (e.g. broadband satellite communications, tracking of ships, satellites, AIS service providing, e-services (e-customs) etc.).

Future solutions to address the challenges of interoperability are specific to each of the following areas:

- Communications
- At sea, broadband internet-like access gained from space and ground networks

- Guaranteed data networks with adaptive bandwidth (generation of common and user-defined situational pictures does not require high bandwidth in contrast to the transmission of real-time imagery)

▶ **Generation of common and user-defined situational pictures and their dissemination**

- Better organisation of user-defined situational pictures from fusion and streamlining of heterogeneous information sources (originating from passive and active underwater, surface, coastal, airborne, space-based sensors) such as AIS, LRIT, VMS (fisheries control), conventional and new technology radars, optical cameras, etc. The challenges are mainly the capability to streamline, disseminate and display useful information in an organised and meaningful manner.
- Exchange of alarms and threat identification reports on suspicious events at national and EU level

▶ **Platforms**

- New generation of all-weather surveillance tools for all types of traffic from the coastline to EEZs (200 nautical miles) and beyond
- Co-location of sensors: AIS, conventional and advanced radars, optical and IR cameras, active and passive underwater sensors

▶ **Operational processes**

- Harmonisation of processes and doctrines; development of operational standards
- Development of joint/cross-sectoral maritime operations

The future solutions to address the detection of small craft and the detection/investigation of anomalies at sea are specific to each of the following areas:

▶ **Detection**

- Coastal based high performance radars (e.g. HFSW, FMCW), airborne radars, remote sensing satellites with high resolution scanning sensors (imagery) and new technology space-borne radars, active and passive underwater sensors, ESM capabilities (including GSM) and optical cameras
- Anti-sea-clutter processing

▶ **Identification**

- Advanced correlation of information processes (AIS, LRIT, space imagery, radar, etc.)
- Radar tracks and electro-optic images correlation
- Advanced satellite/UAV images recognition
- Advanced ISAR techniques applied to long range radars
- Smart floating sensors
- Advanced processing of vessel tracks to detect abnormal behaviour
- VHF and satellite repeated AIS constellation

▶ **Intelligence**

- Network accessibility down to the sensor level
- Second generation of earth observation system (EOS)
- Generation of common and user-defined situational pictures to benefit all users (specific information can be added to the common picture depending on the type of user)

▶ **Mission planning**

- Automatic mission planning optimisation tools

Surveillance of Airspace

The future solutions to address the challenges of detecting aircraft flying low and slow are specific to each of the following areas:

▶ **Intelligence picture**

- Regulated but readily available access to sensitive information across national services and across border agencies

▶ **Detection**

- New and better performing sensors (land, air, space-borne)
- Multiple sensor fusion

▶ **Identification**

- Tracking algorithms benefiting from advanced integration of satellite image recognition
- Equipping lighter and smaller aircraft with low cost Secondary Surveillance Radar (SSR) transponders and making data available to national services other than ATC

▶ **Information processing (including Interoperability and Situation Awareness)**

- Improved information sharing and interoperability procedures and standards (between civil and military authorities)

- **Systems and services**
  - Advanced Integrated Safety and Security Systems and services using future platform capabilities (Airborne, Satellite)

3.5 Priorities

As a result of the analysis of threats, risks, challenges, capabilities, gaps and solutions, the following topics should become the priorities of the EU:

- More cost-effective standardized equipment (at EU level)
- High degree of interoperability
- High degree of intelligence-sharing
- Cost effective and reliable communication systems which will relay both data and voice

The development of interoperability requires further analysis of its scope and the levels at which it should be applied (ranging from between agencies within a Member State, between neighbouring Member States, between Member States and their neighbouring third countries and between all member states and a centralised agency). Information-sharing forms a large part of interoperability.

The scope and the scale of the technologies needed to address the challenges outlined here raise the question of affordability. Research investment as well as dual-use type of equipment could reduce that cost. Affordability also covers the cost of ownership. Equipment must become significantly more reliable, cheaper to maintain and easier to use in order to reduce training costs.

Research is needed in fusion of information. This concerns both sensor fusion and fusion of intelligence information with sensor information used to detect anomalous behaviour and possible threats.

To improve the identification of possible threats - imminent as well as more long-term -increased interdisciplinary research on understanding and detecting specific human behaviours is needed.

More detailed priorities related to border checks include:

- Detection technologies, including technologies to detect dangerous liquids
- Biometrics and automated border control systems

The priorities identified as future "must have" capabilities with regard to maritime border surveillance are:

- **Common information-sharing environment**
  - Definition of the overarching guidelines and principles to develop a common information sharing environment for the EU maritime domain
- **Communications**
  - Broadband communications and internet-like access at sea
  - Definition of information exchange requirements (e.g. interfaces) between organisations in compliance with information ownership
- **Common and end-user defined situational pictures and dissemination tools**
  - Generation of situational pictures from near-real-time fusion of heterogeneous sources
  - Selective dissemination of large amounts of heterogeneous data and information
  - High interoperability in fusing and analysing data enriched by actors
  - Validation of information and cross-correlation of different sources
  - Application of software agents for automatic data mining

The priorities identified as future "must have" capabilities for ensuring the detection of small craft and detection/investigation of anomalies at sea are:

- **Detection**
  - Improvement of sensor performance (new technology radars, space-based sensors, etc.)
  - Integration of assets on platforms

- Combination of assets (coastal, ship borne, airborne, space-based)

▶ **Identification**
- Advanced integration of satellite and UAV image recognition
- Advanced ISAR techniques applied to long range radars
- Improvement of electro-optics solutions
- Validation of information (including correlation of different sources)

▶ **Intelligence**
- Better use of COMINT (COMmunication INTelligence) / ELINT (ELectronic INTelligence) capabilities
- Reasonable access to sensitive information

▶ **Certification allowing the use of UAVs in civil airspace**

The priorities identified as future "must have" capabilities to ensure detection of aircraft flying low and slow, concern development and testing activities in the following areas:

▶ **Intelligence picture**
- Sensors and systems should be integrated in a network based on specific Service Level Agreements (SLA)
- Use of imagery from second generation earth observation satellites
- Generation of a situational picture useful to all organisations (specific information can be added upon the generic picture depending on the type of user)

▶ **Detection**
- Low cost/ high performance sensors (land, air, space based) such as mobile, small, active and passive multi-static radars to be used as gap fillers to ATC/Air Defence coverage
- Dedicated and improved land and sea clutter processing

▶ **Identification**
- Advanced aircraft identification and tracking algorithms
- Distribution mechanism to multiple users of aircraft identification data coming from Secondary Radar Transponders

▶ **Information processing (including Interoperability and Situational Awareness)**
- Integration of Data coming from multiple sensors (Land, Air, Satellite) and distribution to multiple users with a need to know

▶ **Systems and services**
- Integrated Safety and Security Systems and services using future platform capabilities

3.6 Conclusions

In summary, WG3 identified seven major mid/long term challenges:
- Unlawful movement of persons and goods at border crossing points
- People seeking access on the basis of false identity/documents
- Detection of aircraft flying low and slow
- Affordable and user friendly equipment for Border Guards
- Interoperability
- Detection, identification and tracking of small craft at sea
- Detection/Investigation of anomalies at sea

These challenges have resulted in the following main capabilities to be acquired by border guards in Europe:
- Capability to face increasing flows of persons and goods.
- Interoperability and information sharing: data models, information exchange requirements, procedures to maximize Situational Awareness at all levels, between agencies within a Member State, between neighbouring Member States, within the EU and with neighbouring third countries. Information sharing should include also Pre-Frontier Intelligence.
- Affordability:
  - Research is required to achieve an order of magnitude cost reduction enabling large scale deployment.
  - Lower cost of ownership (reliability, easy to maintain and use).
- Social science research is required for understanding and modelling of threats.

4. Working Group: Crisis Management

4.1 Introduction

Crisis Management (CM) is a core capability of modern societies. Managing the return to normal life in case of major incidents as quickly and swiftly as possible is paramount for limiting damage, chaos, and panic. It becomes even more important as an unshaken focussed leadership supports citizens in upholding their spirits and enables them to contribute to the recovery effort.

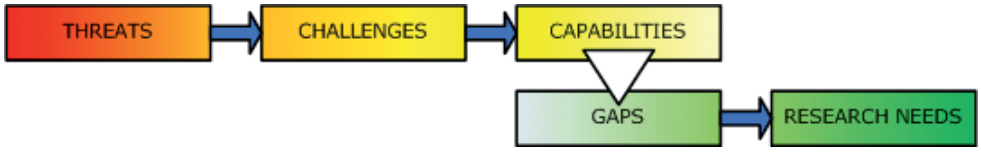
Crisis Management is a multidimensional discipline. It is typically regarded as a complex incorporating both the managerial aspect of organising the mission and the technical facilities employed to assist. This mixture becomes more intricate as Crisis Management evolves along the phases of a crisis, addressing pre-incident phases as well as post-incident phases (cf. picture 2).

Crisis Management principles are independent from the type of incident. Every incident has its specifics and requires specialised instrumentation, but from the management perspective all missions operate similar processes. However, crisis situations have a tendency to become more remote, more dynamic and cover an increasing geographical area. These elements, together with the resulting necessity to inter-operate in a multi-national set of multiple organisations including the affected public generate new challenges for the management element of CM.

On the technical side a number of new technologies heavily increase the potential situational awareness. New sensors allow a more accurate classification of a situation, and information management infrastructures foster the compilation of a growing amount of information at command and control, requiring new forms of display and interaction.

4.1.1 Crisis Management in the context of ESRIF

ESRIF aims to identify research needs. Threats and risks are positioned at the beginning of the analysis. Withstanding a risk that materialises in a crisis situation incorporates challenges of a different nature. In dealing with the challenges certain capabilities need to be present. Any gap in this set of capabilities requires investigations and research in order to close the gap.



Picture 1: ESRIF methodology of work

Driven by the "prepared to react" maxim as part of the ESRIF working arrangement, Working Group 4 focussed on the specific analysis of the needs and the deficiencies within the "response" and "recovery" phase in man made and natural/technical catastrophes. It is evident though, that preparedness aspects of training and exercises need to gain importance in particular with wide integration of the public.

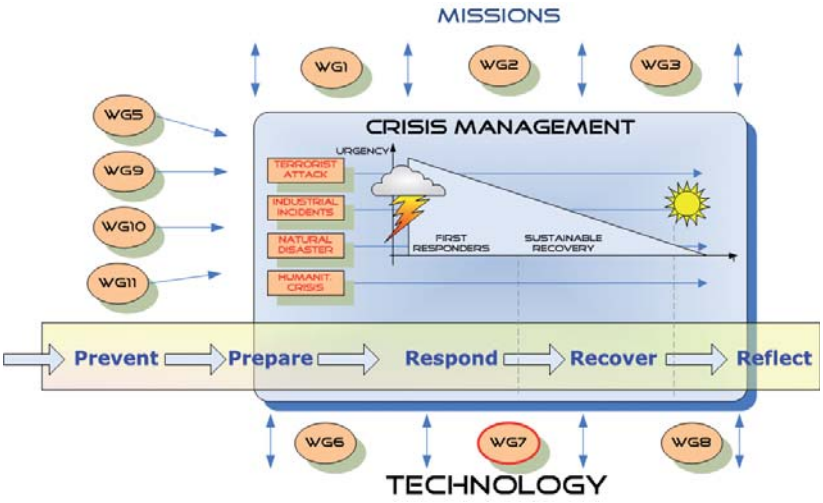
CRISIS MANAGEMENT ASPECTS ELABORATED WITHIN WG4 ELEMENTS	
CRISIS MANAGEMENT PROCESSES	Co-operation, information models, improvement of the effectiveness of CM procedures and processes
REMOTE CRISIS MANAGEMENT	EU external Crisis Management
INTEGRATED EARLY WARNING AND EMERGENCY RESPONSE	From preparedness, prevention and alerting to response and recovery
ROLE OF THE PUBLIC	Communication with the public through all relevant communication lines; Recovery Support
CIVIL-MILITARY COOPERATION (CIMIC)	Including civil-military emergency planning, other forms of cooperation and interoperability
INTERVENTION TRAINING	Training and simulation, computer assisted exercises for Crisis and Emergency Management
INTEROPERABILITY	Communications, semantics, processes
HUMAN FACTORS IN DECISION MAKING	Provisioning of information and data

Table 1: Scope of work for WG4

Technology substantially influences Crises Management in opening new sources of information (e.g. by advanced sensor systems) and exchanging information in near real-time. However, Crisis Management is regarded as a management process with decision makers in the centre rather than a technical undertaking. Technology is a factor enabling novel management approaches and supporting the decision making processes.

As a management process Crisis Management is a tool that applies to different missions (in ESRIF represented by WG1-WG3) using different technology (represented by WG6-WG8).

It furthermore operates in a specific context which is defined by WG5 and WG9-WG11, cf. picture 2.



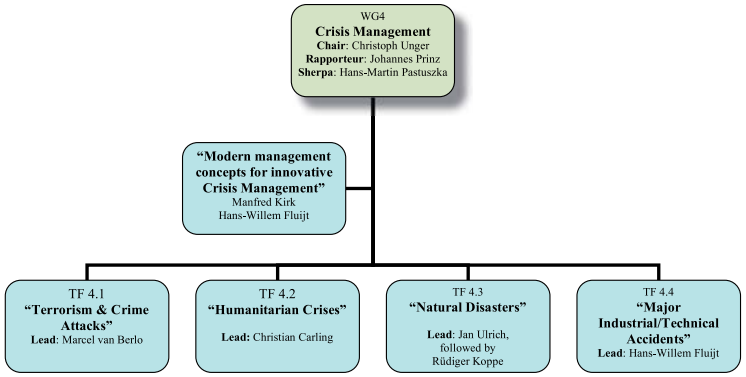
Picture 2: Crisis Management in the context of the other ESRIF WGs

4.1.2 Work organisation

In order to assess the impact of certain crisis categories on Crisis Management, four tasks forces were established. The result of the initial analysis of relevant security policy papers suggested arranging the work along the following four main risk scenarios:

- "Terrorism & Crime Attacks"
- "Humanitarian Crises"
- "Natural Disasters"
- "Major Industrial/Technical Accidents"

In addition, giving room for new developments and ideas in the area of management principles a special fifth, transversal group on "Modern management concepts for innovative Crisis Management" was also established.



Picture 3: Organisation of WG4

4.2 Risks and challenges

Crisis Management methodologies depend on the phase within the Crisis Management cycle rather than the type of incident. In order to justify and substantiate this hypothesis, different risk scenarios have been extracted from relevant security policy papers available in Europe, which then were analysed on their impact on Crisis Management.

Policy Background

Security policy documents are available on both national and European level; with quite varying depths and quality. These policies represent a broad range of risks already visible or foreseeable in the near future. Similar diversity in quality can be found in terms of challenges. Some 30 security policy papers were perceived relevant for the Crisis Management issue and thus analysed within WG4. Experts of different European policy areas complemented the results of the document analysis.

These analysed documents reveal a set of risk categories which appear common for Europe throughout the various sources and have a clear link to Crisis Management.

Main Risk Scenarios
Complex humanitarian crises
Natural disasters
Major industrial accidents
Terrorism and organized crime attacks
Proliferation of WMD

Table 2: Risk scenarios from security policy papers

Operational paradigms of Crisis Management seem almost universally applicable and different risks may lead to similar challenges for Crisis Management. Nevertheless, to considerably minimize the risk of missing important aspects of Crisis Management this complex thematic area has been approached based on these extracted risk scenarios.

Intervention in the scenarios "Proliferation of WMD" and "Regional Conflicts and State Failure" is characterised by regulatory and political activities rather than Crisis Management and operates on very slow pace compared to the other four risk scenarios listed in Table . Thus the analysis of WG4 focussed on the first four items in Table .

4.2.1 Risk scenario "Major Terrorist & Organised Crime Attacks"

In the list of "man made" catastrophes deliberate destructive acts committed by individuals or groups, be it criminally motivated or having a terrorist (political) background, play a major role both in the public perception and in national security policy papers. Sensitised by globally recognised incidents, this risk scenario gets a lot of attention.

Up-to date terrorist attacks are characterised by small directly affected geographical areas but with a widespread mass-psychological effect in the public. Targets tend to be infrastructure elements that are used by a lot of people (public transport, shopping malls, religious or sports events, facilities with a symbolic value, etc.) increasing the perceived risk of each individual to become a target. This reflects basically the intention of terrorist attacks which seems to aim for fear and destabilisation rather than for a high level of destruction in the first place. Infrastructure elements that provide basic public services (i.e. electric power systems, communications systems, food chain, water supply, tourist facilities) are also within the target range as they can affect a broad population with comparably little effort and damage.

Part of the terrorist strategy is the use of weaponry with a high fear factor. CBRN agents or other hazardous materials are regarded most likely to be deployed. All type of arms including conventional military hardware is part of suicidal attack schemes. In deliberate acts the attacker always dictates time and place. There is most likely no warning time.

Different to natural disasters that may emerge without warning as well the reaction to man-made acts of destruction one has to pay attention to securing evidence and traces to the assassin to allow prosecution and collection of intelligence but not interfering with recovery, aid and relief actions.

Due to the well structured characteristics of organised crime the geographical spread might be larger. The damage is often not immediately obvious as the activities address the global financial infrastructure, proliferation of banned material, or human trafficking. In contrast to direct attacks, a crisis originating from organised crime has a very different profile. There is rarely a single point in time that denotes the beginning of a crisis situation; it is much more a developing process.

CHALLENGES "TERRORISM & CRIME ATTACKS"	DESCRIPTION
MANAGEMENT OF THE INCIDENT SCENE	Any response force will have to deal with the management of the incident scene. Many different services from several disciplines have to co-operate. An adequate management of the incident scene is needed to guarantee that all these interests are considered in a best way. The location of the scene may be dynamic. Attack and different levels of effects need not be co-located. A multi–scene incident magnifies the problems and might overwhelm local capacities. Detecting and identifying dispersed CBRN agents, containing the spread of contamination, and mitigating the effects through decontamination are key qualifications of these response forces. Co-existence of securing evidence for prosecution of assassin and rescue activities which may interfere with each other.

CROWD MANAGEMENT AND EVACUATION	Attacks may take place in crowded areas in order to raise the level of public fear. Dealing with a large amount of people directly affected is a vital task of crisis responders.
SEARCH AND RESCUE OF VICTIMS	*Search and rescue of victims* is challenging basically due to the need to assure safety for the responders and the success of the rescue mission, meaning the rescue of a maximum number of people. Main requirements include ▶ Risk assessment for the rescue teams (CBRN, weather forecast, construction – see NY2001), based on adequate sensor systems ▶ Sensor systems in order to locate victims ▶ First aid kits and adequate PPE (personal protective equipment) allowing emergency physicians and other urgent care providers to operate in very harsh environments
PSYCHO-SOCIAL SUPPORT	Affected public and crisis responders have to deal with different forms of stress and other psycho-social strains, thus requiring quick and professional psycho-social support. People will be confronted with injured, mutilated, traumatised persons and probably also fatalities. External circumstances may intensify impressions because of the debris, fire, smoke, noise, suspected contamination, etc. This kind of psycho-social support is not only relevant during the crisis itself, but also afterwards during the recovery phase, sometimes even for the long-term. This counts for first responders as well as for the public.
COMMUNICATION – TECHNICAL ISSUES AND INFORMATION PROVISIONING	Communication is paramount! If information cannot be exchanged technically any operation is limited to what can be exchanged on a vis-à-vis oral basis. Communication requires infrastructure, both the dedicated communications infrastructure and the electrical power infrastructure. In an incident both core elements may be severely affected leading to major outages. In addition, communication requires a common format; communications systems may require technical translation if the interconnected systems are not compatible. Communication is essential to reach the public, to guide the public and develop trust in the operation and in the operating forces. The media can draw massive public interest on certain incidents and perspectives and is, in doing that, a major player in terms of psychological effects.
POLITICAL SENSITIVENESS	The involvement and affectedness of foreign personalities may have to be accounted for possible *political sensitiveness*. Effective communication, mutual trust and adequate transparency are critical assets in such situations and demand well prepared and trained responsible persons and communication procedures.
TRAINING AND EXERCISES	First responders and the respective authorities need to be competent, well prepared and trustworthy on several challenging tasks as outlined before, in order to be able to cope with many different situations, in particular because any new crisis most likely contains a lot of uncertainties, which may influence any decision making process.

Table 3: Challenges for risk scenario "Terrorist & Organised Crime Attacks"

4.2.2 Risk scenario "Major Humanitarian Crisis"

Large-scale or major humanitarian crises rarely build up on their own. They are side products of other types of problems, most of them being man-made; sometimes a natural catastrophe is the cause of a humanitarian crisis but still its occurrence requires human intervention of some sort (deliberate passiveness).

Humanitarian crises are characterised by large numbers; an immense number of people affected, large geographic regions involved; people on the move into remote areas. Humanitarian crisis situations typically do not emerge suddenly and unexpectedly they build up over time and allow for close monitoring and even early intervention.

Humanitarian crises have strong political implications. The political establishment in the crisis zone is often part of the crisis problem and political ties need to be considered. Conversely, people within the EU sometimes have a very selective appreciation for sending help into areas which are not prominent holiday destinations.

It is commonly assumed that these types of crisis are located more outside EU territory but require action from the European Community. However, the EU borders could become a very close area for problems, as the current refugee situation in the Mediterranean illustrates.

Humanitarian crises are a major concern for all actors in the EU's external Crisis Management system . The EU has a number of Community instruments specifically designed for addressing crisis situations, and operates usually in cooperation with international actors, its Member States and the local organisations:

EUROPEAN COMMUNITY INSTRUMENTS FOR CRISIS RESPONSE	
HUMANITARIAN AID	Provides assistance, relief and protection to victims of natural and man made disasters such as conflicts or outbreaks of violence
CIVIL PROTECTION SECURITY MECHANISM	Facilitates cooperation in civil protection assistance interventions
THE INSTRUMENT FOR STABILITY	Crisis response component for providing assistance to enable timely response to political crises or natural disasters when such response cannot be provided through other Community external assistance measures or instruments

Table 4: European Community Crisis Management Instruments

In addition, other Crisis Management related activities are executed under the control of individual EU Member States, other states, international organisations, non-governmental organisations, etc. The main challenges, however, can be sorted into the following points (see table 6).

CHALLENGES "HUMANITARIAN CRISES"	DESCRIPTION
MULTI-FACETED APPROACH	Today, major and large scale humanitarian crises tend to require a *multi-faceted approach* that makes use of more than one Community or other crisis instrument. The European Union and its Member States should have the means and procedures in place to help coordinate humanitarian and other assistance as such, on an operational, non-political level[7].
IMPLEMENTATION OF COORDINATING MECHANISMS AND PROCEDURES	Credibility and visibility requires the EU and its Member States to respond timely, efficiently and effectively to a crisis situation. The practical *implementation of coordinating mechanisms and procedures is a key topic*[3] .
COORDINATION WITH MILITARY FORCES	The case of coordination *with military* forces providing security and also with humanitarian assistance in a crisis is particularly challenging. There is an accepted set of rules for the use of civil protection resources and military assets in response to humanitarian situations, but there is still a large need for constructive development of practical methods of cooperation, especially when the cause of the humanitarian crisis is a conflict, or the crisis takes place in a conflict zone. In addition to the central problem of coordination, there are numerous challenges more directly related to the work in the field.

	They are coupled to a great number of technical and non-technical capabilities, all of which could likely be improved through technological development and innovation programmes to improve operational coordination amongst civil security actors, i.e. emergency responders, fire fighters, security forces, medical teams, EOD/CBRN-squads and technical experts for restoration and reconstruction of infrastructure and lines of communication.
SITUATIONAL AWARENESS	A prerequisite for effective coordination is the provision of a best possible *situational awareness* for the coordinators and the operators in the field. Fast access to ground and space based sensor systems shall improve the assessments for humanitarian relief and reconstruction planning, providing detailed and rapid reference mapping of the affected areas including populated zones, the development of suitable methods to produce specific products to support post-disaster damage and needs assessments for humanitarian assistance and reconstruction planning, other products including rapid damage assessments, situation maps, refugee/IDP maps etc.
CRISIS LOGISTICS	*The logistics* of relief material and personnel and the *sustainability* of deployed European forces (civil and military) in the affected areas, including the provisioning and coordination of transport into the afflicted areas and the handling and transfer to destinations within the areas have to be well addressed.

Table 5: Challenges to the "Major Humanitarian Crisis" risk scenario

4.2.3 Risk scenario "Natural Disaster"

Natural Disasters are nature-borne but can appear "man-made" as well (e.g. climate change induced). However, for Crisis Management the cause of the incident is not relevant.

Natural Disasters build up in a very short time giving authorities little to no headroom for warning activities. The affected geographical areas can be huge and consequently the number of affected people may be large. Bush-fires and floods can spread thousands of square kilometres leaving thousands of people homeless.

Natural Disasters are the crisis situations that are most likely to directly affect EU territory. Recovery is an important factor already during the first interventions.

CHALLENGES "NATURAL DISASTERS"	DESCRIPTION
AVAILABLE INFORMATION/ SITUATION AWARENESS	The fast nature of the crisis development and its size make it necessary to have a reasonable baseline for decision making. Near real-time reporting providing information on various executive levels and across organisational borders is heavily required. Unlike other types of crisis situations, in a natural disaster the reconstruction starts already during the first response actions. Information on location of affected areas, the severity of damage and reconstruction activities need to be fed into a decision baseline.
COMMUNICATION	It can generally be assumed that, after such a disaster, the normal communication lines (terrestrial telecommunication and also mobile/cellular telecom) are not available due to disruption and/or overload. Broadcast (television and/or radio) may not reach the population any more as electric power supply may, at least initially, be down and/or broadcast stations and networks could be destroyed or severely damaged. Only very few private households will have emergency electricity and after a certain period also this may no longer be available due to fuel depletion of the generator. Without discrete and interoperable telecom networks/ systems for emergency relief forces, police, local administrations and respective lines to superior administration and catastrophe relief organisations (including dedicated military units), forces and resources cannot be effectively fielded under these conditions.

COORDINATION AND COOPERATION	*Coordination and cooperation* demands might occur at local level first (until communication lines are restored), then it may cover the vertical dimension from the first responders on the spot to regional and national authorities, and sometimes even beyond that to authorities in neighbouring countries and to EU bodies. In the horizontal dimension, different services from several disciplines, civil and military, and all kinds of relief organisations, professional and voluntary, sometimes with different nationality have to be fielded and somehow coordinated, at least at the lowest level by the emergency headquarters, in order to assure that the best possible help is provided to all affected people and the whole region of the disaster, and not primarily to "high-profile" targets.

Table 6: Main challenges for the "Natural Disaster" risk scenario

4.2.4 Risk scenario "Major industrial & technical accident"

Major industrial and 'technical' accidents may involve products and by-products of hazardous nature. Effects comprise explosions, large fires, toxic substances in the air, contamination of water, food, livestock and ultimately of people, and radiation. The geographical pattern varies from local to wide-spread. Most scenarios develop a large coverage and long time effects (contaminated soil, oil spills) due to the spreading of the hazardous substances and agents with wind, waterflows and sorption. Industrial accidents occur without indications and warnings and are a surprise even for those responsible for the technical process that eventually failed.

Most industrial accidents with major consequences were not "man-made" in the sense of intentional acts, but typically occur as a result of human error or technical failures . While those accidents and their causes itself would be rather a topic for safety-related research than for security (at least until the "man made option" is rolled out), their potentially disastrous dimensions are definitely within the scope of Crisis Management, not least in terms of care for affected people, evacuation needs and effects containment and recovery.

Industrial accidents could occur within the whole supply chain, i.e. from R&D to recycling and waste disposal, with their specific demands for response forces.

CHALLENGES "INDUSTRIAL ACCIDENTS"	DESCRIPTION
COMPLEXITY	Crisis Management has to start its operation on the basis of volatile situational awareness. A stable initial picture of the situation is often difficult to get, as affected companies develop their communication strategy on damage, risk and consequences on the spot. The complexity derives also from the potentially large number of people involved; both victims and first responders. And the numbers constantly increase because of the spreading of toxic fumes, displacement of toxic cloud, propagation of the contamination, etc. Measures have to be taken not only on the site of the accident but also at other locations, to provide medical and psychological help to the victims, housing for the persons who have been evacuated, etc.
RISK IDENTIFICATION	A specific challenge in the case of industrial accidents is to *identify* the specific products involved and released to appropriately determine the technical and medical response. The identification of these products may however take valuable time; initial results of the analysis will need confirmation. The safety of first responders is at stake as well as the safety of the affected public.
COMMUNICATIONS	Guaranteed free bandwidth for the Crisis Management teams is required when fixed phone lines have been destroyed and mobile phone networks are overloaded or do not function properly, including interoperability amongst the remaining systems. The quality of transmissions needs to be ensured, as communications may be obstructed by ambient conditions, e.g. environmental restrictions.

ASSESSMENT OF THE SITUATION AND DECISION MAKING	The leadership structure may require constant adaptation along with the development of the scene. Hand-over procedures together with legal provision controlling the access to information in all phases are required. In particular, as with the growing size of the incident, political considerations are involved.
EFFECTIVE (MULTINATIONAL) COOPERATION	Individual organisations are well organised and perform well. Co-operation however requires a broad set of technical and non-technical skills. Each involved organisation including the industry directly affected by the accident follows individual goals with a culture typical for these organisations. Understanding not only these cultural differences but also motivation based on legal circumstance that may even result in different technology used and incorporating them effectively into a Crisis Management team is crucial. This is a key challenge for crisis situations with a huge geographical spread. Specific challenges are different standards for identifying hazardous materials and documentation, language barriers, difficulties to trace back the manufacturer, the need for rapid risk assessment, based e.g. on real meteorological conditions on-site, real-time transmission of the risk assessment to the different responding agencies, lack of interoperability of communication systems, lack of GIS systems and lack of standard formats, communication between responding agencies and between first responders on the ground, different standard operating procedures, lack of standardised denominators and terminology, lack of agreed standards for toxicity levels, etc.
COMMUNICATION AND INFORMATION TOWARDS THE MEDIA AND THE PUBLIC	Modern communications technologies allow practically everyone to actively participate in the public perception of a crisis. Not only real time coverage of established news stations but also social networks (e.g. facebook, twitter) become opinion leaders generating information where the quality and validity is not confirmed. The confidence of the population in the acting authorities is under special scrutiny and affects cooperation in following instructions and orders. People tend to trust more in what friends say than what comes from an anonymous authority. Therefore information spread over social networks may strongly affect the public perception of a situation. The crisis responders need to ▶ Provide real time information to a multi-cultural audience and to overcome cultural and language barriers. ▶ Fight myths: toxic and moreover radiological and biological accidents generally generate great fear worsened by existing myths and misconceptions about the nature of the risk.
PSYCHOLOGICAL NEEDS	The emergent psychological needs of the population may aggregate and contribute to panic and disproportionate fear. The challenge is to provide acceptable psychological and psychosocial support (and possibly advice as far as managing the crisis is concerned) to the affected public and the Crisis Management teams, which also could suffer from the traumatic effects of the incident.
CONSEQUENCE MANAGEMENT	Interruption of critical infrastructure for a long period of time leads to massive outfall. Ensuring business continuity, however, protection of the environment and maintaining public order are particular challenges for consequence management. In the case of biological and radiological contamination, however, the crisis may last for many years, demanding long-term oriented, sustainable response and recovery measures.

Table 7: Challenges to the "Major Industrial Accidents" risk scenario

4.2.5 Core Challenges for Crisis Management

The detailed assessment of the four selected risk scenarios reveals different perspectives, as well as a common notion of the main operational challenges for Crisis Management. This conforms to the initial hypothesis that CM needs are rather independent from specific incidents.

According to the synthesis of the surveyed risk scenarios, the following core challenges can be extracted for CM, which need to be tackled with appropriate capabilities:

CORE CHALLENGE FOR CRISIS MANAGEMENT	DETAILS FROM THE ASSESSMENT
ENABLING THE PUBLIC	Training & exercises (EX)
STRENGTHENING RESPONSE FORCES	Communications – technical and information; training & EX
STRATEGIC PLANNING	Multi-faceted approach; risk identification; complexity management; consequence management
STRATEGY AND TACTICAL SIMULATION	Crowd management and evacuation; complexity management
INNOVATIVE CONCEPTS	Multi-faceted approach; complexity management
SITUATIONAL AWARENESS AND DECISION MAKING	Scene of incident management; crowd management; political sensitiveness; situational awareness and assessment; risk identification; consequence management
CO-OPERATION	Scene of incident management; Communications – technical and information; Implementation of coordination mechanisms & procedures (including military); complexity management; effective cooperation
COMMUNICATION WITH THE PUBLIC AND THE MEDIA	Crowd management; political sensitiveness; complexity management
MANAGING RESOURCES	Scene of incident management; search & rescue of victims (SAR); crisis logistics
OPERATIONS SUPPORT (MEDICAL AND PSYCHO-SOCIAL)	SAR; psycho-social support
RECOVERY LOGISTICS	Crisis logistics; consequence management

Table 8: Core Challenges for Crisis Management

4.2.6 Long-term issues for Crisis Management

Long-term scenarios as elaborated in WG5 will potentially lead to variations in the scale and characteristics of future incidents, but the types of crises analysed in WG4 were found to be robust also in the long-term view, potentially with growing incidence rate (natural disasters and humanitarian crises e.g. due to climate change, industrial accidents e.g. because of increasing technological complexity and interconnectivity).

Most identified CM challenges, in particular those dealing with information, communication and coordination needs will remain highly important in the long-term. They correlate with the "scenario-independent" characteristics of Crisis Management and its needs. Logistics could be clustered in this group as well.

Some challenges, however, vary in their importance, from (G) – where the demand for capabilities to tackle these challenges

might be low due to the overall optimistic global environment and development of global capabilities – over (M) and (N) in between to (W), where the comparable demand might be much higher as the global environment is much more conflict laden.

ESRIF SCENARIO	POTENTIAL IMPACT ON CRISIS MANAGEMENT
(G) GLOBAL GOVERNANCE	Major crisis interventions take place worldwide in a coordinated, effective and efficient way – novel and far reaching Crisis Management capabilities tackle the challenges of information overflow. **A globalisation of Crisis Management** would have consequences for European and national capabilities (principle of subsidiarity, role of federalism etc.).
(M) MULTI-POLAR REALISM	Humanitarian or natural disasters could be abused as a "justification" for interests-driven military interventions worldwide. Imaginable consequences for Crisis Management policies could be ▶ A militarisation of Crisis Management ▶ A redundancy of civil protection capabilities, ▶ An increasing rivalry between military and civil protection forces, in particular regarding resources and political support.
(W) THE WEST BETWEEN THREAT AND ATTRACTION	Public Crisis Management capabilities and procedures are predominantly limited to national and, to a lesser extent, European level. Limited budgets and constantly growing public debts attract the outsourcing of these capabilities. Private organisations are preparing to fill the gap – and are competing against the remaining public agencies. **"Blackwaterisation" of Crisis Management** would force major shifts in the current aid paradigms which are currently based on national and private engagement. A drastic change in the perception of the NGO is also required.t
(N) NEW WELFARE FOR ALL	Future Crisis Management capabilities have been established, with a sound based mixture of national, European and global responsibilities. The thriving economy could prepare the ground for a tendency to organise civil protection in novel public-private partnerships (PPP), which could lead to not considered possible **"innovation" in Crisis Management.**

Table 2: Long Term Scenarios in light of Crisis Management

4.3 Required capabilities, gaps and derived research

The findings on Crisis Management do not claim to be comprehensive or exhaustive. By nature they represent a snapshot of an ongoing process rather than a final result. Further continuous investigations are necessary in particular to elaborate the differences in national capabilities and to take technological, sociological and management theoretical improvements into account.

Withstanding a risk that materialises in a crisis situation incorporates challenges of a different nature. In dealing with the challenges certain capabilities need to be present. Any deficiencies in this set of capabilities require investigations and research in order to close the gap.

Crisis Management depends on the type of crisis only in the way different tools are used. The activity principles turned out to be the same for all crisis situations. Most capabilities are even similar in all mission phases and thus lead to a large category of common need capabilities. Therefore, the elaborated findings of WG4 with some 70 topics of different range and granularity were clustered along major capability areas avoiding an unbalanced situation with regard to specific scenarios and reflecting more the generic nature of Crisis Management.

4.3.1 Priorities for Research and Innovation in Crisis Management

P	CAPABILITY AREAS	RESEARCH & INNOVATION NEEDS	
1	ENABLING THE PUBLIC	European citizens should be regarded as a decisive and integral active part in any future Crisis Management solution. Every individual has his or her own resilience capabilities that need to be enforced and deployed in a crisis situation. Capabilities aspects comprise: ▶ Exercises and Trainings with the public ▶ Tools and Equipment for the public ▶ Communications infrastructure for public use	Research and innovation should analyse how the public could be best enabled to actively contribute to such solutions, what the key enablers are and how the public should be educated, trained and prepared to be ready to act accordingly when the moment is there – taking into account cultural diversity and marginal groups.
2	Strengthening response forces	Response forces need state-of-the-art technical equipment in the field of sensors, communications and utilities. However, the most promising way to strengthen and enforce crisis response forces is to bundle and deepen all efforts at the European level, in the Member States and by the private sector in the broad area of education, training and exercises. Capabilities aspects comprise: ▶ Exercises and Trainings for response forces ▶ Tools and Equipment for response forces ▶ Simulation and training facilities ▶ Lessons Learned cycles ▶ Harmonisation of operations standards ▶ Large scale exercises	Research and innovation need to address the use of virtual live exercises and other simulation-supported training methods, in particular multi-hazards training simulators, the development of methods and tools for lessons learned analysis, exchange and integration into planning and training. Standards need to be determined e.g. for PPE used by different first responders.
3	Strategic planning	Traditionally, Crisis Management forces are strongly operations and incident oriented, with little need for long-term, strategy oriented planning. With the growing complexity of Crisis Management operations the need for a more systematic and long-term oriented planning becomes evident. Capabilities aspects comprise: ▶ Preparatory actions that are to be conducted prior to an incident ▶ Plans and Standards ▶ Contingency and Backups ▶ Supply (e.g. energy and water support) of the intervention forces ▶ Security of to be deployed infrastructure ▶ Risk Management	Research and innovation should support this kind of planning by developing strategic foresight and risk assessment capabilities, supporting scenario development and analysis, providing monitoring and mapping tools for Crisis Management capabilities, and contributing to a systematic and coherent capability analysis and development. The development and evaluation of emergency and contingency plans should be improved by exploiting the "Concept Development & Experimentation" approach

4	STRATEGY AND TACTICAL SIMULATION	The need for "intelligent" planning and decision support on the strategic and tactical level is noticeable. Capabilities aspects comprise: ▶ Simulations used in the planning process ▶ Assumed behaviour of public and critical infrastructures ▶ Service levels of intervention forces ▶ Long term effects of an incident ▶ Simulations to be conducted during operations to support the decision making process ▶ Flow of goods and persons, merging of data from different sources into one operational picture	Research and innovation activities in the security sector dedicated to M&S-based supporting tools need to be continued having a close look at the emerging technologies in particular on the interoperability issues for M&S tools.
5	INNOVATIVE CONCEPTS FOR MANAGEMENT	The idea of innovative concepts is that the changing security environment with its inherent uncertainties and emerging new challenges for security forces require not only improved strategic planning capabilities, but also continuous reviewing of current Crisis Management concepts. Capabilities aspects comprise: ▶ Trust in information ▶ Management tools and work flow ▶ Dynamic organisational developments ▶ Motivation ▶ Network enabled operations	Research and innovation should support the process of adaptation of these concepts to the new challenges two-fold: on the one hand, modern management concepts and tools and their possible use for innovating Crisis Management concepts should be assessed, understood and exploited (e.g. adaptive complexity management). On the other hand, novel system of systems approaches like the NEC (network enabling capabilities) concept should be analysed for civil security applications and related capabilities should be developed.
6	SITUATIONAL AWARENESS AND DECISION MAKING	With the increasing amount of available information coming from more and more sophisticated sensor systems on the one hand and by means of information sharing with other organisations on the other, research on Crisis Management processes and workflows together with human factor issues shall improve the effectiveness and efficiency of the crisis managers. Capabilities aspects comprise: ▶ Integration of structures and technologies that provide sensor/surveillance data ▶ Geo-referenced information space ▶ Data fusion ▶ Information representation ▶ Information flows ▶ Near real time aspects ▶ Network centric capabilities ▶ Information distribution to field ▶ Dependability of systems ▶ Decision Support Systems ▶ Early indications for warning	Research and innovation shall focus on new ways of offering information to the user. The rapidly increasing amount of data available needs accurate compilation depending on processes, workflows and most importantly the individual needs of the user. Each person develops a very personal model to cope with information overflow. "One size fits all" will not be appropriate for future amounts of data.

7	CO-OPERATION	The stated growing complexity of crises situations and their response needs counts also for the number of persons, agencies, authorities and organisations involved in dealing with crises. Capabilities aspects comprise: ▶ Communications technology ▶ Technical interface definitions ▶ Workflows ▶ Language barriers ▶ Legal aspects of information sharing ▶ Multi-organisational dynamics ▶ Cross-border dynamics ▶ Political dynamics	Research and innovation shall investigate and improve the ability of all actors to flexibly cooperate with multiple organisations in order to cope with fast developing and changing crisis situations (multi-dimensional, multi-national, multi-agency, spacious or remote, etc.), and to identify and develop cross-cultural needs capabilities (e.g. overcoming language barriers) for crisis managers. Core area is communications technology.
8	COMMUNICATION WITH THE PUBLIC AND THE MEDIA	Public media have an immense influence on the perception of the performance of the Crisis Management and intervention forces. The may both help and obstruct Crisis Management activities. Capabilities aspects comprise: ▶ Preparing the public ▶ Alerting ▶ Reliable information sources during crisis ▶ De-escalation schemes ▶ Integration of political statements	Research and innovation shall relate to the understanding and exploiting of new forms of addressing public by Crisis Management actors in order to cope with the fast spread of information during a crisis to the public (e.g. via all forms of media), and of addressing the media for the benefit of crises containment and overcoming.
9	MANAGING RESOURCES	Managing resources, in particular critical resources and volunteers, is essential to be able to deliver effective and efficient crisis solutions. Capabilities aspects comprise: ▶ Integration of volunteer help offered in terms of labour, money, tools etc. ▶ Logistics for fast integration ▶ Standards and standard practices ▶ Termination of volunteer help	Research and innovation should focus in this area on how to improve the ability to manage existing capabilities and (physical) resources in an optimal way to effectively handle crises, i.e. sharing resources among different Crisis Management actors at local, multi-regional, multi-national level and thus facilitating joint resource allocation.
10	OPERATIONS SUPPORT (MEDICAL AND PSYCHO-SOCIAL	Medical and psycho-social support of Crisis Management operations are vital. Stress and traumata of victims, eye witnesses and the response forces itself have a strong impact on the dimension and magnitude of a crisis. Effective intervention strategies and related support should be developed respectively existing approaches consequently enhanced. Capabilities aspects comprise: ▶ Stress and Traumata help for victims, intervention forces and volunteers ▶ Medical emergency provisions ▶ Support for displaced persons, refugees registration and processing	Research should identify optimum deployment scenarios of medical and psycho-social intervention forces. Tools and methods of intervention should be improved.

11	RECOVERY LOGISTICS	Complex crises situations, wide regions affected, operational areas potentially worldwide and probably the need for longer-lasting operations pose specific demands on the logistics capabilities of Crisis Management forces in Europe. Capabilities aspects comprise: ▶ Reconstruction after a crisis ▶ Financial instruments and organisations ▶ Recovery structures	Research and innovation should enhance present capabilities by developing post-crisis needs assessment methods and tools for reconstruction and recovery planning, and appropriate approaches for facilitating coordination needs in this regard. This should cover structural damage assessment tools and related data integration and analysis as well as dedicated Crisis Management resources and sustainability logistics planning.

Table 30: Prioritised capability areas and related research and innovation needs for Crisis Management

4.3.2 Further findings

Crisis Management is considered a very specific management discipline. It is heavily influenced by technological capabilities but still bound into existing organisational structures and leadership concepts.

Compared to the time when Crisis Management structures were developed and implemented a radical shift in information availability took place and is still progressing. While current organisations build upon a process of information aggregation along a hierarchy emerging technologies promise to provide any individual within a mission with the same high level of information in near real-time. This situation enables new structures of decision making that have not been possible in the past.

4.3.3 Alternative Crisis Management approaches

Considerations on alternative Crisis Management approaches are based on a series of scientific papers and military articles referring to military applications – including critical evaluation. Findings derived from the analysis of alternative management models for Crisis Management can be summarised as follows:

Complexity *Rapid change* *Uncertainty* *Novelty*	
Surprise	*Efficacy (results)*
Extent of the event and extent of consequences	*Effectiveness (performance)*
Extent of destruction (including destruction of confidence)	*Costs* *Accountability and control*
Table 41: Crisis Management Characteristics	Table 52: Crisis Management Evaluation Criteria

RESEARCH TOPICS	DETAILS FROM THE ASSESSMENT
RELATIVE ADVANTAGES BUT ALSO THE LIMITATIONS OF EACH CM METHOD AVAILABLE ON THE MARKET	The specific technologies CM methods draw upon and the conditions which must be fulfilled for implementation need to be determined, with regards to the whole process or specific phases, or aspects of the CM process, with regards to different types of crises and of the above characteristics of incidents and criteria. Each CM method or model should be field tested. Conceptual, theoretical, practical and empirical combinations of the various methods and models should also be evaluated.

ADEQUACY AND LIMITS OF VALIDITY OF MILITARY APPROACHES AND OF THE BUSINESS/MANAGEMENT MODELS FOR CM	Models, technology and technical solutions, applicability and usefulness should be more thoroughly investigated.
DUAL- OR MULTI-USE, MULTI-PURPOSE, MULTI-TASKS, MULTI-MISSIONS, MULTI-EFFECTS, MULTI-MODES (CIVIL/MILITARY, NORMAL LIFE/CRISIS SITUATION, ETC.) TECHNOLOGY AND APPLIANCES, AND FIRST-RESPONDERS TEAMS	Investigations in modularity and adaptiveness of CM tools and equipment is essential, as the increasing number of modes and states of technology the human being has to cope with becomes critical.
AUTONOMY (INCLUDING FROM TECHNOLOGY)	

Table 6: Alternative Management Issues to be investigated

By looking for alternative management approaches for the benefit of CM, some overarching needs should be taken into account, which could be summarised as follows:

Table 74: Enlarging the spectrum of solutions and the range of resources

Look not only for first-order but also for long-term, higher-order solutions (e.g. to cope and live with crises by reducing their long-term impact).
Develop solutions by looking for richness, contradiction, and diversity of approaches.
Humans all have something to say about crises, and the way to deal with them.
Crises are fought not only from the top but also from the bottom; the potential and the capacity of the common, the poor and the excluded to innovate and to cope with crisis situations must also be acknowledged.
Culture represents both a source for meaning and know-how, and possibly a key aspect when implementing solutions.
Creativity and resilience are part of human nature, which must be revealed, stirred, encouraged and upheld.
Reflect not only on the way to handle crises but also on the risks we take and on our own responsibilities for the crises that are occurring.

To continue this thinking and to build on the virtual network of scientific researchers and CM practitioners all around the world the creation of an International Crisis Management Excellence Center is suggested.

4.4 Conclusions

Crisis Management is a very specific instrument for executing a mission. It is not a mission in itself. Crisis Management is the management and leadership topic dealing with a level of uncertainty that is uncommon to other management disciplines; but it is not a purely technological topic. Crisis Management is under an increasing level of public scrutiny and it is facing an enormous potential when finding a way to include the public in the crisis mission.

ESRIF KEY MESSAGES	CONTRIBUTION OF CRISIS MANAGEMENT
SOCIETAL SECURITY AND RESILIENCE	Research and development for Crisis Management foster the idea of European societal security and resilience through the promotion of putting the public and its crisis response capabilities at the forefront of all research activities, because crises are fought not only from the top but also from the bottom. The ultimate goal is to enable the public to cope with the changing security environment and its impact on society.
TRUST	The civil security challenges presented by Crisis Management depend highly on the trust of the public. Focused education, training and other forms of trust building will be essential, like new forms of communication between public authorities and the population, and appropriate measures for an improved cross-cultural understanding of Crisis Management stakeholders. Human sciences should be recognised and exploited for the benefit of trust-building and trusted Crisis Management.
BROAD-BASED CAPABILITY DRIVEN INNOVATION	Demand and supply side for Crisis Management capabilities face their common responsibility for ensuring effectively tailored synergies unleashing security solutions through a shared systematic interaction for innovating Crisis Management through a capabilities-based approach. For future Crisis Management capabilities and related technologies it will be essential to focus on adaptiveness, i.e. to increase the functionality of units and technology in terms of multi-use, multi-purpose, multi-task, multi-mission, multi-effect and multi-mode abilities.
AWARENESS RAISING THROUGH EDUCATION AND TRAINING	Education, training and exercises are the pillars of effective and efficient Crisis Management. Significant progress will be achieved by the development of dedicated education and training programmes for all security stakeholders (including the public), and the expanding of joint and multinational training and exercises of European level, exploiting simulation-based support to the maximum and eventually leading to the creation of an International Crisis Management Excellence Centre.
INTEROPERABILITY	Future Crisis Management solutions account for the various and increasing interoperability needs by reflecting existing and developing systems, looking at an early stage for interfaces to adapt existing technology to the new, and addressing the growing complexity of multi-dimensional, multi-national and multi-agency Crisis Management operations technically, organisationally, semantically and culturally.
A SYSTEMATIC APPROACH TO CAPABILITY DEVELOPMENT	Strategic foresight and risk assessment, scenario development, capability-based planning including performance evaluation, and system-of-systems approaches like the NEC concept are the basic assets for an improved and complexity countering capability development process for Crisis Management in Europe.

Table 15: Key Messages of ESRIF and WG4 contribution

5. Working Group: Foresight and Scenarios

5.1 Introduction

It should be clear from the chart of ESRIF working groups in the introduction to Part II that the role of WG5 Foresight and scenarios is different from all the other groups.

In particular the WG has had the dual mission of, on the one hand, working together with all other WGs on the long-term security perspectives as part of ESRIF's mandate, on the other developing a research agenda for its area of expertise. This is a methodological area of potential relevance to all substantive security domains. However, methodological advances require input from real problems to be sound, and therefore the collaboration with other ESRIF WGs was essential for developing WG5's research agenda.

According to its terms of reference WG5 has four focus areas, also corresponding to the work-packages of the WG (champions in parentheses):

1. **State of the art scan – mapping of relevant existing foresight studies (Per Wikman-Svahn supported by Matthias Weber)**

2. **Context scenarios to frame European security in the 20+ years timeframe and help identify emerging insecurities, scope for novel security concepts, unintended consequences of security measures etc (E. Anders Eriksson)**

3. **Foresight methodologies for managing security research and innovation (Matthias Weber)**

4. **The role of foresight and scenarios to support high quality societal debate on issues of security and insecurity (Erik Frinking)**

Kristiina Rintakoski was the WG leader and E. Anders Eriksson rapporteur.

The structure of this chapter generally respects the order of work-packages above, but there is no simple one-to-one mapping between WPs and sections:

- Sections 5.2 and 5.3 both report the State of the art, the first in terms of foresight at large – i.e. not specifically focusing on security whereas Section 5.3 reports the mapping done of recent security related foresight studies.
- Section 5.4 reports the context scenario work and the extensive interaction with other WGs in that setting in methodology and process terms – and presents the context scenarios developed and exploited.
- Section 5.5 is the pivotal element of the chapter where substantive conclusions from the context scenario work are identified and in turn provide the impetus for identifying knowledge and competence gaps. Hence this section bridges on the one hand WP2 and 3 and on the other WP3 and 4.
- Section 5.6 develops research needs and priorities addressing the knowledge and competence gaps identified in Section 5.5.
- Section 5.7 finally briefly relates WG5's work to the joint results of ESRIF, part I of this report.

The conclusions for ESRIA of WG5 are based on three strands of input: a general state-of-the art survey of foresight (Section 5.2), a survey of foresight exercises in the security domain (Section 5.3), and the experience of developing and exploiting a set of context scenarios with the other ESRIF WGs (Section 5.3). These inputs convinced us of the general usefulness – not to say necessity – of security analysis approaches based on foresight and scenarios. But we also found considerable need for developing new knowledge fusing this with risk analysis. For this new knowledge domain we suggest the heading of strategic foresight and risk analysis. A particularly important focus area cutting across strategic foresight and risk analysis is better understanding of the continuum of perspectives on societal risks and threats ranging from consequence orientation (only magnitude of consequences matter) through to probabilistic risk analysis (consequences are always weighted by their probabilities). Our knowledge and competence agenda for strategic foresight and risk analysis identifies the following six key areas included in ESRIA:

- It still represents a major difficulty to fully grasp and model the interplay of human behaviour with new scientific and technological opportunities, both in terms of generating new threat potentials and in terms of new preventive or reactive measures.
- Creativity is an essential pre-requisite for imagining future context scenarios and mission scenarios, but it is difficult to cultivate and mobilize.
- The monitoring and assessment of threats and options is a challenging task, in particular in view of the diversity and the lack of consensus about the goals and objectives against which to assess them, e.g. against the dimensions of a European concept of security.
- As a pre-requisite for conducting systematic risk assessment, it is essential to better understand the complex interdependencies of an increasingly broad range of factors of influence.
- While participatory cultures differ largely across Europe, security is an area that tends to have a rather limited tradition of broader societal debate. With the broadening of the security concept, however, this seems to be an important component.
- However, independently of the specific participatory cultures, there is a need to make the pros and cons of potential alternatives for security investment (broadly understood) transparent in order to be able to establish priorities in an informed way.

5.2 Foresight for research and innovation policy:

Rationales and state-of-the-art

This section discusses Foresight for policy in general but with a focus on research and innovation policy[1]

5.2.1 Rationales for conducting Foresight

Foresight as a methodology for dealing with emerging future challenges has acquired quite some prominence in policy circles over the past fifteen years. As captured in the subsequent definition, it is not about predicting the future – in contrast to earlier approaches typically labelled 'forecasting' – but about acting consciously to prepare for the contingencies and uncertainties resulting from the inter-play of future developments in science, technology, economy and society:

- Foresight covers activities aiming at thinking, debating and shaping the future. It can be defined as a systematic, participatory, future intelligence gathering and medium-to-long-term vision-building process aimed at present day decisions and mobilising joint actions (EC, 2002). This is even more essential today because the complexity of science, technology and society interrelationships, the limitation of financial resources, the increasing rate of scientific and technological change impose on governments and the actors in the research and innovation system to make choices.' (EC, 2009).

Foresight thus stresses the possibility of different futures (or future states) to emerge, as opposed to the assumption that there is an already given, pre-determined future, and hence highlights the opportunity of shaping our futures. This is very well compatible with the perception that the origins and forms of future security threats are becoming more diverse. Furthermore,

1 Section 5.2 draws extensively on Havas et al, (forthcoming).

foresight can enhance flexibility in policy-making and implementation, broaden perspectives, and encourage thinking outside the box ('thinking the unthinkable'), which are also important elements for tackling future security issues.

There are several reasons why foresight has acquired this high level of prominence. A number of important technological, economic, societal, political and environmental trends and developments affect all countries as well as most policy domains. In order to deal with the challenges associated to these developments, a new culture of future-oriented thinking is needed. This applies also to policy-making processes, which can be assisted by foresight in various ways.

The increasing number and variety of foresight programmes suggests that foresight can be a useful policy tool in rather different types of contexts, ranging from national and regional innovation systems to sectoral and corporate policies. The major factors driving the diffusion of foresight can be summarised in telegraphic style as follows (Havas et al., forthcoming):

- Given the significance of globalisation, sweeping technological and organisational changes, as well as the ever-increasing importance of learning capabilities and application of knowledge, our future cannot be predicted by any sophisticated model in a sufficiently reliable way. History also teaches us valuable lessons about the (im)possibilities of planning and predicting the future, not least in the context of security. Therefore, flexibility, diversity, open minds for, and awareness of possible futures are thus indispensable.

- In the knowledge economy, more attention is required to develop a number of skills, such as creativity, innovative problem-solving, communication and co-operation proficiency in multidisciplinary, multicultural teams. New forms of co-operation (e.g. clusters, innovation networks) have become a key factor in creating, diffusing and exploiting knowledge and new technologies, and therefore in satisfying social needs and achieving economic success. Developing these kinds of skills requires exploring future skills and capability needs.

- As for policy-making itself, there is a widening gap between the speed, complexity and uncertainty of technological and socio-economic changes giving rise to security issues, on the one hand, and of the ability to devise appropriate policies, on the other. Under these circumstances, longer-term considerations and the precautionary principle are bound to gain a growing attention in guiding policy-making processes.

- Governments try hard to balance their budgets, while cutting taxes. Hence, they need to reduce public spending relative to GDP. In the meantime, accountability – why to spend taxpayers' money, on what – has become even more important in democratic societies. Public R&D and innovation expenditures are as much subject to these demands as investments in security assets (even if both areas have received a lot of attention and preferential treatment when it comes to financial allocations during the decade or so).

- Policy-makers also have to deal with intensifying social concerns about new technologies. This is the case, for instance, for ethical and safety concerns related to biotech or nuclear technologies, and fears of unemployment and social exclusion caused by the rapid diffusion of other new technologies. But it is also reflected in the broad notion of (societal) security that has become prominent in policy debates.

- The credibility of science is somewhat fading, and with it the 'objectiveness' of policies based on scientific research. Scientists themselves are known to have different opinions and come to different conclusions on the same issue. This also applies to security research, where expert circles alone do not dispose of the necessary legitimacy to define what is 'true'. Instead, participation of a wider audience is increasingly needed.

Foresight helps policy-makers to sense and anticipate these kinds of developments. It allows realising and reacting to trends, and thus points to action needed to block or slow down negative trends and accommodate favourable developments. Moreover, recent foresight actions aim explicitly at picking up weak signals: weak but very important hints that a fundamental re-assessment and re-alignment of current policies are needed. In other words, foresight can serve as a crucial part of an early warning system, and it can be used as an instrument for an adaptive, 'learning society'.

5.2.2 Positioning foresight in the policy process: towards policy integration

In the 1960s, government policies in relation to research and technology were predominantly inspired by an approach that today is often labelled as 'picking winners': promising technologies, sectors and large players were selected as being of particular public or strategic interest and were thus doted with significant amounts of financial and other types of support. With the recognition of the limitations of government's ability to actively plan and shape future developments in an efficient and fully informed manner, the late 1970s saw the emergence of new paradigm in research, technology and – then also – innovation policies, which was characterised by a focus on shaping framework conditions that are conducive to innovation. This 'hands off' approach was subsequently evolving into what is nowadays called the systems approach to research and innovation, which not only deals with framework conditions but also with the institutional and structural settings for Research, technology development and innovation (RTDI). In line with these concepts, the 1990s were also characterised by a great reluctance of government policy to prioritise and select technologies and research themes in a top-down manner. In recent years, and driven by fiercer competition at global level for, especially, private investment in RTDI processes, we can observe a shift in policy-making practices from shaping framework conditions and structural settings towards strategic decision-making (e.g. in terms of defining thematic priorities of a country and region in a medium- to long-term perspectives.

Similar to this shift in approaches to innovation processes and STI policies, there has been a shift in the conceptual understanding of policy processes. Taking into account insights from strategic planning and complex social systems thinking, recent developments in policy-making processes go beyond earlier top-down models and stress interactivity, learning, and the decentralised and networked character of political decision-making and implementation. Earlier technocratic and linear process models of policy making in terms of 'formulation – implementation – evaluation' phases were replaced by cycle models, where evaluations are supposed to feed back into the policy formation and implementation phases. Already in these cycle models, policy learning is seen as an essential ingredient of political governance, to ensure continuous adaptation and re-adjustment of policies and related instruments.

More recently, it has been recognised that the effectiveness of policy depends also on the involvement of a broader range of actors than those formally in charge of policy decisions. The concept of distributed policy-making and intelligence (Kuhlmann, 2001) draws our attention to various policy practices relying extensively on the knowledge, experience and competence of a variety of agents. For government policy to be effective, this implies the participation of stakeholders. Further, the role of government is shifting from being a central steering entity to that of a moderator of collective decision-making processes, that is, the principles of modern democracy have an effect in these fields, too.

With such an open and distributed model of policy-making in mind, it is now increasingly recognised that an opening of political processes is necessary to ensure the robustness and the effectiveness of its outcomes. This is also reflected in the EC's White Paper on Governance (EC 2001), which stresses five principles of good governance: participation, accountability, openness, effectiveness, coherence.

The complexity and the interdependencies involved in policy-making are also recognised in the need for policy co-ordination, if not integration, in four different respects:

- horizontal policy co-ordination, i.e. between different policy areas
- vertical policy co-ordination, i.e. between different administrative layers
- multi-level policy co-ordination, i.e. between different levels of governance (European, national, regional)
- temporal policy co-ordination, i.e. between different phases of policy making processes. (OECD, 2005)

In this context, foresight assists increasingly interdependent and partly autonomous decision-making processes in a systematic manner.

5.2.3 Changing practices of Foresight

The aforementioned shift in conceiving of policy-making processes is reflected in the evolving practices of foresight (cf. UNIDO 2003, ForLearn 2009). First of all, it has emerged as a distinct approach as opposed to forecasting exercises on science and technology. Historically this trend is linked to the adoption of the term 'technology foresight' as distinct from 'technology forecasting' and

the like. The underlying difference is that foresight is a participatory activity, involving representatives of different stakeholder groups, while forecasting activities are solely based on S&T expert opinion.

As a second important trend, several foresight programmes have incorporated market and business aspects, while yet another group of them considered societal issues. This broadening of the scope of forward-looking exercises can be interpreted as a reflection of the abandoning of simplistic models of technological change, and the adoption of a systemic understanding of innovation processes, including the co-evolution of social, economic, and technological changes.

Thirdly, we can see a strong emphasis on, and belief in, the contribution of foresight activities to shaping rather than predicting and controlling the future. The Delphi surveys in the 1970s and 1980s, as well as the key technology studies conducted in the US, in France and the Netherlands were strongly influenced by the linear idea that the consensus achieved could serve as a forecast, and thus as a foundation for taking preparatory actions to exploit emerging technologies. In the meantime, countries that until the 1990s were relying on Delphi surveys to support their research and technology policies have recurred to complementing their tool box by other methods to promote more intense participation (e.g. direct communications among the participants); the cases in point are, for instance, the German Futur process or the French FutuRIS project.

Foresight processes bring together not only experts, but also decision-makers from research, industry, policy-making and society, and thus a shared understanding of current problems, goals and development options can be expected to emerge among those actors that have an important role to play in shaping the future. This converging understanding of the issues at play is likely to contribute to improving implicitly the coherence of the distributed decisions of these actors, in line with the shared mental framework developed. In other words, the future is being shaped by aligning expectations and thus 'creating' a self-fulfilling prophecy. These so-called process outputs are often regarded as more important than the actual substantive (or tangible) outputs like reports and websites.

Finally, and most recently, we can observe an increasing interest in foresight activities that aim at supporting strategy formation both at collective level and at the level of individual organisations, e.g. 'Adaptive Foresight' (Eriksson and Weber, 2008), or 'Sustainability Foresight' (Truffer et al., 2008). This interest is fuelled by the recognition that there is a translation problem apparent in foresight approaches that predominantly rely on broad participatory processes, namely the translation of shared collective problem-perceptions, expectations and visions into concrete decisions of individual actors and organisations. From this perspective, Foresight must be interpreted as an integral element of networked and distributed political decision-making processes.

5.3 State of the art scan of recent security related foresight studies[2]

The aim of this section is to present the result of a survey of recent foresight studies of relevance to the context of Europe's future security. The purpose of making the survey was to achieve further contextualisation and quality assurance of the work of ESRIF, in particular as regards foresight work.

The scan started with a request to ESRIF members in spring 2008 to provide references to recent foresight reports of relevance to ESRIF's work. The answers were reviewed and a selection of works of primary relevance for the present context was made. The selection criteria were as follows: the work should be published 2003 or later, have a mid- to long-term perspective, and be of relevance to Europe's future security context. This together with additional searches resulted in a list from which a core set of studies was selected for a more detailed analysis. The selection for the core set was primarily made on the basis that the available documentation of the study should be of sufficient breadth and depth to be meaningful to subject it to a deeper analysis. Based on these criteria the following core set of 12 studies was selected.

1. **EU Institute for Security Studies (EUISS), (2006), The New Global Puzzle: What World for the EU in 2025**
2. **UK Ministry of Defence, (2007), The DCDC Global Strategic Trends Global Strategic Trends Programme 2007-2036**
3. **National Intelligence Council, (2004), Mapping the Global Future**

2 For a more extensive presentation, see Wikman-Svahn (2009).

4. **National Intelligence Council, (2008), Global Trends 2025: A Transformed World[3]**
5. **Pullinger, Stephen (Ed.), (2006), EU research and innovation policy and the future of the Common Foreign Security Policy, ISIS Europe**
6. **NATO, (2005), NATO Future World Scenarios Future Worlds**
7. **Organisation for Economic Co-operation and Development (OECD), (2003), Emerging systemic risks in the 21st century : an agenda for action**
8. **World Economic Forum, (2007), Global Risks 2007- A Global Risk Network Report**
9. **Glenn, Jerome Clayton & Gordon, Theodore J. (ed.), (2006), 2006 state of the future, Washington, D.C.: American Council for the United Nations University, The Millennium Project**
10. **Shell International, (2005), Shell Global Scenarios to 2025: The Future Business Environment - Trends, Trade-offs and Choices, London: Shell**
11. **Deutsche Bank Research, (2007), Deutschland im Jahr 2020**
12. **Délégation aux affaires stratégiques (French Ministry of Defence), (2008), Prospective géostratégique - A l'horizon des trente prochaines années**

A brief description of state of the art scan results along with definitions of some useful terminology:

- 11 of the 12 studies in the core set highlighted important 'trends' – i.e. factors that shape the outcome of the future (e.g. 'changing demographics', 'economic inequalities'). Sometimes the word 'drivers' was also used in the studies[4]

- 7 studies presented more than one possible outcome of the global future, here called a 'context scenario'. A context scenario is typically described using a narrative – a storyline describing a possible future world

- 5 studies described more specific security scenarios, here called 'situational scenarios' (e.g. 'Nuclear device detonated in Europe'). A situational scenario can have today's world as its scene, but it can also be set in a future scene defined by a context scenario

- 6 studies explicitly listed specific 'threats' (e.g. 'Proliferation of Weapons of Mass Destruction (WMD)', 'Natural catastrophe: Inland flooding')

- 4 studies explicitly listed 'discontinuities', i.e. high-impact events that are very unlikely to occur, or occur with extremely low frequency (e.g. 'Global pandemic', 'Globalised economic collapse')

The primary analysis made in the state of the art scan was to map the trends identified by the studies in the core set and to survey the methodologies used in the different studies. The result is presented in the following sections.

5.3.1 Key trends

The studies in the core set were examined in terms of which trends they emphasized. In order to be able to map and compare the trends in the studies, a 'nomenclature' of key trends was constructed by clustering the trends found in the studies[5]. This exercise resulted in a set of 25 key trends categorised under 6 major headings: Demography, Economy, Environment, Science & Technology, Social Values & Identity and Governance & Order.

3 This study was included at a late stage.
4 The exception was Global Risks 2007.
5 The set used to derive the key trends was different from the final core set of studies. The studies used in the derivation of the nomenclature were, from the core set: The New Global Puzzle, The DCDC Strategic Trends, Mapping the Global Future, Emerging Systemic Risks, NATO Future World Scenarios. In addition the following studies were also used: När krisen kommer, Securely into the future 2025, Megatrends of the world's development, Protection of the Critical Infrastructure and key development trends of the global (EU) development. From these, ca 130 different trends were identified and used for clustering.

Demography	Science and Technology
Migration	Technological development
Urbanisation	Differences in access to technology
Ageing population	Information flow and sources
Diseases	Proliferation of WMD
Population growth	
	Social values and Identity
Economy	Changing values
Economic globalisation	Social cohesion
Economic growth (and turbulence)	
Emerging economic powers	**Governance and Order**
Social and income inequalities	Organised crime and illicit trade
	Terrorism
Environment	New conflicts
Climate change	International power relations
Environmental degradation	Global governance
Limited resources (natural and energy)	Democratisation
	Role of the state

Table 1 Nomenclature of key trends

The set of core studies were then mapped against these key trends. When some studies especially stressed a few trends more than others (i.e. 'main trends'), such cases were identified. Finally the trends identified in ESRIF (cf. below) were mapped against the other studies.

It turned out that most of the studies covered key trends in all of the 6 major headings. Emerging Systemic Risks did not stress trends under Social values and Identity¸ nor did NATO Future World Scenarios. EU research and innovation policy differs from the rest in that it did not mention trends under as many as three chapters: Demography, Environment or the Social Values and Identity. (This may be explained by the more limited scope of this report compared to the others.) Although Shell global scenarios to 2025 is a broad study, it is notable that it did not stress Demography as a driving force. (However, it did include it as a background trend.) The New Global Puzzle, DCDC Global Strategic Trends, Prospective géostratégique and the Mapping the Global Future stand out by spanning a large set of key trends, ranging from 17 to 21. The rest of the studies typically span 7 to 11 key trends.

On a more detailed level, one can notice that a trend typically is covered in 4-7 studies. The most popular key trends are Economic growth (and turbulence), Technological development, Global governance featuring in 9 different studies. The key trends Environmental degradation and Democratisation are the least common, each represented in only 3 studies.

5.3.2 Methodology

The studies were also studied from a methodological point of view. In particular they were assessed in terms of:

- Level of references to textual sources
- Level of outside participation

Level of references to textual sources

Most reports had a low or limited amount of references supporting substantive statements. The outstanding report in this respect is The New Global Puzzle, where statements are almost always supported by a reference. Deutschland im Jahr 2020 has a high level of references, mostly however to reports published by Deutsche Bank. Shell global scenarios to 2025, Emerging Systemic Risks and Prospective Géostratégique supported many of their statements (judged to be at a moderate level).

Level of outside participation

All reports seem to have used a combination of textual and human sources, although this is not always explicitly stated. The level of participation differs considerably between the studies, from the 29 international and regional conferences and workshops held in order to prepare Mapping the Global Future (this was considered to be a 'high' level), to the 15 experts contributing to a single workshop for the EU research and innovation policy (a 'low' level) . The relative weight of the sources also differs, e.g. The New Global Puzzle seems to be primarily based on textual sources, while the Global Risks 2007 seems to be mostly based on expert involvement in workshops. Only Global Risks 2007 and the DCDC Global Strategic Trends listed individual contributors. State of the Future described the regional and sectoral demography of the Delphi performed. Deutschland im Jahr 2020 referred mostly to work done within the organisation.

Other observations related to methodology

None of the reports explicitly described the criteria for identifying, selecting and using participating experts or literary references. The level of review of previous work undertaken is not always clear. The Mapping the Global Future definitely builds on previous own work (CIA Global Trends 2010, Global Trends 2015). Also, while not mentioned in the report DCDC Global Strategic Trends most likely builds on own previous work (including the JDCC study 'Methodology, Key Findings and Shocks'). NATO Future World Scenarios explicitly states that a review of 30 previous foresight exercises was undertaken (with references given to these), 'encompassing over 100 different scenarios'. The State of the Future builds on own scenario work in the UN Millennium Project since 1996, while also stating a continued survey of published information about global scenarios developed by other organisations.

Most studies provide very scarce documentation of the methodology used and even studies that provide relatively detailed information on methodology are not very explicit with the steps taken. Therefore, it is hardly possible to use any of the studies in the core-set as a role model for a methodology suitable to the needs of ESRIF WG5.

5.4 The context scenarios - working with the other WGs

5.4.1 Needs and expectations

To address the need for long-term foresight ESRIF employed an approach where a set of context scenarios with time horizon at ca 2030 were developed and used to scope how current trends may combine to create alternative future 'scenes'. The scenarios[6] were based on trends identified by ESRIF Integration Team and WG5, and prioritised by these constituencies in accordance with their appreciation of ESRIF's remit.

These scenarios were then used to test how short and midterms risks and challenges previously identified by other WGs within their respective areas of responsibility may evolve into the long term and also as creative devices to identify new emerging risks and challenges. This work took place first in summer of 2008 and then in December.

Prior expectations that this work should lead to relatively detailed insights regarding specific risks and challenges were not borne out. The main reason for this is arguably that the mission-oriented WGs – quite naturally considering ESRIF's absence of financial resources to engage in detail-level work – did little in terms of well-specified situational scenarios. Instead they typically worked with relatively generically defined – and hence robust with regard to external variations – classes of risks and challenges.

Despite this mismatch with expectations the context scenario work did create both substantive and methodological insights, reported in Section 5.5.

5.4.2 Methodology and process

Methodologically the work proceeded in the following steps:

6 See Section 5.3

5.4.3 Identification and prioritisation of key trends (or alternatively: key external variables):

This was done by ESRIF Integration Team members via an e-mail questionnaire and at a WG5 workshop. Subsequently the results were checked against the state-of-the-art scan; as can be seen from Table 1 we identified 25 key trends in recent relevant foresight work. The result of the comparison is that, with some reservation for Demography where only certain aspects of migration and diseases featured[7], the ESRIF foresight work was well in line with the state-of-the-art.

Had the state-of-the-art material been available earlier it could have been of great help in identification of trends. As for prioritisation, however, it is key for the ESRIF relevance of the ensuing sets of scenarios (or however one chooses to make use of identified key trends) that this is firmly ESRIF based.

The trends thus identified as most important by ESRIF WG5 were the following:

- **Global economy**
  - Technological developments
  - Complexity & interdependency
  - Cyber space life styles
  - Energy scarcity

- **EU's wider neighbourhood**
  - Climate change leading to environmental degradation
  - Social dysfunction in EU's wider neighbourhood

- **Social cohesion in EU**
  - Exclusion & radicalisation – 'indigenous' population
  - Ibid – 'immigrant' population

- **Global politics**
  - Multi-polar world
  - Post-Westphalian era

Drafting of context scenarios

It is possible to base foresight work on identified and prioritised trends – perhaps labelled as in the standard business strategy exercise, opportunities and threats. Developing context scenarios based on key trends does, however, have many advantages. Thus scenarios developed as logically compelling narratives can help in understanding how trends may interact to cancel out, modify, or amplify one another. They may also help in identifying how possibly emerging novel trends or singular events (like a major terrorist attack) may alter henceforth prevailing understandings of the relationships between key trends.

In developing the ESRIF context scenarios the following criteria were applied:

- Relevance – the work should inform the specific context it is commissioned for. Therefore it should start with the most salient contextual factors (key trends) determining the scope for European security research priority setting. In principle the list above was used, albeit not slavishly.
- Plausibility – the scenarios should be reconcilable with processes of change starting from today's situation and developing in internally consistent ways.
- Challenge – the scenarios should be able to produce a new and original perspective on the issues under consideration[8].
- Representativity (spanning) – the scenarios should be challenging also as a set in the sense of being as different as possible (subject to the above criteria) from one another[9].

---

7 The most well-known demographic trend, ageing population, can also be said to be a well-understood certainty that should be included in all scenarios. At least one other WG has brought the shrinking work-force up as a challenge.

8 The concept "challenge' here applies to both risks and challenges as these concepts are used in ESRIF.

9 This builds on criteria from Eriksson and Weber (2008), p. 475.

Note that the criteria define a balancing act as both the plausibility and the relevance criteria prohibit making scenarios 'too challenging'; this also makes a lot of sense since if a context scenario were so challenging, e.g., as to include a major war affecting Europe within the next few years, the issue of research with a view to long-term security risks and challenges would have major problems defending a place on the European security agenda, hence such a scenario would be irrelevant for ESRIF's purpose.

Already in making the first draft of the scenarios some variables receiving less attention in the prioritisation exercise were included as they were tentatively identified as key intermediaries to the policy problems likely to arise in applying the scenarios, viz.:

- Political cohesion of EU
- Acceptability of security measures
- Public/private roles in civil security

However, in ascertaining that the set of scenarios be both representative (maximally spanning) and plausible – for which a dedicated IT tool was used – the latter three dimensions did not feature; they were seen as dependent variables the (qualitative) value of which derives from the key trends treated putatively as independent variables – which of course does not rule out that patterns of dependency also among these may be subsequently discovered. With a set of core context scenarios defined in terms of combinations of key trends at hand it is then possible to add any number of dependent variables in response to the scenario users' needs (e.g., structure of organised crime or security effects of major nano-technology breakthrough). This further detailing of scenarios is essentially part to the next phase – exploitation. It is, on the other hand, not unusual that exploitation uncovers needs also to modify the core scenarios.

Exploitation of scenarios

In ESRIF the exploitation step happened in the form of workshops with Integration Team members, written input on impacts of context scenarios on identified risks and challenges for other (mainly political mission) WGs, and bilateral meetings between WG5 and other WGs. The first two took place during late spring and summer, the latter in December 2008. Generally speaking the face-to-face meetings were the most useful ones. As already commented this step was not without its problems. These problems provided helpful food for thought for WG5's research agenda as further outlined in Sections 5.5 and 5.6. The substantive conclusions drawn by other WGs are reported in their respective chapters and in the joint conclusions of ESRIF, part I of this report (cf. Section 5.7).

The context scenarios

By the process described above ESRIF WG5 developed four main context scenarios that were characterised in terms of seven main dimensions (see Table 2). None of the scenarios is to be seen as positive or negative along all dimensions. Instead, each of the scenarios shows some positive and some negative facets. Still, Multi-Polar Realism (M) and The West between Threat and Attraction (W) were seen by scenario exploitation participants as having more negative than positive facets, with Global Governance (G) and New Welfare for All (N) showing the opposite tendency. The key point of these scenarios is how they have been exploited (cf. above). Still we find it important to make them publicly available.

SCENARIOS DIMENSIONS	GLOBAL GOVERNANCE (G)	MULTI-POLAR REALISM (M)	NEW WELFARE FOR ALL (N)	THE WEST BETWEEN THREAT AND ATTRACTION (W)
Global politics (including cooperation for mitigation of climate change)	Unprecedented levels of cooperation in the face of Climate change	Competition and lack of trust among world powers	US and EU strongly committed to liberal democracy; strained relations with authoritarian powers	US with junior partner EU engaged in Global struggle against violent extremism; interest based cooperation with others

Global economy (including effects of technological development)		Long boom due to free trade and massive investment in Climate change mitigation/ adaptation	Weak due to protectionism and inability to deal with Climate change	Medium growth rate, rapid innovation and industrial pattern change	Medium growth rate, restructuring within established industrial pattern
EU's wider neighbourhood (including effects of climate change)		Positive social and environmental developments; little migration push	Environmental degradation and struggle for resources lead to armed conflict and	Positive political and social development; considerable environmental problems lead to	Armed conflicts and environmental degradation lead to mass migration
			mass migration	strong migration push	
Social cohesion in EU	**'immigrant' population**	Generally thriving off the boom, little tendency to radicalisation	Strong tendencies to violent radicalisation in both groups leading to dangerous conflicts	Effective social policies based on innovative public/ private partnerships lead to inclusive welfare	Major problems linked to Global struggle allegiances
	'indigenous' population	Some traditional industrial regions hit hard by competition with tendencies to racist radicalisation			Small problems
Political cohesion of EU		Different abilities to tap into the global economic boom lead to strains	Strong to cope with external and social pressure	Strong	Varying enthusiasm with respect to Global struggle lead to strains.
Acceptability of security measures		More 'Chinese' values lead to higher acceptance of discipline and invasion of privacy	Very high due to external and internal threats	Low level of security threat and generally high standards in civil rights put strict limits	Very high due to external and internal threats
Public/private roles in the civil security sector		Bigger role for private actors including voluntary organisations – citizens for security	Traditional roles with big primes catering to 'military' style demands	Innovative use of private sector, in particular SME's	Considerable outsourcing to big private firms

Table 2. ESRIF's context scenarios: A systematic comparison

5.5 Knowledge and competence gaps

This section presents the substantive conclusions drawn from WG5 working together with other WGs and then, based on this, the knowledge and competence gaps, which subsequently will lead us to research needs and priorities.

Consequence vs. risk: a long-term perspective on security problems

A first result of the work together with other WGs with the context scenarios is that the scope of societal risk grows over time.

Many mechanisms like climate change, scarcity of raw materials, the introduction of nano technologies, and the proliferation of cyberspace lifestyles generate or enable new risks but seldom lead to the radical removal of old ones. Increasing complexity and interdependence make the networks of higher order effects of an incident harder to foresee and comprehend. While the mixture of trends and events may differ dramatically between plausible futures, only few risks and challenges are likely to become completely irrelevant.

It turned out that ESRIF members differed in their reactions to this finding. With a reasonable simplification it is possible to distinguish between two main positions.

The first view is that if a risk is real, sooner or later it will manifest itself. Therefore, the key aspect of major risks is the magnitude of their consequences, their future likelihood is difficult to assess and, at least according to some, also irrelevant. Therefore in principle security solutions must be put in place for all real risks of major magnitude, to disallow them by design, intercept them ('incident prevention' as opposed to 'root-cause prevention', which is of limited relevance per this view) or to reduce their consequences – often referred to as resilience. Combining this with the growing panorama of risk one is led to fear that an ever-increasing share of our wealth would have to be expended on security – directly and indirectly, e.g., due to time delays caused by security screening. This can be called a consequence-oriented view.

An alternative view can be understood departing from the observation that societies differ greatly with regard to the levels of, e.g., serious violent crime even though this phenomenon exists in essentially all societies. In line with this the general character of scenarios M and W as 'malign' and G and N as 'benign' comes very strongly across in our work with the other WGs. The insight from this comparison can be expressed such that security at societal level is no zero-sum game. Societies in the world differ with regard to the levels of trust and social cohesion, and, as a consequence, of real and perceived security. Per this view it is natural to base security decisions on both magnitude and likelihood. Then there is a security dividend for high-trust societies that do not have to spend so much on perimeter defences and intervention forces: Even if the scope of risk increases, the combined impact may still go down. Thus here investing[10] in 'root-cause prevention' can be a very viable alternative to 'incident prevention', resilience, and crisis management. At a more day-to-day level per this view it is natural to make security operations intelligence-led, varying, e.g., levels of access controls with levels of assessed threat and risk. According to a standard definition of risk as being a combined measure of likelihood and consequence this view can be labelled risk-oriented. The most well-known technical approach here is of course probabilistic risk assessment (PRA), using the statistical expectation of the consequences as the composite measure.

It is possible to carve out two radically opposed positions based on the discussion above. Our main assertion is that the most compelling challenge lies in developing intermediate positions between the two views. But as a background to this, in Box 1 we do precisely such carving out of the extremes.

Box 1: A discussion of consequence vs. risk oriented views in relation to ESRIF's key messages
We start with 'societal resilience' – or perhaps better 'human' to stress which aspect we are after. From this vantage point – and with the benefit of a long-term perspective – the risk-oriented view suggests reducing fundamental causes of risks and threats ('root cause prevention'): for example, less social exclusion in Europe is likely to lead to less violent radicalisation and hence reduced risks for home-grown terrorism. The consequence-oriented view may also lead to proposals for increasing trust and social cohesion, but here the focus is typically to prepare people to better handle and reduce consequences of, e.g., a terrorist attack in preparation or being perpetrated. While this is no irrelevant concern for the risk-oriented view either, the two views in pure form are likely to lead to different results on the importance of striving for inclusiveness also of marginalised groups in building cohesion.
In terms of technology the consequence-oriented view stresses innovation and a flexible system-of-systems approach ('systematic approach to capability development') to be able to satisfy the ever increasing scope of security demands without running out of reasonable economic bounds. The risk-oriented view may lead to similar approaches to flexibility – but here more to enable intelligence-led operations of security systems, i.e. smoothly

10 By 'investment' we mean decisions that are costly to implement and/or revoke, In addition to, e.g., equipment this can also apply to organisation and legislation. Research and innovation involve many investment decisions of this nature under 'broad' (or 'deep' – terminology differs) uncertainty.

adapting security to the spectrum of risk as it evolves over time[11].
Similar analyses can, more of less, be made for the other key messages to the effect that they are robust in the sense of being applicable to both perspectives. At a more detailed level, however, the precise interpretation of the key messages tends to differ according to view.
At the level of what exact portfolio of security measures to invest in, the difference between the two types of view is likely to be even more pronounced. Furthermore under the risk-oriented view different context scenario will lead to different portfolios of measures being optimal, hence giving rise to multi-period investment planning problems.

The observations in Box 1 are indicative of the fact that even the types of analytic approaches to inform security investment decisions differ between the views.

The risk-oriented approach in its most extreme form has a well-developed probabilistic risk analysis methodology. This makes many problems, e.g., various types of aggregation, quantitatively tractable, which under other approaches must be analysed in a more judgemental fashion. This is true for both investment and operational decision-making.

The consequence-oriented approach, arguably, has time-honoured safety engineering practices like safety factors and margins, as well as the traditional scenario-based approach to defence planning. More recently the precautionary principle has been developed in the environmental policy area.

But in addition to being less analytically tractable these approaches run into even more real problems when facing budget constraints that forbid investments sufficient for dealing with all conceivable scenarios.

The shortcomings of the consequence-oriented approach are a problem since some types of security investment problems are hard to properly appreciate within the probabilistic framework of the risk-oriented approach: situations where things like very long time-spans, very 'broad' (some say 'deep') uncertainty, rare but dramatic events, or antagonistic behaviour need to be considered.

As already foreshadowed above our analysis suggests the need to develop approaches intermediate to the extreme consequence oriented approach and the extreme probabilistic risk assessment – both for professional analysis and public debate. Therefore we propose a development based on the above-mentioned precautionary principle in the environmental domain. However the environmental principle deals with another type of issue, viz. whether or not to undertake human interventions. In security we are instead dealing with countering 'interventions' from external actors (including Nature). Yet – in line with the consequence-oriented view – a straightforward extension of the precautionary principle could be argued for to the effect that if a serious enough case can be made for a risk having the potential to cause severe or irreversible harm to the public or to the environment, then it should be considered in security policy, e.g. in decisions on capability development or legislation. One problem with this, as already commented, is the risk for excessive claims on limited resources[12].

In response to this WG5 has developed a 'balanced precautionary principle'. This combines the systematic scenario-based approach to defining priorities with an all-hazards approach by requiring the scenarios used in priority-setting to represent the whole space of risks in an unbiased way (cf. the concept of 'representativity' in Section 5.4) – it is not practically feasible to include literally all hazards, but all broad types of hazards should be considered. And a decision to prioritise some extremely unlikely types of insecurity at the expense of others should be fully transparent

11 Arguably (in particular governmental) security services should be more willing to pay for flexibility and adaptability than most other actors, since they form a final defence line and are expected to be able to handle precisely those problems that no-one else is able to handle. While a normal company can always say that this particular demand is too marginal to cater to, security services are not really in the position to make that choice.

12 Another problem worth mentioning, which is however a common feature of a precautionary principle and PRA applied to antagonistic insecurity, has to do infringements on civil liberties. Without special restrictions in this regard, both the precautionary principle and PRA are likely sometimes to suggest such infringements on bare suspicion.

in the decision-making process. Probability estimates of risks should be taken into consideration when appropriate, but even when this is possible it does not automatically mean that the specific weighing together of consequence and likelihood of PRA should be applied.

The balanced precautionary principle requires an analytic paradigm that fuses the broad scanning and participatory aspects of foresight with the analytic versatility of PRA. We will develop that line of thinking under the heading of Strategic foresight and risk analysis. Strategic here refers to 'investment' decisions as defined above[13]. This is very much in line with the foresight tradition and with how WG5 has understood its remit. This does not exclude, however, that similar approaches fusing consequence- and risk-oriented views may be applicable also to the tactical role of risk assessment in intelligence-led operations.

Identifying knowledge and competence gaps in strategic foresight and risk analysis

Foresight, understood along the lines of the definition in Section 5.2, has not yet been widely used in the context of security. However, scenario thinking is not uncommon in this context, and it actually has one of its roots in defence research and analysis. In the 'balanced precautionary principle' developed above scenarios is a necessary component.

But whereas 'situational scenarios' as extrapolations of current threats are quite common, the use of 'context scenarios', i.e. of scenarios exploring different future contexts within which new and qualitatively different security threats could emerge, is a more novel development.

The foresight tradition that builds on the so-called five 'C's': Communication between different actor and stakeholder groups, Concentration on the (mid- to long-term) future, Consensus-orientation, Coordination of the behaviour of different actors, and Commitment of participants to implement the insights gained in the process, promises to be very relevant to current debates on the future of security and security research in Europe for a number of reasons:

- The growing recognition that security needs to be understood in a much broader sense than in the past (e.g. in terms of societal or comprehensive security) equally broadens the range of stakeholders likely to be affected by any action taken in this regard.

- As a consequence, there is little consensus on what (European) security is and what it should be, what its dimensions and priorities are. It is a contentious concept driven by both technological and societal developments, and closely related to important economic interests.

- Looking at security from a European perspective requires taking into account the matters of diversity as well as the principle of subsidiarity in order to achieve a productive division of labour with Member States, regional and local competencies. It thus opens up additional arenas for debating and shaping the future.

- And finally, with the prominence acquired by rather unexpected threats to security (terrorism, critical infrastructures, crises, etc.) the necessity to provide a frame for thinking the unthinkable has been accentuated. It requires moving well beyond the extrapolation of current trends and exploiting unknown territory.

The current capabilities and methods in foresight are quite powerful, but have been developed in a different context than security. The well-established analytical paradigm in security is, as discussed above, probabilistic risk assessment. As indicated by the 'balanced precautionary principle' there is great scope for a fusion of foresight and strategic risk analysis, i.e. risk analysis as applied to strategic problems like investment decisions. Here the more embryonic discipline of security economics is also a player.

13 See footnote 10.

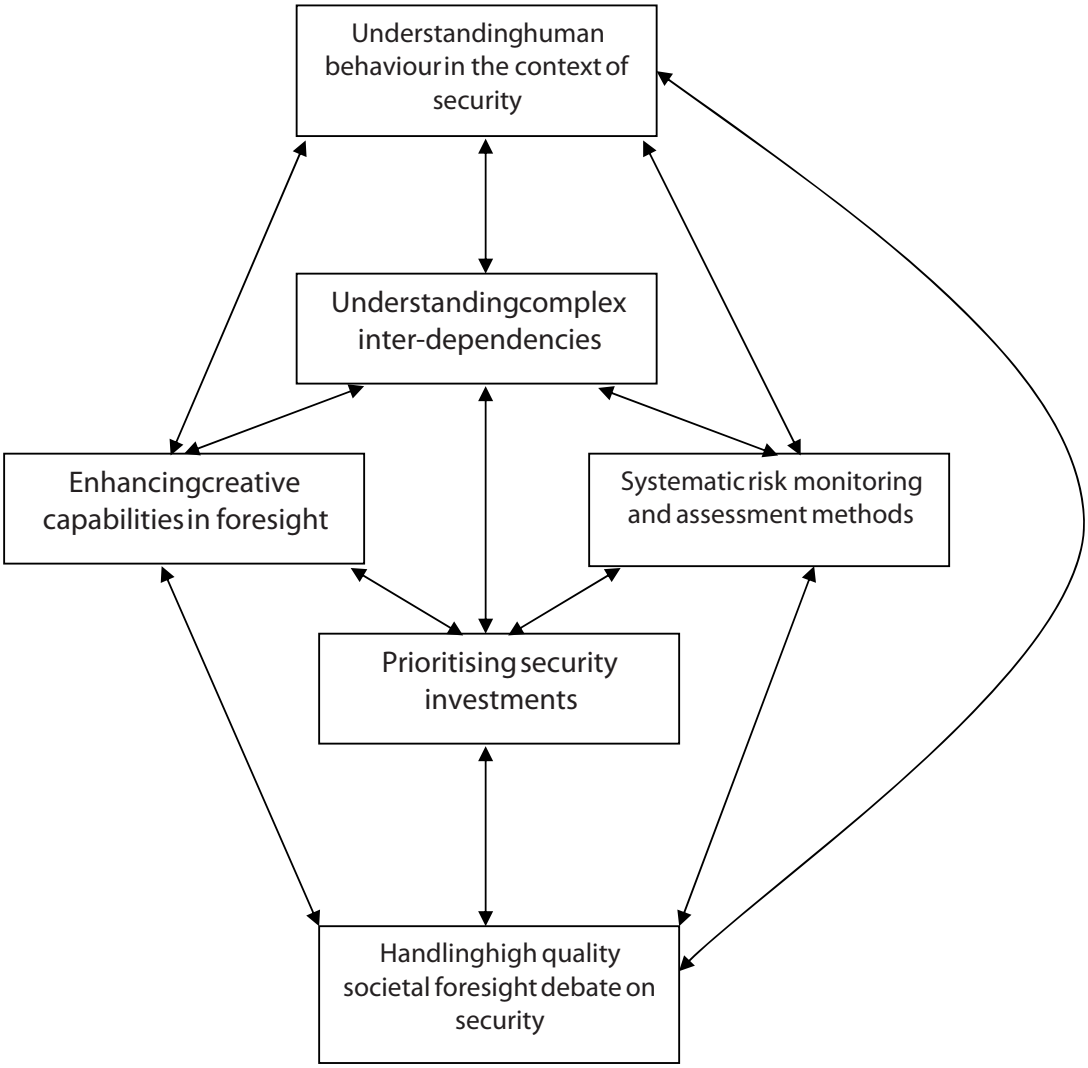


Figure 1. Interrelationsships among research priority areas

In order to establish foresight-based reasoning in security, a number of shortcomings need to be overcome:

- It still represents a major difficulty to fully grasp and model the interplay of human behaviour with new scientific and technological opportunities, both in terms of generating new threat potentials and in terms of new preventive or reactive measures.
- Creativity is an essential pre-requisite for imagining future context scenarios and mission scenarios, but it is difficult to cultivate and mobilize.
- The monitoring and assessment of threats and options is a challenging task, in particular in view of the diversity and the lack of consensus about the goals and objectives against which to assess them, e.g. against the dimensions of a European concept of security.
- As a pre-requisite for conducting systematic risk assessment, it is essential to better understand the complex interdependencies of an increasingly broad range of factors of influence.
- While participatory cultures differ largely across Europe, security is an area that tends to have a rather limited tradition of broader societal debate. With the broadening of the security concept, however, this seems to be an important component.
- However, independently of the specific participatory cultures, there is a need to make the pros and cons of potential alternatives for security investment (broadly understood) transparent in order to be able to establish priorities in an informed way.

The interlinkages between these knowledge and competence domains are outlined in Figure 1. The need to understand consequence vs. risk orientation as a continuum of perspectives outlined above should be seen as a cross-cutting focus area involving all the above domains.

5.6 Research needs and priorities

This section explains the research needs and priorities related to strategic foresight and risk analysis. These needs are based on the knowledge and competence gaps identified above and are discussed under the interrelated 6 sub-categories presented in figure 1.

Understanding and modelling complex inter-dependencies.
Security problems typically have complex interdependencies, inducing big risks for unintended consequences. This needs to be considered in decision-making.

- Many approaches to modelling complex inter-dependencies exist but a lack of consolidation and knowledge accumulation leads to a tendency of reinventing the wheel.
- There is need for systematic evaluation of approaches leading to consolidation of methods to model complexity and interdependencies between sectors and synergies between security measures incl. risks for counterproductive effects.
- A key aspect is the methods' ability to support effective interfacing with decision-makers and experts.

Systematic risk monitoring and assessment method.
There is limited ability to recognise 'weak signals', either with respect to emerging risks or with respect to possible solutions/technologies; to identify early on potential areas of conflict and problems; as well as for dealing with them on the public agenda. Progress can be made by improving

- Monitoring and early warning of potential security problems and solutions ('technology watch')
- The robustness of methods and tools for risk monitoring and assessment
- The understanding of the use of intelligence in the operation of security solutions; and
- This may be supported at a more technical level by development of multilingual semantic analysis systems

Prioritising security investments.
Security analysis requires the simultaneous application of all the 'current capabilities' (i.e. tools for projecting both i) potential uncertainty related to alternative futures and ii) current insecurities likely to prevail in the future, to the present day investment decisions). This requires

- Development of architecture (methods and approaches) for prioritising security investments
- New key capabilities bridging extant ones
- Human factors/user interface issues
- Case-oriented empirical research on decision-making in the face of insecurity

Handling high-quality societal foresight debate on security.
There is lack of ability to deal with future deep uncertainty; and need for translating strategic insights/concepts into R&D or investment priorities. No mature security specific communities are available; there is a short term focus of policymakers; and a lack of common vision and understanding of future threats to security interests. This calls for

- Foster shared understanding of long-term security issues in European policy communities (content)
- A shared conceptual framework for security policy writ large among European decision-making and decision-supporting communities; embed sound foresight and risk analysis practices in decision-making
- Develop strategies for sound foresight and risk analysis practices to affect public perceptions of insecurity: processes (process)
- Improve understanding the of interdependencies between the internal and the external dimensions of security and defence issues

Enhancing creative capabilities in foresight.
The potential of ICT is not yet exploited, e.g. virtual reality tools, etc. More sophisticated methodologies are needed to explore future worlds in a systematic manner. Aspects include:

- Advancement of scenario methodology as an essential tool for enabling and organising creativity
- Development of cooperative ICT tools to facilitate deliberation and creative collaboration within distributed teams
- Development of creativity-enhancing methods and tools

Understanding human behaviour (individual and group) in the context of security.
The impacts of interventions in interdependent sets of root causes can be captured at a very abstract and general level only. Major threats associated with emerging technologies reside in the – often unexpected - use that can be made of them. Aspects include:

- Development of an operational concept of societal resilience
- Improve understanding on ways of affecting 'root causes' of insecurity (e.g. violent radicalisation)
- Understand Human-System Integration aspects of the operation of security solutions
- Investigate malevolent uses of emerging technologies from an inter-disciplinary perspective

5.7 Conclusions

The work in ESRIF's Integration Team meant that the eleven WGs came together to develop a joint perspective on ESRIF's overall mandate. The common part I elements are typically such that they have their roots in several of the WGs and in many cases the concrete form of the idea has emerged via the Integration Team process in a way that makes the final product relatively far removed from all WGs. Still it is possible to say something about which of the various categories of ESRIF statements have the strongest WG5 links. Needless to say we are in no case claiming exclusiveness here.

Of the **key recommendations** Societal resilience (not least the social cohesion aspect with its ability to prevent root causes of crime and terrorism) and A systematic approach to capability development have a particularly strong WG5 pedigree. The long term perspective makes investment in resilience (which also includes Trust and Security by design) a relevant option, and the increasing scope and complexity of insecurity identified by WG5 made a more systematic approach to security investment a necessity in order to avoid excessive cost.

Of the **ESRIA areas** particular WG5 relevance applies for New technologies, new threats and Informed Decision Making, where the methodology-oriented research agenda for strategic foresight and risk analysis resides.

As for the chapter on **ESRIA implementation** features of specific WG5 interest include the interest in the emergence of a joint European security culture (under Security Governance at EU level). Also the idea of Exploiting knowledge synergies is very much in line with the key recommendation on a systematic approach.

Of the **ESRIF Recommedations,** finally, 5. A holistic approach and 6. The globally inter-related nature of security are the ones most reflective of WG5's work.

6. Working Group: CBRN

6.1 Introduction

Working Group 6 (WG6) covers the area of chemical, biological, radiological and nuclear (CBRN) threats. CBRN is a security challenge area which is exemplary for incidents with a relatively low probability of occurrence, yet having a high impact on those directly on the receiving end and on society as a whole. Although WG6 is considered to focus mainly on technology, the very specific threat and disruptive consequences of CBRN necessitate a multi-disciplinary approach. The CBRN working group has obvious interfaces to working groups 1, 2, 3, and 4 on security of the citizens, security of critical infrastructure, border security, and crisis management, respectively. All these missions have to deal with the entire threat spectrum, including the high-violence end partly reflected by CBRN.

The working group assessed the foreseeable threat to Europe posed by CBRN weapons on a mid- to long-term perspective. CBRN delivery systems include more or less sophisticated weapons with a high degree of technical complexity, but also improvised low-tech devices. Such unconventional weapons have the potential to create extraordinary harm even posing an existential threat to one or more member states. Based on mid- to long-term projections of both the security threat and the enabling technologies, WG6 outlined a timely security research and innovation strategy to provide civil society with tools to counter the CBRN threat including tools that will limit the proliferation of weapons of mass destruction.

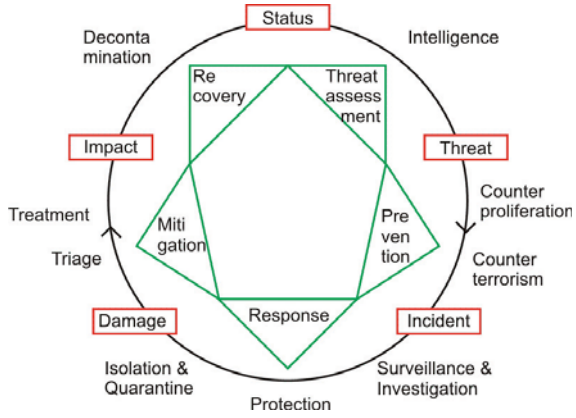


Figure 1: CBRN cycle showing stages, intervention strategies, and tools

The output of WG6 work is a research and innovation agenda for CBRN counterterrorism by bringing together the demand and supply side of CBRN security technology with the aim to strengthen a public/private dialogue in this area and to raise the competitiveness of the European security industry.

The scope of WG6 includes threat assessment, prevention, preparedness, response, mitigation, and recovery (the CBRN security cycle) regarding incidents with chemical, biological, and radiological agents. Nuclear weapons, primarily considered in the sense of a military threat, are not part of the scope of ESRIF. During the ESRIF process, it was decided that the explosives threat area would be covered by WG1. Whereas the focus of the CBRN WG is on deliberate incidents ('acts of man'), related crises due to infectious diseases and chemical or radiological accidents ('acts of God') would be considered, provided sufficient crossover was generated.

The approach adopted by the working group is described below:

- Identification of mid-term threats and challenges taking into account existing security policy decisions, strategies, and plans on the European and national level
- Current and foreseeable primary security challenges, including means and motives of actors (individuals, non-state, and states)
- Identification of long-term threats and challenges mainly building on foresight and scenario techniques as well as linking predictions and expectations about future developments with the focal areas of the ESRIF working groups
- Identification of required capabilities to enhance security within the scope of ESRIF's considerations
- Identification of related research requirements taking into account ongoing and planned programs and work and prioritization of the research needs
- Presentation and communication of the findings

The following reports have been delivered:

- WP1: Present to mid-term CBRN security challenges and capability gaps
- Identifying current and foreseeable primary security challenges, including means and motives of actors (individuals, non-state, and states), in accordance with the CBRN cycle
- Capability gaps, structured according to threat assessment, prevention, response, mitigation, and recovery in relation to CBRN
- WP2: Key Technological Developments enabling CBRN Development and Deployment in the mid- to long-term Perspectives (20 y), as a forecast of dual-use potential
- WP3: CBRN Long-term Security Challenges and Capability Gaps, identifying
- Long-term primary security challenges, including means and motives of actors
- Long-term capability gaps, structured according to threat assessment, prevention, response, mitigation, and recovery
- WP4: Outlining R&D achievements to fill mid- and long-term capability gaps: report with R&D recommendations on how to address long-term security challenges
- WP5: this chapter of the ESRIF end-report: Agenda on R&D achievements: strategy to keep R&D efforts up-to-date with developing security requirements

WG6 consisted of some fifty participants coming from thirteen member states plus representatives from EU and the European Defence Agency. The following stakeholders were represented: governments (14), industry (13), research institutes (17), and end users (6). The actual intensity of the contribution of WG6 participants varied widely. Roughly one-third was very active in attending meetings, participating in discussions, and in writing and reviewing draft reports. Another third of the participants occasionally contributed in some way, whereas the remainder contributed only in a passive way.

Executive Summary

This chapter on chemical, biological, and radiological incidents and accidents, together with the European Security Research & Innovation Agenda (ESRIA), outlines a timely security research and innovation strategy to provide European society with tools to counter the CBRN threat including tools that will limit the proliferation of weapons of mass destruction. The scope of WG6

includes threat assessment, prevention, preparedness, response, mitigation, and recovery (the CBRN security cycle) regarding incidents with chemical, biological, and radiological agents. Nuclear weapons, primarily considered in the sense of a military threat, are not part of the scope of ESRIF.

ESRIF WG6 consisted of some fifty participants. This chapter addresses CBRN related threats and challenges, current capability gaps, and suggested means for closing those gaps through research. A drafting team made up of six core members wrote the chapter aided by subsequent input from other active members, DG JLS, and Europol.

Chemical, biological, and radiological incidents, be they intentional or accidental, remain major threats to Member States for the coming decades. Although the scope of this threat still includes large-scale attacks by States, the pendulum is swinging more toward the use of small, improvised devices by terrorists. Of particular concern is the spread of technical knowledge and capabilities that could be misused in the form of CBRN weapons.

The CBRN security field is characteristic for having a very low occurrence rate but high impact. This implies that hands-on experience for response organizations is relatively low, preparation is not particularly high on operations agenda, and the necessity for building capabilities is not always evident. This does not particularly call for development of dedicated CBRN systems, but rather for seeking to develop and subsequently implement CBRN solutions into and onto existing and developing security systems: an all hazard approach.

Prevention is crucial and should receive particular attention by equipping intelligence agencies and policy makers with improved information analysis tools. Consequence management to overcome CBRN attacks and hoaxes requires networked warning and situational awareness systems with development of more effective and reliable detection and identification capabilities. Other important capability gaps involve broad-spectrum medical countermeasures, less-burdensome physical protection for first responders, and providing safe containment and decontamination procedures that work quickly without giving harmful side effects. Special focus must also be placed on understanding and metrics of psychological and sociological consequences of CBRN incidents.

The analysis performed by ESRIF WG6 reveals that an important number of shortfalls in capabilities exist. During the ESRIF mandate, DG JLS launched its CBRN Action Plan (Communication from the European Commission (EC) to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan), which also deals with a large number of gaps. The action plan focuses primarily on short-term organization and operational issues, while this work is much more R&D focused on longer-term initiatives. WG6 advises the EC to take steps to enhance Europe's ability to overcome CBRN incidents efficiently and cost-effectively both now and in the future.

WG6 recommends that EU establish dedicated CBRN expert-centres to gather and distribute information and experience. Such centres should guide education of EU citizens on how to prepare for and respond to crises. Furthermore, EU should create of a network of laboratories for forensic analysis and agent identification. By doing so, instalment of CBRN expert centres contribute to member state resilience toward CBRN threats.

The EC is recommended to develop methodology and build infrastructure for intensified exchange of sensitive information like threat awareness, dual-use potential of emerging technology and trends in radicalization. The EC should promote a full system-of-systems approach to CBRN(E) counterterrorism following the full CBRN security cycle, including shared situational awareness, a robust interoperable first response. Emphasis should be on integration of this approach into other hazard areas that the security community must cope with.

On an EU level, networks should be established to monitor transport and trade of CBRN agents, raw materials, and related equipment, preferably supported by new or improved international treaties. EU should fund and sustain a security industrial policy to create adaptive and modular solutions that are required for dealing with consequences of rare events. Finally, EU member states are advised to agree on a number of official planning scenarios for states and public organizations to be the basis for security policy, development of doctrines, identification of capabilities and gaps, R&D strategy, and training exercises.

6.2 Threats and challenges

6.2.1 Present to mid-term CBRN security challenges

CBRN threats and challenges to the EU come from both states and non-state actors. These actors will have different motives to develop and potentially use CBRN threat agents against targets within the EU, and have different capabilities to pursue their goals. This threat assessment, on an unclassified basis, will assess the threat to the EU from these actors, taking into consideration some of the most important motives for acquiring these weapons and the estimated capabilities that various actors have for developing, obtaining, and potentially using CBRN weapons.

6.2.1.1 State actors

There are states in the international community that have motives for developing and possessing CBRN weapons. States are the actors with the best capabilities to maintain sophisticated weapons programs. This should be recognized, and so should the fact that control over CBRN weapons in certain states could change quickly because of political unrest, sabotage, natural disaster, etc. Furthermore, it should be recognized that, as the level of technology rises globally, especially in relation to biotechnology, more and more states will have laboratories and production facilities that could potentially be used as stand-by offensive CBRN capabilities. Considerable knowledge and technology could leak from official state institutions to the «free market» due to major changes in regimes and economics of states, thus increasing the threat that state-controlled CBRN capacities could fall into the hands of non-state actors.

On the other hand, states are probably the least likely actors to actually use CBRN weapons towards EU territory, taking into account that states are generally rational actors that will have several constraints against the actual use of CBRN weapons, primarily because the EU is not presently in a conflict situation where such weapons would achieve any worthwhile objective. Nevertheless, the potential threat from states' unconventional weapons programs against the EU does continue to exist.

6.2.1.2 Non-state actors

Non-state actors in this context are typically terrorist organizations. These organizations are present inside and outside the EU and, for organizations primarily based outside the EU, it will often be the case that there is cooperation with persons and/or groups inside EU territory.

It does not seem very likely that non-state actors with traditional political or social motives such as separatism will use CBRN weapons in an attack in the EU. However, it does seem relatively likely that non-state actors motivated by ideas that are more apocalyptic would find it attractive to construct and possibly employ a CBRN weapon. The capability to do so will depend on several factors, such as state sponsorship, scientific qualifications, access to relevant materials, etc. Terrorists can easily obtain particularly toxic chemicals (other than those strictly regulated by the Chemical Weapons Convention).

Use of CBRN agents has a major psychological dimension. In some cases, the objective of a non-state actor could be to simply cause panic and fear. This objective can be achieved by small low-tech attacks that might affect only a limited number of people but still cause an enormous effect on society (the 2001 anthrax letters in the US is one such example). Even hoaxes may very well serve the terrorists' aims in generating panic and disorder.

As societies become ever more resilient and resistant towards conventional terrorist attacks, the motivation for terrorists to spend additional resources on non-conventional (i.e. CBRN) weapons will likely increase. At the same time, the availability of relevant technology will make acquisition easier.

6.2.1.3 Reflections

In relation to non-state actors, there is a relatively high probability that a terrorist attack involving C, B, or R-weapons will take place in Europe over the course of the next 10-20 years. The use of N-weapons is less likely. It is critically important that the EU address this possibility in order to be able to counter and recover from such an attack, should it occur. This should be a multi-faceted approach that includes improvement of traditional preparedness elements such as detection and analysis capabilities,

medical counter-measures, decontamination, and protection. It is also essential to consider how European societies can overcome an attack involving CBRN weapons and still sustain social cohesion and stability.

It is relatively unlikely that a non-EU state will attack the EU using CBRN weapons. However, it should be noted that, due to dual-use technological developments, non-EU states that have engaged in offensive CBRN programs in the past will increasingly possess a stand-by CBRN capability.

6.2.2 CBRN security deployment in the mid- to long-term perspectives (20 years)

This part of the summary analyses key technological development trends that will contribute to the development and deployment of CBRN weapons and materials in the mid- to long-term perspectives, defined as 20 years into the future.

6.2.2.1 Developments in chemical dual-use technology

The ever-increasing range of toxic chemicals and the new processes that enable the synthesis of such chemicals on scales of a few tens of kilograms make it easier to use chemical substances offensively. New methods of manufacture will have an impact on the ability to produce either classical warfare chemicals or other toxic chemicals. Many parts of the chemical industry around the world operate with multipurpose batch facilities, which can readily switch from one product to another. This versatility provides the means to produce a wide variety of chemicals on which the world depends to sustain a modern way of life, but it could also be misdirected to produce chemical warfare agents. In the future, technology now considered advanced will become available to a wider community, including those that have malignant purposes.

A wide range of new reactor technologies including phase-transfer catalysis, microwave reactors, and electrochemistry are worth mentioning. Some of these process technologies can be scaled down to sizes that could be operated inconspicuously outside a normal chemical production setting. The potential offensive use seems obvious, although some difficulties in producing chemical weapon agents in a "backyard" setting still exist.

Small reactors fabricated by technology adapted from the micro-electronics industry can be surprisingly productive when operated continuously. With technologies such as microreactors becoming more widely used in industry, scaling up bench-top production processes is much easier and faster. Biotechnology will steadily increase in importance, especially the manufacture of (complex) organic chemicals. Enzyme-catalyzed reactions as well as reactions in more complex biological media are alternatives to more conventional syntheses.

As concerning means of delivery and dispersal, various technological developments can have implications for more efficient delivery of chemical weapons. Nanotechnology, for example, can be used in many ways, one being the use of particles as carriers of toxic agents, enabling aerosols to be transported easily through protective clothing and/or deep into lungs or skin.

The widespread use of unmanned aerial or ground vehicles indicates the coming of age of remotely piloted vehicle technology. While much of the technology associated with cruise missiles is controlled, the sophistication of what is available commercially is growing rapidly and therefore could get into the hands of terrorists in the future.

Another factor is the development of the binary weapon in which the agent is stored as two precursor chemicals that only need to be combined to form the final lethal product. This reduces the risk that a terrorist must face in the storage and transport of their weapons. It also reduces the threat of accidental exposure upon dispersion of the agent. If the chemical device is engineered correctly, with some sort of time delay, the terrorist could be long gone before the lethal agent is made.

6.2.2.2 Developments in biological dual-use technology

The Biological and Toxic Weapons Convention (BTWC) entered into force in 1975. The disclosure of offensive weapons programs after it entered into force, consisting of highly advanced molecular biology research creating agents with new characteristics for offensive purposes, points to the potential for further misuse of biotechnology.

Today many biotechnological techniques are widely used and spread throughout the scientific community. Although the methodology for modifying most bacteria and viruses to change their characteristics is quite easy depending on which organism

is used, some can still be very difficult to manipulate genetically. Some bacterial and viral traits that may be desirable to alter for malicious purposes include higher transmission and transfection efficiency, increase in morbidity and mortality rate, resistance to drugs, change of immunological characteristics, and pseudotyping (specific targeting like ethnic groups, sex, age, etc.).

Another area of importance for the emerging development within biotechnology is the availability of materials. For about four decades, it has been possible to synthesize stretches of the four nucleotides that are the building blocks of DNA. In 2002, an infectious polio virus was constructed artificially and now it is possible to make nucleotide stretches from 100 to 20000 base pairs routinely, which is considerably larger than the polio virus of 7400. Genomes can thus be constructed by synthesizing nucleotides and this is a much faster method compared to old-fashioned cloning techniques.

In order to synthesize genomes, it is essential to know the desired sequence. Sequencing is now a routine task in many laboratories and previously tedious work has been replaced with the possibility to sequence whole genomes in reasonable time. The time has fallen exponentially and the genomes of viruses as well as bacteria can easily be derived from a database.

Development of dispersal devices will generally follow the development of biological agents since such devices are designed to accommodate the limitations of the agent. Environmentally stable biological agents can, in comparison to labile ones, be dispersed in a more harsh way, and high-quality powders do not require advanced dispersal devices compared to slurries, which do. Coating techniques are generally of concern since they are important in stabilizing and thereby facilitating dispersal of proteins, including possible biological agents. Different particle engineering techniques, including supercritical fluids, spray-drying, dry coating, microencapsulation, nanotechnology, etc., can be combined with molecular biology to create entirely new potential for biological weapons design.

The potential for malicious use of biotechnology is a great concern. However, it should be noted, especially when discussing this threat in combination with non-state actors, all genetic manipulations of existing bacteria and viruses or newly created agents need to be tested in animal models to confirm their efficacy as a biological weapon. This requires substantive infrastructure and resources and is very time-consuming to perform in an optimal manner.

6.2.2.3 Developments in radiological and nuclear dual-use technology

Production of radiological and nuclear material is predominantly carried out on an industrial scale. However, this may change with the utilization of new technologies. For clandestine irradiation of raw material, already existing installations could be used. It is conceivable to irradiate such isotopes in a reactor, especially in a research reactor. Neutron generators are getting smaller and cheaper and may be used in parallel to their actual purpose. The same holds for accelerators, particularly compact cyclotrons, many of which are commonly used in hospitals. These compact cyclotrons will get even smaller, easier to operate, and cheaper.

For enrichment, the technique of Atomic Laser Isotope Separation should be monitored. It will be possible to achieve high enrichment with just a few steps. Another aspiring technique may be the use of nanosieves (a new type of membrane with molecular-sized pores) for enrichment, as well as for separation. Both methods are extremely selective, producing material nearly without any perturbing neighbour isotopes. It might be possible for a terrorist organization to operate such equipment in a relatively small-sized laboratory, which will be nearly impossible to detect. Although this is theoretically possible, the resources required to scale up to produce meaningful quantities of nuclear materials is probably beyond what terrorist organizations have at their disposal. All developments of high-yield separation bear the possibility of separating material that could be used for nuclear weapons.

For processing burned (used) fuel rods, modern separation systems with remotely controlled machines and appropriate hot cells will be available worldwide. For all deliberations, it should be kept in mind that the necessary quantity of fissionable material for a nuclear device is relatively small. Over time, there will be reduced investments and less manpower necessary for production of fissionable material on a small-scale basis.

New techniques for aerosol technology may be used for dispersion of radioactive or nuclear material. Nanoparticle research may lead to a special powder that easily enables aerosols to be absorbed after inhalation. In addition, these techniques could

simplify the dissolution of radioactive or nuclear material for utilization by dispersal devices. The development of unmanned ground and aerial vehicles, autonomously as well as remotely controlled, will lead to smaller and universal vehicles. Additionally, the number of ballistic missiles and countries able to produce them are constantly growing.

6.2.2.4 Reflections

Technological progress in chemistry, biotechnology, and the radiological/nuclear field take place at a very rapid pace. These developments are generally of a desirable and legitimate character benefitting the daily lives of people. However, a downside to these technological developments is they make it easier to develop, acquire, and deliver a CBRN weapon. In other words, CBRN-weapons-enabling technologies are present in more and more states globally and at more advanced levels. This should be clearly recognized in order to counter undesirable effects of this otherwise positive technological progress.

6.3 Capabilities and gaps

Based on the threat assessment and security challenges, this section outlines the main CBRN capability gaps in the coming decades. It is essential to consider how European societies can overcome an attack involving CBRN weapons, while maintaining social cohesion and stability, and addressing the psychological dimension of a post-attack situation in terms of assisting affected persons.

The major security objectives as described in the CBRN cycle (threat assessment, prevention, preparation, response, mitigation, and recovery) establish a foundation for enabling protection of EU member states against CBRN threats. It requires gathering, fusing, and analyzing all source information and disseminating timely and actionable threat information. It involves calling attention to threats that require immediate, enhanced, or sustained action that enables authorities to make better decisions. Defeating the threat requires a high level of cooperation among intelligence, law enforcement, defence, public health, and scientific communities conducted through a network of cross-community and cross-national partnerships.

Due to the complexity of the CBRN threat, a comprehensive and adaptive risk management strategy in the field of CBRN is necessary. In this context, the approach should be more focused on managing risks rather than a very tough counter proliferation agenda in order not to frustrate legitimate and desirable technology development.

This risk management strategy should take all stages of management of a CBRN incident into consideration, including the intentions of actors for possibly using a CBRN weapon and analysis of the likelihood and potential consequences of a CBRN attack. It should be multi-faceted and integrate into generic security measures. It must include traditional preparedness elements, but also measures and considerations on how Europe could overcome a CBRN attack and still sustain social cohesion and stability. The following sections primarily follow the CBRN security cycle and address crosscutting as well as specific C-B-R/N issues, where applicable.

6.3.1 CBRN Integral Threat Assessment

Counteracting CBRN terrorism requires in-depth insight of intentions and capabilities of potential actors. The majority of efforts of threat assessment are the responsibility of the intelligence community. It needs to be stressed that ESRIF WG6 did not deal specifically with actor intentions or information on new religious, nationalist, and political developments. However, within the scope of ESRIF a number of capabilities has been identified which are needed to supply the intelligence community with the proper knowledge base, tools, and technical information to improve the work they need to do. In addition, there is a need for interfacing and collaborating with the research and intelligence communities. Data systems are needed for better transfer from the intelligence community into the non-classified industrial area as well as transfer of knowledge of emerging technologies from research arenas into the intelligence services.

6.3.1.1 Actor analysis and threat awareness

Technology can help evaluate foreseeable trends in CBRN threats. Current knowledge of potential actors' technical capabilities is based on subjective expert opinions, which is, however, necessary to be able to assess, from a technological perspective, the probability that a certain attack will be successful. This is not to be confused with the probability that a certain type of attack takes place, but is rather a measure of technical feasibility and likely effects.

Moreover, surveillance tools for detection of offensive capacity need to be in place; emphasis should be on emerging technologies with dual-use potential, identifying important, unique, and detectable indicators for CBRN terrorism. This also involves mapping disincentives and thresholds for choosing CBRN agents as violent means.

A related capability gap is the (knowledge of) awareness of stakeholders about the threat. This includes the need for national and international information exchange, e.g. sharing of scenarios, reports, incident database, and harmonisation of import/export regulations. Development of advanced modelling and simulation tools in the form of so-called "serious games" showing the potential of real-world CBRN-related scenarios would be extremely useful for both insight and training.

6.3.1.2 Generic methods for risk assessment and information management

There is a need for generic methods for risk assessment and adaptive information management on newer, mostly small-scale, threats. In this sense, ESRIF WG6 identified capability gaps on integration of information coming out of detection networks, intelligence, and dispersion modelling. Integrated information (CBRN situational awareness) must be fed into decision support tools and integrated into command and control.

This implies a need for modelling capabilities for attack simulation and intervention planning taking place at numerous incident sites (in/out-door, urban, sub-urban, rural, industrial, infrastructure). Related gaps are on forecasting of incident propagation; health evolvement of exposed persons; dispersion modelling tools in urban environments and complicated assets such as airports, harbours, and big events; and development of 3D maps of high-level targets.

On a higher abstraction level there is a need to develop tools to calculate the impact (also higher order) of CBRN attack employing metrics other than casualties (e.g. psychosocial impact or economical impact).

6.3.1.3 Intelligent database analysis and sharing capabilities

Improvement of risk management requires that EU member states agree on a number of official planning scenarios to be the basis for further planning and policy. As part of this, identification of agents that have the potential to be used for malicious purposes as well as the consequences of such incidents is required. For this purpose, intelligent databases of agents and of delivery means must be designed. These should be capable of identifying and analyzing agents and assessing their potential for being misused. Based on yet-to-be-established priorities, qualitative and quantitative agent hazard characterization must be performed. Descriptions of chemical, biological, and radioactive sources used in normal operations (e.g. industry, medicine, research) should contain, as a minimum, the following characteristics: physical-chemical composition, intended use, risk classification, and images. This implies the need to be able to synthesize or culture highly toxic or highly virulent agent, to handle and characterize agents and to investigate and predict toxicity and virulence. All activities associated with establishing these characteristics must be subject to strict security guidelines.

Vulnerability assessments should be conducted based on the development of approved scenarios in order to assess the state of preparedness and protection to low-impact incidents, which may nevertheless cause significant psychological, health, and economic effects. Further, sets of focused scenarios at EU level, including events with cross-border effects and prediction of agent distribution of a variety of CBRN agents are needed. General risks and vulnerabilities should be communicated to all involved in planning and response and not kept in the hands of security officials only.

6.3.2 Prevention

6.3.2.1 Multinational counter-proliferative organisational measures

The best defence against CBRN terrorist threats, next to eliminating the cause, is to prevent extremists from having the availability to CBRN agents and knowledge. An ideal future within the multinational arena would be to envision legally binding global treaties as well as agreements on export control of sensitive technologies, materials, and knowledge. This, together with nationally implemented non-proliferation measures, would create a solid base for preventing access to CBRN materials and knowledge. The importance of international treaties for limiting proliferation of materials and knowledge to non-state actors should not be under-estimated.

Identified capability gaps are the requirements for taking a multinational approach towards increased security of CBRN-related infrastructure, not only by states negotiating international treaties but also involving industry, academia, and research institutes. A global awareness of the dual-use potential associated with the CBRN area needs to be achieved in order to reduce proliferation of dual-use knowledge, equipment, and materials from R&D institutions, industry, and hospitals. In addition, a global commitment is needed for controlling and facilitating implementation and global adherence to CBRN regulations and international conventions.

The fast speed of new technical development within the civilian R&D community demands an ability to perform technical assessments, focusing on the dual-use dilemma. A scientific advisory board, preferably governed by an international treaty, could potentially achieve this, which, in turn, would lead to better and more flexible coverage of emerging threats in future CBRN-related treaties. One such issue of concern is the possible misuse of non-lethal weapons where support by treaties and diplomacy is needed.

6.3.2.2 Counter-measures and limitation of terrorist capabilities

Enhancing border and domestic security operations is prerequisite for the prevention of CBRN attacks by non-state actors. Terrorist threats can be mitigated by preventing extremists from entering EU territory or illicitly transporting materials, components, and devices across our borders. Within EU borders unlawful access to materials and attempts to acquire, transport, and use these materials must be prevented. Ideally, the aim of EU would be to have full control of CBRN material and precursors as well as delivery systems to prevent illegitimate uses of the knowledge and materials.

Capability gaps that need to be addressed in this respect include improved border control of goods and people. Already there are a significant number of initiatives underway in the first pillar context to ensure an effective common approach to risk analysis and management by customs for security and safety purposes. A strong international cooperation is also needed to combat illicit trafficking and terrorist use of CBRN material by dissemination of information between national authorities and regional and international organizations. Facility security and security checks of persons working with sensitive CBRN issues need to be developed. Additionally, technology for identification of suspected illegal CBRN laboratories and production facilities are lacking today.

6.3.3 Preparedness

Preparedness covers many aspects but the main capability gaps identified are in the area of measures that should be in place to monitor the possible illegal attempt to use CBRN material for terrorism purposes and intercept it before the attack occurs. In this respect, there is a major difference between chemical and biological from one side and radiological/nuclear on the other side. For C and B current detection techniques require an interaction with the material, so there is a clear need to develop a viable standoff detection capability. A major problem in the chemical field derives from the broad spectrum of chemical agents to be detected. In the biological field, the challenges derive from the large variety of agents and the long time required for their identification.

On the contrary, techniques for the detection of R/N materials are quite mature and widely deployed, based on a wide variety of instruments: fixed portals to monitor transit of people/vehicles/goods, transportable detectors installed on land/air carriers, hand-held equipment for manned inspection. In this case, the capability gaps are mostly related to metrological limitations of current technology. For example: large efficiency detectors generally have poor discrimination and raise a large quantity of innocent alarms, nuclear material can be easily shielded or masked with other legal radioactive material, R/N material is difficult to detect in large volumes, and the impossibility of stand-off detection of alpha radiation.

For B and C an alternate possibility would be to replace the detection of material/agents with the detection of their effects/properties: toxicity in the case of chemical or virulence for biological. For chemical toxicity detection, arrays of representative toxicological end-points should be identified and transformed into detectable signals. For detection of virulence, the first steps to take would be to define proper virulence factors and derive a representative selection. Next efforts should then be aimed at design of measurement concepts. Such generic principles are not applicable to R/N because detection of radiation does not point necessarily to a threat/illegal material due to the large variety of innocent/legal materials containing radioactivity. Another gap specific for a biological incident is the lack of mobile real-time detection equipment.

Since it is quite evident that there is no single detection technology for all threats, integration and networking of sensors will play an important role in all scanning equipment deployed at borders or other transit points. Furthermore, inspection equipment will have to integrate all sensors both from the hardware side and from the point of view of signal analysis (data correlation, data fusion algorithms, imaging and 3-D reconstruction techniques, artificial intelligence). Another important avenue of improvement could come from the development of specific detection architectures (for airports, seaports, border checkpoints). For the use of first responders, the development of multipurpose detectors is highly important, as well as detectors that are embedded in daily-use equipment.

Development of new instrumentation will require the parallel development of international standardization and, by consequence, testing and validation procedures.

Since preparedness is an issue with a strong technical component, a key element will be training, including practical emergency exercises. Most of the people involved in security controls at crucial points (borders, main transport nodal points, buildings of high institutional/religious/cultural importance, places hosting major public events, etc.) do not have a special education in the field of CBRN hazards. Nor do most people involved in reaction activities in response to a terrorist attack (fire brigades, rescue teams, police, medical staff, crisis management teams, etc.). Dedicated training for all these categories of people should be prepared and carried out in the fields of awareness, detection, protection, response, and mitigation/remediation. Establishing specialized dedicated training centres at the European international level will be extremely beneficial. Moreover, politicians and public administration managers should be made aware of the need to set up proper security measures and available means and techniques. Finally, the public should be adequately informed to complete the goal of building a comprehensive "security culture."

6.3.4 Response

CBRN incident management is difficult due to many adverse factors. First responders have at best a theoretical experience with handling such events, as they fortunately do not happen on a regular basis. This makes it necessary to train first responders, but also all other involved authorities, adequately to these relatively rare incidents. Besides their direct impact on the physical health of affected persons, CBRN agents pose a special challenge to manage their psychological effects on the population. The terror caused by the application of CBRN agents may outweigh the physical damage by far. A timely, competent, and reliable communication by first responders and authorities is crucial in the management of a CBRN crisis.

In addition, the technical means of the first responders to handle an incident are currently far from ideal. Personal Protective Equipment (PPE) is heavy and bulky and is a physiological burden that interferes with the operational duties of first responders. In addition, PPE is not standardized or universal.

Not having the capability to detect and identify CBRN agents without the aid of analytical devices causes further impediment. An ideal instrument would identify all relevant agents instantaneously at the site of the incident, have a high sensitivity, produce no false positive results, and be easy to operate. Currently available detection and identification systems are mostly characterized by a narrow spectrum of detectable agents and an insufficient sensitivity to measure toxic / contagious amounts of agent. Moreover, they do produce false positive results. To compensate these lacks, the operators need a very good knowledge of the agents and the devices used to identify them. Operators have to be particularly knowledgeable about the limitations of tools they are using to avoid producing wrong results.

The degree or dose of contamination of persons should also be diagnosed on-site. This would expedite triage and allow medical staff to begin treatment as early as possible.

Easy-to-use tools must be developed to provide enhanced situational awareness, needed for prioritizing resources, developing response plans, reducing vulnerabilities, and mitigating consequences. These instruments should have integrated communication systems to allow instantaneous support by off-site experts, e.g. in the interpretation of results. All decision makers should be kept informed.

CBRN incidents are not just local events. To manage such an event successfully, a fast and efficient co-operation of many different agencies at the local, national, and often international level is crucial. To achieve this, first responders need to adopt a joint doctrine

having clear Standard Operating Procedures. There should be standard protocols for triage, decontamination, transport of victims, tracing and tracking of evacuees and patients, forensics, and so on. Sufficient practice of these protocols and procedures in the form of universal, multi-agency trainings, drills, and simulations would minimize chaos during a real incident.

Due to the possible very large impact of CBRN incidents, first responders will need national and possibly even international support. Therefore, these joint doctrines and SOPs must be adopted at the European level. Furthermore, equipment and tests should be standardized.

Sampling and identification methods should be improved and include proper forensic aspects. A network of certified testing laboratories should be established capable of forensic level analysis complementary and in co-operation with proper national traditional forensic laboratories. In addition, there is a need for standardized protocols involving not only sampling and identification procedures but also standards for transport of samples. The approach applied by the Chemical Weapons Convention community could be used as a model.

6.3.5 Mitigation

In order to achieve societal resilience the preparedness for the medical treatment before and after a CBRN attack is crucial. The ideal future would consist of a society where generic treatments of the exposed were present; a standard that in and of itself would be counteractive for potential terrorists since the pure knowledge of a very limited outcome of an attack could have a restraining effect. The CBRN defence arena has to deal with agents and diseases that are not always covered by regular drug development, which means that there are needs for additional efforts by society.

More efficacious medical countermeasures with improved compliance and safety profiles need to be developed. Test protocols need to be standardized. Preferably, new medications will have long shelf lives, not require special storage, and be easy to administer.

Within the biological area the development of new vaccines are very expensive and time consuming. Vaccines also need to be administered in advance to give optimal protection which stresses the importance of also developing effective and, preferably, generic therapeutics.

Identified capability gaps highlight the very limited access of safe and effective medical countermeasures for treating patients suffering from disease due to exposure to chemical and biological compounds in the CBRN area.

The problem of multi-resistance is growing so there is a need to develop new broad-spectrum antibacterial and antiviral substances based on new modes of action against pathogens. The necessity for new concepts for vaccine development against novel emerging viral infections similar to influenza is obvious, the optimal being generic vaccines giving protection to many different viral diseases. Development of vaccines against some multi-resistant bacterial pathogens is also required.

During a chemical incident, there could be a need for rapid treatment of large numbers of casualties. Even before the trained "first responders" arrive, non-trained citizens could provide help for themselves and each other. For this reason, research is needed to determine whether all citizens should receive training to provide first aid during a CBRN incident.

6.3.6 Recovery

Full societal recovery after a real CBRN incident could take years or even decades depending on the type and magnitude of the incident and where it takes place. The recovery process can be divided into two distinct categories: 1) recovery of people and 2) decontamination/remediation of buildings, equipment, outdoor surfaces, and contaminated soil and groundwater.

6.3.6.1 Decontamination and remediation

Decontamination and remediation of the impacted area(s) will begin with an assessment of the damage, which could potentially require hundreds or even thousands of samples for lab testing. Incidents involving volatile chemical agents and biological agents that do not survive long might not require decontamination, but long-term monitoring could be necessary. By contrast, non-volatile chemical agents, radiological particles, and some biologicals are extremely persistent and would require thorough decontamination.

Decontamination and remediation needs to be thorough enough to allow for reuse/habitation. Knowing what level of contamination is safe is essential. Measurable cleanliness criteria based on solid scientific data and procedures that can meet those criteria are yet to be established.

Current decontaminants have limitations, do not fully neutralize all agents, and are not completely safe. Strong neutralizers tend to destroy parts of items decontaminated. Some decontaminants have shelf-life or storage issues, some are flammable, and most are not friendly to the environment.

Current technology involving applicators for decontamination operations need to be improved. Lightweight portable decontamination systems would be helpful in certain circumstances. Automated decontamination equipment such as unmanned vehicles would allow recovery teams to work outside of harm's way. Dedicated decontamination teams need to be created, equipped, and trained throughout Europe.

Other capability gaps identified for this phase are the ability to thoroughly decontaminate human remains for transport and burial, decontamination of sensitive equipment and aircraft, finding decontaminants that work against a broad range of toxic industrial materials (TIMs), and disposal of contaminated wastewater and debris.

6.3.6.2 Psychological and social resilience

Europe's societal resilience rests on a combination of people and the social structures in which they live and work. Both can be exposed to risk. The resilience of society will depend on the interlinking of the two, on their mutual trust and confidence, and their actual capacity to support one another.

The immense societal reaction that CBRN incidents cause can be subdivided into layers of effects: 1st tier being effects on health and first responders' actions at the site of the attack, 2nd tier effects on societal functions shortly after and close to the location of the attack, and 3rd tier effects on society as a whole in terms of the colossal damages that will consequently incur both in human life (the so-called psycho-social impact) but also in economics and political stability.

Apart from any physical damage to the population in terms of casualties, high emotional impact and psychological consequences are central aspects of terrorist CBRN attacks. While emergency responders are trained for and accustomed to facing stressful situations, the sheer magnitude of a CBRN event, the ongoing threat (possible multiple attack) and the extreme danger represented by CBRN agents, could reduce the efficiency of first responders due to both acute and post traumatic stress reactions. The public and other services involved in the response are currently generally not at all prepared to face the consequences of CBRN incidents, such as poison, disease, and radiation. In that respect, the effects of CBRN terrorism are believed to be much stronger than the effects of "ordinary" terrorist attacks. The so-called "ripple through society" caused by the initial attack is expected to be much broader, i.e. the amplification factor from tier 1 to tier 2 to tier 3 is bigger for CBRN than for E (explosives).

The psychological reactions might not only affect people near the impact site but also people living far away who were not exposed to the CBRN substance. Indeed, large numbers of persons who feel like they have or might have been contaminated will ask for medical help thereby overloading the medical response system.

Because the probability of a CBRN occurrence is relatively low, not much is known about the role psychosocial mechanisms play. A thorough understanding of those mechanisms seems to be an important gap as it is a key starting point for developing "psychological" therapy.

In order to cope with the higher order effects mentioned above information seems to be a key issue. This concerns education and awareness building prior to the attack and risk communication during and after the attack, focusing on both the first responders as well as the public. Most importantly, citizens must understand that risks need to be known, confronted, and minimised—not avoided. There can be no guaranteed foolproof preventive security system.

The role of the authorities as a reliable source of information is obvious, but the media are also key players. In order to provide the public with accurate, timely information and advice, media members must be considered part of the response mechanism.

Even the people themselves are key players (full-fledged security actors). In order to respond in an effective manner, the public should be informed about the nature of the threat and trained in the precautions they should take beforehand and actions during and immediately after attack. Afterward, both responders and society as a whole may need some kind of emergency psychological support.

6.4 Research & Innovation Priorities

The scope of this section is to outline CBRN R&D achievements needed to fill the mid- and long-term capability gaps, which means that it is strongly oriented towards those capability gaps that can be accomplished through technical means. CBRN is a complex field and not surprisingly, a great number of scientific and technological disciplines need to be addressed to achieve the innovation considered necessary to better manage this security area. As will be clear from the large number of topics summarized below and from the CBRN part of the ESRIA, research areas involve chemistry, (micro- and molecular) biology, (nuclear) physics, information management, social sciences and many others, but most of all integration of all of them.

6.4.1 CBRN integral threat assessment

Development of tools for improved information-gathering, assessment and sharing involves a number of disciplines, such as information technology, chemistry, microbiology, nuclear physics, and psychology.

- Map, through multidiscipline approaches, relevant potential pathways to CBRN terrorism and their unique and specific signatures, sensitive to group dynamics and technological abilities
- Identifying important, unique, and detectable indicators for CBRN-terrorism (including yet unforeseeable ones)
- Structured and effective awareness-raising methodologies for early-warning purposes
- Mapping disincentives/thresholds for choosing CBRN agents as violent means
- Objective/quantitative algorithms
- Intelligent database analyses and sharing capabilities (agents, devices, scenarios)
- Develop cautious awareness-raising dialogue that gains support from civil society, law enforcement, academia, etc., to detect anomalies
- Meta-analysis of the complex threat dilemma and development of new, non-frequentist and non-deterministic analytical methods
- Risk assessment methodology to derive the probability of successful incidents using input from actor profiles, actor capabilities, consequence prediction, probabilities and countermeasure efficacy
- Full CBRN cycle incident modelling and simulation for threat analysis, policy making, planning, decision support, and training (including all relevant administrative and law enforcement authorities)

6.4.2 Prevention

6.4.2.1 Multinational counterproliferative organisational measures

The development on organizational level for multinational counter proliferation is mainly performed by the work coupled to international treaties and export control regimes. However, some research could add extra value. Natural scientists and security policy analysts in collaboration with end users such as diplomats could perform this research.

- Design of toolbox for monitoring and verification of implementation of (new) CBRN treaties
- Development of deterring and norm-enforcing tools and methodologies against illicit use of agents
- Develop methods for safe disposal of radioactive sources
- Develop methods for replacement of potential dual-use materials or equipment (e.g. replace radioactive sources by non-radioactive means)
- Establish methods for assessment of new or unregistered substances by substructures, properties, and molecular simulation according to schedule 1,2,3 of CWC

6.4.2.2 Counterterrorism capabilities

Research to be performed for effective counter-terrorism applications involves experts and scientists within IT-security, physics, microbiology, chemistry, image interpretation, etc. The involvement of end users such as intelligence agencies, police, customs, and actors within the judicial systems is preferable.

- Development of (dynamic and secure) information sharing systems regarding trade and transport of CBRN materials
- Improvement of tracking and tracing of goods including precursors and production equipment
- Development of fast and reliable detectors to monitor large-volume containers for chemical, biological, and radiological materials
- Research of new methods for the signature of covert production facilities by emission, shape, and defining new measurable properties

6.4.3 Preparedness

As already remarked previously, preparedness has a large technological connotation and therefore most of its capability gaps can be tackled and possibly solved through dedicated research and development projects.

6.4.3.1 Chemical incident preparedness:

- Miniature Chemical-Lab: transportable / moveable / portable – the smaller the better; non invasive and non-destructive techniques included
- Passive or active detection/imaging technology for the detection of hazards
- Detection of novel types of agents (e.g. bioregulators, peptides, non-lethal weapons, non-traditional agents)
- Innovative database for the prediction of toxicity by molecular and submolecular properties
- Novel screening system for toxic effects in relevant biological systems (e.g. cell lines) to allow for detection of hazardous effects of threat agents

6.4.3.2 Biological incident preparedness

- Fast, affordable, genome sequencing in combination with immediate comparison to extensive, open, and easily accessible sequence databases that incorporate refined homology search algorithms
- Knowledge base to assess and validate virulence properties of agents with anomalies and unusual genetic properties
- R & D towards detection of suspicious aerosols

- Extended strain collections with a greater variation with respect to diversity and representation of world-wide geographic origin
- Research to estimate population genetic parameters for natural populations of relevant agents

6.4.3.3 Radiological/Nuclear incident preparedness

- Technology to mark radioactive sources with a fingerprint
- High sensitivity/selectivity portal monitors to scan goods with negligible false alarms
- Novel detection technologies (muon radiography, spectroscopic portal monitors, new scintillators, active interrogation, photofission, thermal infrared spectroscopy)
- High-dose-rate linear accelerators for active investigation
- Increased capacity with small mobile detection devices

6.4.3.4 Crosscutting preparedness issues common to all CBRN

- Remote sensing technologies (e.g. satellite surveillance) for stand-off detection
- Harmonisation of testing and validation procedures for new detection equipment
- Training, including development of simulation tools (e.g. scenarios based on virtual reality), role playing games, and practical exercises

6.4.4 Response

- Detection and on-site identification: see 11.4.3
- Micro-systems technology for miniaturization
- Transportable CBRN laboratory
- Development of methods and procedures for forensic sampling and analysis for unknown samples, including transport procedures
- A joint effort for putting together resources for developing and producing a large number of affinity molecules in large quantities
- Research on BW agents, their close neighbours, and natural microbial background as basis for all work in this field
- Establish advanced capabilities to genome sequence database, process and analyze unknown viral and bacterial agents
- Development of multi-purpose, standardized body protections that are encapsulated yet operational over longer periods with increased mobility, communication, and tactile capability
- Breathing systems delivering overpressure in mask and suit without using compressed air
- Design and production of C-resistant materials to be incorporated in light-weight low-burden protective clothing
- Design and production of lighter respiratory protection
- Escape hoods for short-term airways protection of citizens

- Improved COLPRO systems
- Development of operating procedures focusing on the particulars of CBRN threat agents in addition to ordinary chemical, biological, and radiological poisoning (all hazards approach) taking adequate measures to keep a forensic approach and not to destroy evidences during action
- Development of standard protocol for triage, decontamination, and training programs for mass CBRN incidents
- Design of a system for search and rescue, triage, and transport of contaminated victims and tracing and tracking of evacuees and patients (mass casualties and large-scale evacuations)
- Fieldable R/N biodosimetry (or fast post accident dosimetry) and chemical, biological point of care diagnosis

6.4.5 Mitigation: Broad-spectrum medical countermeasures

R&D with the aim to develop new medical treatments after CBR-exposures are mainly performed by advanced researchers within the areas of chemistry, molecular biology, and physics. Involvement of pharmaceutical industries is important as well.

- Research to elucidate molecular mechanisms of infection for development of novel strategies for generic treatment methods with lower selection pressure for development of resistance
- Intensified R&D to understand molecular mechanisms of important viral infections where priorities should be focussed on infections where vaccination is the best option
- Novel R&D approaches for identification of essential host factors common to groups of viruses for recognition of novel targets for drug development (this technology requires novel efficient genetic screening techniques for entire eukaryotic genomes)
- A synthetic biology approach with establishment of toolboxes for rapid engineering of multiple variants of viral particles
- Develop and improve treatments which do not involve antibiotics, preferably group specific treatments (this requires that key virulence factors common to many pathogens need to be identified and evaluated as targets for drug development)
- Antidote activities on stabilization, appropriate coating material and fillers, microencapsulation, and improved logistic systems.
- Development and stockpiling of antitoxins and chemotherapeutics
- Research in other novel approaches for developing medical countermeasures such as proteomics, metabolomics, enzyme-based bioscavengers, oxime-based therapy, etc.
- Research on potential acute and delayed adverse health effects from low-level exposure to nerve agents
- Basic research designed to measure sensitive markers of nerve agent exposure to assure that low-level exposures are not associated with long-term or delayed health effects
- Development of exposure markers for C agents relevant for triage and estimation of actual exposure/uptake/excretion

6.4.6 Recovery

6.4.6.1 Decontamination and remediation

R&D in the field of CBRN decontamination and land remediation requires several different disciplines. Various decontamination systems exploit physics-, chemistry-, and biology-based technologies. Furthermore, researchers and developers in the areas

of chemical, mechanical, civil, environmental, and software engineering are useful. Collaboration between industry, academia, and governmental labs is not uncommon.

- Standardization of decontamination and other recovery procedures including mortuary affairs
- Standardization of methodologies that determine safe contamination levels
- Development of decontamination products to increase potency against all CBRN threats and reduce hazards; that are environmentally safe, reduce resource requirements, and are nonhazardous to sensitive equipment and electronics
- Development and coordination of international test operating procedures for the standardization of efficacy testing for existing and future decontaminants
- Establishment of a database for all decontamination and materials compatibility testing
- Development of self-decontaminating materials and coatings
- Improved contamination simulation algorithms
- Creation of a categorized and prioritized list of TIMs for assistance in developing and testing decontaminants and recovery operation procedures
- Development of easy-to-use lightweight applicators
- Development of automated decontamination equipment such as unmanned vehicles making the recovery process safer
- Creation of and training for dedicated decontamination teams
- Development of better CBRN simulants for both testing and training purposes
- Development of proper disposal plans for contaminated waste water and debris

6.4.6.2 Psychological and social resilience

- Investigation of psychological mechanisms to understand (mass) response to extreme CBRN incidents, also related to other kinds of incidents and accidents (this means, for instance, understanding ethical concerns and addressing psychological issues such as fear)
- Generation of an increased understanding of public communication and education prior to any kind of attack in order to create a more resilient society even in overcoming the stress and trauma related to a relatively low-probability phenomena such as CBRN terrorism
- Investigation of effective means to communicate with the public during a crisis (modern information technology allows individuals to exchange data virtually with the whole world immediately, however, during a crisis, many of the usual means of communications may not be available)
- The development of realistic training procedures and facilities for responders (should include stress resulting from the presence of CBRN hazards, which would require live-agent training facilities where threat scenarios can be played)
- The development of CBRN incident serious gaming products onto real-world scenarios to establish awareness, identify critical elements, and verify research needs

6.5 Recommendations and Conclusions

Although society should continue to try to persuade people to respect one another through diplomatic and social means, there will likely always be those who threaten and use violence as a means to their ends. Because of this unfortunate fact, the community needs to prepare for facing and recovering from awful threats like CBRN. The analysis performed by ESRIF WG6 reveals that an important number of shortfalls in capabilities, from technical, organizational, and societal in nature, must be filled to achieve this goal. The working group advises that the EC take initiatives to efficiently and cost-effectively enhance Europe's ability to overcome CBRN incidents.

WG6 recommends that EU establish dedicated CBRN expert centers to gather and distribute information and experience . Such centers should guide education of EU citizens on how to prepare for and respond to crises. The centres could have a coordinating role in multi-disciplinary R&D and knowledge management. Knowledge management systems should be in place to enable exchange of experiences, identify best practices and lessons learned (from small-scale incidents, training, and simulations), and design doctrines for proper responses. EU should create a network of laboratories (e.g. forensics, standardized testing and evaluation). By doing so, instalment of CBRN expert centers contribute to member state resilience towards CBRN threats.

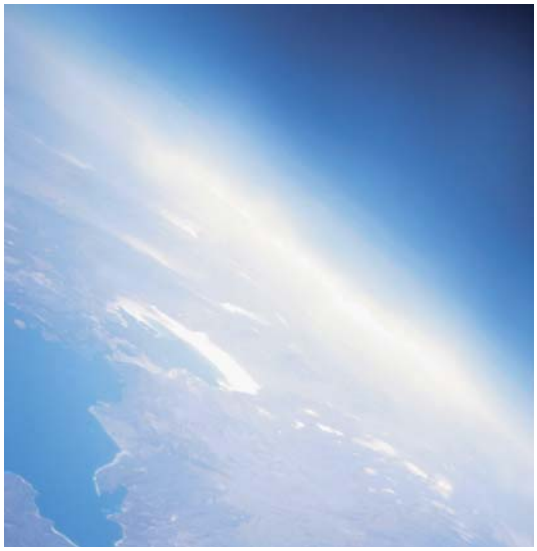
The EC is recommended to develop methodology and build infrastructure for intensified exchange of sensitive information like threat awareness, dual-use potential of emerging technology and trends in radicalization. The EC should promote a full system-of-systems approach to CBRN(E) counterterrorism following the full CBRN security cycle, including shared situational awareness, a robust interoperable first response . Emphasis should be on integration of this approach into other hazard areas the security community has to cope with.

On an EU level, networks must be established to monitor transport and trade of CBRN agents, raw materials, and related equipment, preferably supported by new or improved international treaties.

EU should fund and sustain a security industrial policy to create adaptive and modular solutions that are required for dealing with consequences of rare events.

Finally, EU member states are advised to agree on a number of official planning scenarios for states and public organizations to be the basis for security policy, development of doctrines, identification of capabilities and gaps, R&D strategy, and training and exercises.

7. Working Group: Situation Awareness and the Role of Space



7.1. Introduction

7.1.1. Scope

The proliferation of uncontrolled situations, including natural catastrophes, epidemic diseases or terrorism, can rapidly build up into threats on a larger scale. Thus, information, intelligence and surveillance became strategic assets, without which operations undertaken by organisations have little chance of success. Nevertheless, freedom of the citizens shall be considered as a priority and it is recommended that legal frameworks should be established to ensure privacy against the increasing information gathering capabilities.

Working group seven (WG 7) of ESRIF, coordinated with other mission areas, was responsible for related cross-cutting technological aspects. Identified as 'Situation Awareness and the role of Space' WG 7 dealt with skills contributing to a common operational picture relevant to urban security, internal security (i.e. border, transport) and peace enforcement scenarios.

It considered, inter alia, present and future needed sensors and platforms (ground, sea, air and space) for the perception and gathering of data and elements of the environment along with secure and reliable communications including Network Enabled Capabilities'(NEC) concepts and mobile ad-hoc networks, as well as the information processing and decision support functionalities needed to enable sense-making.

The group analysed new rules and new technologies to foster information sharing - identifying adequate methods and formats of information management. Based on intelligence and surveillance it also examined the international cooperation framework regarding data and information fusion of heterogeneous sources for better comprehension and recognition of the meaning and significance of a situation. Moreover, it considered the need for risk assessment and early warning by adding-up modelling and simulation for projecting and anticipating the status and events.

The work approach lead to the assessment of the current situation and the analysis of the near to long-term future challenges for the areas of interest for Situation Awareness (SA) and the deduction of required capabilities to cope with the envisaged scenarios. Finally, the group had to recognize the gaps, prioritize them and plan a roadmap with the necessary recommendations.

It is important to realise that the needs for high levels of protection of possible targets of antagonistic threats (e.g., subway systems) must be balanced against the needs for integrity, privacy and personal freedom of the European citizen. Achieving such a balance is possible by ensuring that the technological research proposed in this report is integrated with ethical and integrity aspects. New technologies will also enable us to ensure that the personal data acquired in preventive security context can only be acceded under strict and enforceable conditions - e.g. by magistrates - and is destroyed as promptly as possible.

7.1.2. The context

Modern European society is more and more demanding in sophisticated goods, competitive economy and rapid and easy access to information and places. Hence, society is also more vulnerable to threats and the ability to manage and face unexpected situations.

Risks and responses to such risks must be handled on a global scale and in an increasingly integrated way. As a result, technologies in the area of Situation Awareness must evolve and be enhanced so that they can contribute to properly manage future threats.

Considering this, *Situation Awareness defined as the accessibility of a comprehensive and coherent situation representation which is continuously being updated in accordance with the results of recurrent situation assessment*[1] is a key factor, particularly in view of the increased level of security needed by the evolution of threat scenarios (organised crime, terrorism, natural disasters, pandemics, illegal immigration etc.).

Within the ESRIF context, WG 7 identified the main topics contributing to an improved Situation Awareness and established sub-themes for more in depth studies. Coordinating the needs of the mission areas and addressing cross-cutting technological elements, the work was structured through the following domains:

- Surveillance platforms and sensors
- Communications
- Information integration management and
- Space

The four domains, although analysed per se in view of threat scenarios and mission areas, are also considered in an interdependent perspective.

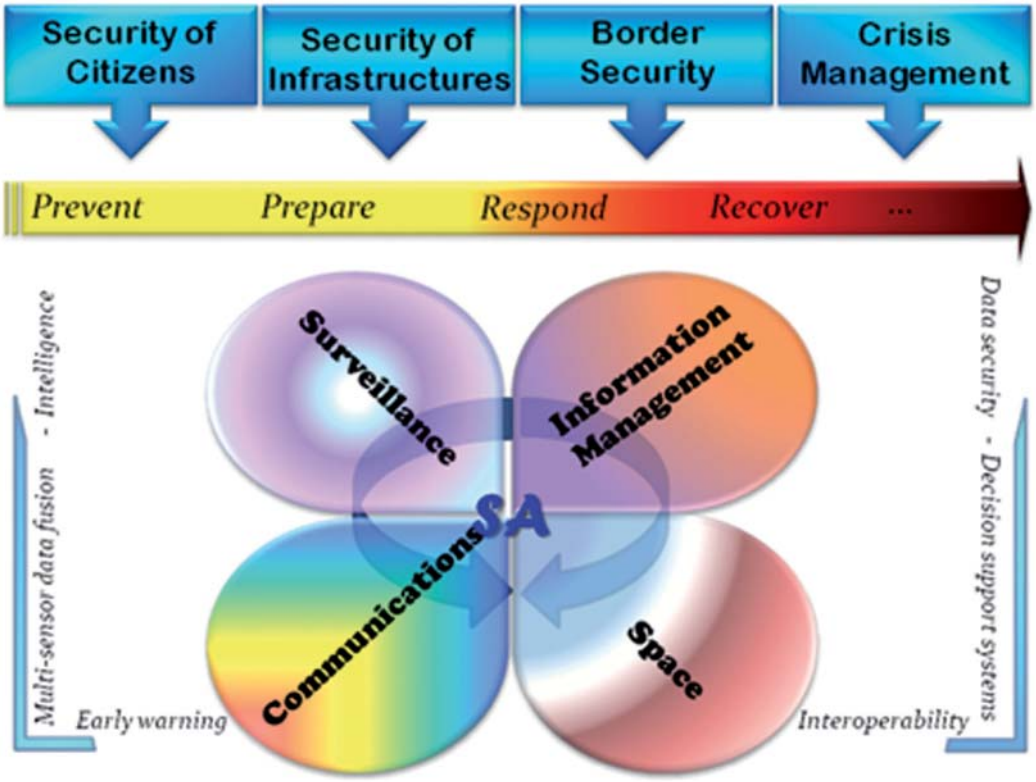


Figure 1: Situation Awareness for an increased level of security

In principle SA has always been required to properly perform essentially operational tasks. However the current evolution of information and communication technology stress this need even further, because of the fast changing environment and the need to perceive, analyse and understand a huge amount of data.

1 As defined by Sarter, N.B.,& Woods, D.D. 1991. Situation awareness: A critical but ill-defined phenomenon. The International Journal of Aviation Psycology, 1(1), pages 45-57

Nonetheless, to protect information housed in heterogeneous, decentralised and interconnected networks new techniques as well as regulatory and organisational solutions are needed to guarantee their safe and secure use. Privacy and data protection capabilities are essential to ensure that data fusion and analysis on this scale does not infringe upon personal liberties.

The power of information is increased by providing widespread access to data, conducted through advanced integrated **communication** networks. Though, the problem is not a lack of information but finding what is needed and when it is needed to increase proper situation awareness.

As a consequence, **information management systems, including decision support systems**, are crucial to support operational end-users and decision-makers in their work to gain situation awareness which requires also investment on interoperable and network command and control capabilities. This includes improved surveillance (ISR) capabilities with respect to coverage, quality and the fusion of real-time sensor data (space, air, land, sea) as well as intelligence and open source material in order to establish a common recognised operational picture. The role of space is vital in this scenario through GMES (Global Monitoring for Environment and Security) and its first wave of services, also interacting with other European space programmes and deployed space based capabilities.

Command and control capabilities for situation awareness require a large improvement in existing centres including the development of domain and scenario specific models to be effectively used for early warning, situation and threat assessments. These capabilities must be supported by robust, secure and interoperable communication systems linked to the significantly improved protection of supervisory control and data acquisition systems (SCADA). **Network centric communication** supported by satellite is also a key capability to properly support most of the communication needs in terms of secured bandwidth and flexible access.

While using the necessary infrastructures, on the operational level the capability to enhance collaboration between individuals and organisations is fundamental to plan complex endeavours by de-conflicting, coordinating, collaborating and planning (or simulating) operations. This requires more than ever public-private partnerships and the introduction of new consistent and complementary knowledge through civil governmental and military cooperation.

Finally, achievement of truly interoperable systems and integration of applications at national and supranational level is a key requirement to make effective data collection, harmonised requirements and validity of evidence of digital forensic capabilities, to track and trace criminal actions in information networks.

Discussion with the Member States is required to support a regulated evolution towards a full deployment of interoperable systems.

7.2 Situation Awareness

Some of the challenges Europe and the entire world are facing in addressing situation awareness, particularly in the fields of emergency response and crisis management include the ability for making adaptive decisions in situations involving uncertainty, based on the knowledge of actual and near-term events within a specific environment and context.

To help agents achieve situation awareness it is necessary to develop information fusion reasoning and knowledge-gathering processes tailored to the specific application domain. The behaviour of the agents as well as what information they need will differ depending on their goals. In the security context it is fundamental to reach a high level of perception of the environment in order to prevent problems in the assessment and cognitive processes.

Disregarding the specificity of the risks and challenges per domains, be it for the security of citizens, critical infrastructures, border control or crises management, common requirements, capabilities, systems and technologies can be identified.

With the aim of covering the three stages of SA – perception, comprehension and projection – we will go through the different elements that contribute to recognise, monitor, prevent and respond to threats.

7.2.1. Risks and challenges

7.2.1.1 Surveillance

The observation and monitoring of movements, activities and behaviours from a distance or by evaluation of electronic information, data and traffic records is very useful to law enforcement for the prevention of criminal acts. Technologies for integrity-preserving surveillance need to be developed and adapted.

There is a particular need for fixed and mobile robust automated surveillance systems to meet increasing surveillance requirements with respect to coverage and quality. A distributed self-organising sensor network with sensing and communication capabilities to be spread in selected areas is needed to improve related security information to protect the citizens.

Sensor architecture capabilities and the selective use of surveillance sensors and systems - be it long-distance (e.g. digital/ thermal imaging) or short-distance (e.g. terahertz, biometric) - depend on the goals, the relevant scenarios and the decision-tasks. Ethical issues and full respect for privacy, liberty and civil rights are aspects that cannot be neglected in all present and future technological developments. A balance must be achieved between the privacy rights of citizens and the need to protect Europe and its citizens against threats.

Analysis of the challenges and required surveillance capabilities by different mission areas has been analysed by WG 7.

Security as a form of protection involves a set of procedures or measures in relation to relevant scenarios to identify, review and evaluate adequate responses to anticipated risks. In the ESRIF context the analysis of risks and challenges within the different mission areas clearly showed that there are commonalities allowing the recognition of key challenges for surveillance. Those include the need for automated surveillance and permanent monitoring by using multi sources surveillance at borders and tools for heterogeneous data fusion as well as the interoperability of systems and sharing of data sources. Moreover, the use of space based sensors (optical and SAR imagery) will be fundamental to a wide spectrum of applications.

The description and reasoning per mission area is summarised in Table 1.

Surveillance		
challenges	description	reasoning
Security of citizens	• Fixed and mobile robust automated surveillance systems, to meet increasing surveillance requirements with respect to coverage and quality • Develop innovative sensors (e.g. explosives detection) and the related processing methodologies • New simulation engines for calculation of optimal sensor constellation • Automated analysis of information and alerts generated by the general public	Having a distributed and self organising sensor network with sensing and communication capabilities, positioned in selected areas, will improve the coverage and security information to protect the citizens. Additional Having a distributed and self organising sensor network with sensing and communication capabilities, positioned in selected areas, will improve the coverage and security information to protect the citizens. Additional sensor capabilities and related processing methodologies will enable real-time data exploitation and immediate actions from agents. Simulation tools will facilitate an automated evaluation of best sensing sources for a specific scenario, while automated processing will assist on decision-support and spread of general alert messages to citizens.
Security of infrastructure	• Permanent monitoring of the environment, both in & outside a critical infrastructure, operational night and day and in any weather condition, to combat the terrorism, organized crime and sabotage • Develop unnoticed and reliable sensors • Increasing need for interlinked emergency communication and response systems • Combat the Emergence caused by technology trend (e.g.. the use of mobile phones as bomb trigger). • Mitigation of the increasing dependence of Infrastructures from the Technology • Space Situational Awareness	Appropriate development of unattended ground sensors can enable fusion and decision support systems to automatically alert users when a threat towards an infrastructure is detected. The capability for real-time Appropriate development of unattended ground sensors can enable fusion and decision support systems to automatically alert users when a threat towards an infrastructure is detected. The capability for real-time assessing natural or man-made disasters with effect on power, gas and telecommunication infrastructures is an increasing must. Combination of heterogeneous sensing techniques and interworking public-private security with SOC's alarm connection is of utmost importance for coordinated responses. Satellite based information will serve to build databases to allow coherent monitoring and provide a dynamic knowledge-base to reinforce global safety and security.
Border surveillance	• Use of disparate forms of real-time and historical data, facilitating effective decision-making and performance in a complex environment • Detection of aircraft flying low and slow • Detect small craft and anomalies at sea • Combat the unlawful movement of goods/substances and people at regulated border. • Looking at the scale and scope of Europe's borders, long endurance platforms and improved services required	Capture, fusion, correlation and interpretation of disparate forms of real-time and historical data is fundamental for quick and appropriate response in complex endeavours. Interoperable databases will be essential to allow surveillance information to be cross-referenced to combat unlawful movements. Space and aerial platforms, including UAVs, combined with in situ data gathering, and integrated services with secure data transfer will contribute to superior detection of anomalies and promote improved security and protection.
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 • search and rescue of victim • Integration and fusion of data gathered from a wide array of sensors including space, air, land, sea, and personnel • Enhanced surveillance by unmanned platforms • Civil-military cooperation	Tools for environmental monitoring, combined with different (man or unmanned) sources data gathering will contribute to an integrated infrastructure to cover broad range of services and applications in early-warning and crisis management. Mechanisms for data exchange, advanced visualization techniques and improved development in human-system interaction are essential to facilitate faster and better decision-making. Continuous monitoring together with positioning and timing capabilities will improve the efficiency of search and rescue teams.

Table 1: Risks and challenges for surveillance

7.2.1.2 Communications

A key aspect to consider when dealing with the security of the citizens is the likely intervention of different kinds of first responders. Depending on the scale of the events, coordination among these actors is required at a command and at an operational level. These actors will have different communications systems, ranging from radio, terrestrial networks to satellites that are not interoperable by default. Some first responders may even rely on communications service providers (i.e. telecommunications and mobile infrastructure companies) whose infrastructures normally collapse due to the huge increase of demand by population when a disaster occurs (terrorist attack, natural disaster…). In order to optimise the operations complete situation awareness is needed, so data flow from different organisations and/or sensors must be supported by reliable communications.

Some of the challenges to be considered are interoperable communication and message exchange at all levels. Table 2 addresses some of the identified challenges in the area of communications.

Communications		
	Challenges description	reasoning
Security of citizens	• Interoperable communication and message exchange • cross-organization interoperability • Adaptive systems for heterogeneous networks. • Develop Over The Horizon (OTH) communication channels more resistant to terrorist attacks. • Secured communication networks • Communication to the general public (warning, alerts, guidelines...).	Coordination among actors is required at a command and at an operational level. Their different communication systems are not interoperable by default and first responders may even depend from service providers and weak infrastructures. Robust and secure logical network can ensure continuous access to essential information. Less vulnerable satellite bands for communication can prevent disruption of communications. Social and psychological aspect must be considered when dealing with communication to the general public.
Security of infrastructure	• Automatic authentication of people accessing terminals and networks • Robust encoding. • Cyber-warfare. • Robust and secured sensor network within an infrastructure and for remote control and monitoring	Use of intrusion detection systems to identify malicious suspicious traffic and identification of predefined dubious behaviour patterns. Improve the protection and resilience of communication networks and have robust and secured conectivity.
Border surveillance	• Improving end-to-end secure communication. • Broadband interoperable and robust software defined radio waveforms solutions. • Ability to use Network Enabled Capabilities (NEC) concepts and mobile ad-hoc networks (MANET). • Robust satellite communicatio for encompassing large geographical areas.	Have a single logical network to provide the necessary capability to support quality of services (QoS). Intelligent and self-adaptable communications system is necessary to respond to dynamic situations. Communications infrastructures to be designed with attributes like self-healing, adaptability, resilience and robustness.
Crisis Management	• Flexible and easily deployable mobile ad-hoc network and global connectivity. • Interoperable communication and message exchange at all levels (warning, alerting, reporting and command functions). • Multinational cross-organization interoperability. • Adaptive systems for heterogeneous networks. SDR platforms supporting different waveforms (existing legacy and new generation interoperable and high data rate waveforms) • More efficient use of frequency spectrum, power and transmission antenna gain. Cognitive radio concept.	Necessary to provide a global network which heterogeneous devices and equipments can connect to and where mobility is a must. Take distributed communication schemas into account rather than focusing in traditional centralised decision-making posts. SDR based waveforms could be a dynamic and flexible solution to achieve interoperability and enable ad-hoc voice communications. Consider the use of alternative satellites working in less vulnerable bands. Cognitive radio capability to be considered.

Table 2: Risks and challenges for communications

7.2.1.3 Information Integration Management

The quality of decisions in security operations heavily depends on the decision-makers' knowledge of how critical situations unfold, i.e., their situation awareness. Research on how to enhance situation awareness is thus of vital importance for the security of European citizens. One of the critical elements of situation awareness is to comprehend the meaning of a situation and to make projections of its future development. By improving these abilities through technological and methodological innovations, decision-makers will be able to more rapidly identify and respond to hazardous events. This includes technology to integrate and interpret vast amounts of information from heterogeneous sensors and information sources. In this area as well as in the surveillance area there is a need for research on how to construct systems that balance the security needs with the privacy and integrity rights of citizens.

Due to the large variety of potential situations and the open ended problems encountered, this technology cannot be fully automated. Thus mixed initiative interaction between humans and technical systems must be supported and also the ability to collaborate regarding the assessment of situations among operators and analysts that may be separated by geographical, organisational and cultural boundaries. Semantic interoperability of designed information management systems is thus a key challenge.

For this purpose the key issue in distributed systems in dynamic environments is getting the right information at the right time and at the right place, including addressing privacy and security issues. An evolutionary path towards this ideal is

depicted in Figure 2, which is derived from the NATO Networked Enabled Capability (NEC) roadmap. The three layers can be linked to the three levels of SA. The roadmap distinguishes four phases. The phase transition between deconflict and coordinate mainly concerns improving interoperability while the phase transition between coordinate and collaborate concerns going from centralised to decentralized control. In the final phase the whole system organisation can adapt itself to the common goal.

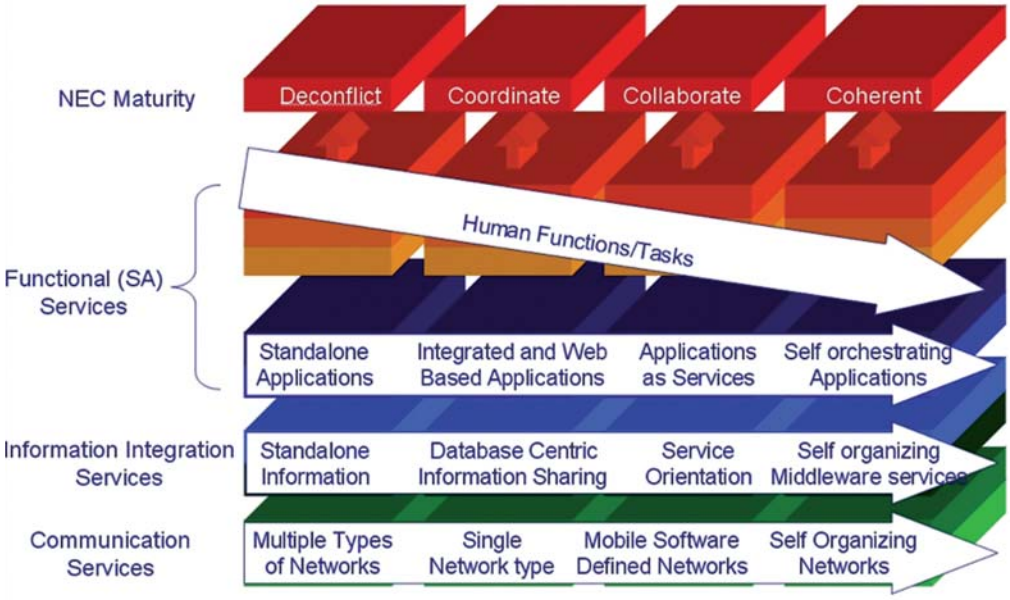


Figure 2: NATO Networked Enabled Capability (NEC) roadmap

Based on this framework challenges and future needs are addressed for the different application domains.

Table 3 below addresses identified challenges for information integration and management.

Information Integration and Management		
	Challenges description	reasoning
Security of citizens	• tools for information fusion that enable automatic and semi-automatic production of intelligence • dealing with de-confliction of requests • improving the compatibility of all interfaces (HW and SW, including format) for data-exchange • support in the decision making process • resolution of conflicting request • Solutions for information integration must be designed to respect human privacy	Use of intelligent decision making support with an information management and integration that is adaptive to changing situations and a dynamic management of private and public information. Enhance interoperability; provide intelligent tools for the mining, analysis, and exploitation of massive sources of heterogeneous and multi-dimensional information. Provide intelligent tools enabling the anticipation of future events and the evaluation of scenarios
Security of infrastructure	• establishment of a critical infrastructure warning information network • communication, coordination, and cooperation nationally and at EU level • interworking capabilities between the public and the private sector • data and information fusion capabilities tailored to the needs of infrastructure protection • EU alert system capable of respond Solutions for information integration must be designed to respect human privacy	Collection of information from many widely dispersed sources for availability to consequence managers. This implies interworking of public and private authorities. Planning and assessment of geolocation of relevant sensors may help simulation, training and real-time management and help in risk analysis and damage assessment. Public officials need immediate access to warning information.
Border surveillance	• Global tracking of naval and cross-border traffic • Improved data mining and image/pattern recognition • Create metadata systems • construct semi-automatic capabilities for data and information fusion • fully automatic systems for early warning and intrusion detection • Solutions for information integration must be designed to respect human privacy	Make available information to those with permission to do information fusion, exchange techniques, gateways and translators. Better tools for analysing data and information, constructing hypotheses and reasoning about them. Systems that make use of open source information from, e.g., the Internet, to discover unauthorized border crossing should be researched.
Crisis Management	• Development of Open Architectures (SOA and SW Infrastructures) that allow data exchange also among legacy systems • innovative solutions for mixed-initiative interaction support to decision making • Early warning systems • capabilities have to support mixed initiative between public and private sector • Solutions for information integration must be designed to respect human privacy	Contribute to the enhancement of the knowledge of each system allowing to optimize the sensors surveillance parameters (Knowledge Based Systems). Automatic and semi-automatic fusion of heterogeneous data sources and reasoning agents that help human analysts construct and validate or refute hypotheses about future events. UAS can supply a wide range of services in support of surveillance and intelligence operations.

Table 3: Risks and challenges for information integration management

7.2.2 Required capabilities

Security today and in the future will not be effective without proper technology and cyber information management. There is a general perception that technology can be an enabler for global security but it can only became effective if it inspires support from the public through an acceptable social balance between the possible risks and benefits and when adequate procedures to protect the privacy of the citizens are established and known by the public.

The persistence of organised violence in different forms - financial, political, ethnic - threatens the security and prosperity of European citizens. The increased globalisation of networks and flows means that risks are no longer confined geographically and that authorities and nations need to collaborate in order to make effective responses to threats. With proper governance of actors, missions and procedures as well as research into new integrity-preserving technologies we can allow a balanced implementation of security measures that guarantee the protection of personal freedoms.

Special attention will have to be dedicated to collected data gathered during preventive actions. Today, automatic analysis algorithms are often too expensive and not robust enough to provide reliable meta-data extraction at a quality that is comparable to human capabilities. At the same time, legal mechanisms are required that take full advantage of technological opportunities and to allow acceptance of meta-data evidence or to provide accountability for actions taken.

Integrated Surveillance Management - seamless, unimpeded access to surveillance and intelligence data of different tiers, require interoperability/interfaces and procedural as well as legal frameworks.

Enhanced hazard or asset detection and identification, including global tracking of naval and cross-border traffic - The current generation of visual surveillance systems suffers from a lack of robustness at different levels. The use of other means of location or identification and tracking (even not absolute) such as tag (e.g. containers tags) or biometry can greatly enhance video tracking by associating and correlating discontinuous video tracking sequences. Integration of sensors, knowledge databases, identification parameters databases, etc. within existing systems, and taking into account interoperability issues between systems that will need to collaborate, is a must. All this will have to be considered during the development of future systems.

Harmonised global border control - Concept-to-Capability facilities offer a synthetic environment where integrated sensor solutions can be developed and deployed, providing cost-effective and demonstrable operational capability across a number of disciplines for border control like land, maritime and air operations. Unmanned Air System can supply a wide range of services in support of surveillance and intelligence operations.

Sharing of sensors and sensor data (meta data) in support of risk and vulnerability assessment allowing early warnings and threats - Sensor platforms are commonly either used by public or private authorities. Mechanisms for ad-hoc, incident based sharing of sensor or meta-data need to be devised. Interworking between public and private security installations is commonly performed on an alarm basis in a preconfigured manner, e.g. permanent connection of alarms to a security operation centre (SOC). Mechanisms for the sharing of sensor as well as meta-data derived from sensor data need to be implemented. Methods are lacking that integrate vulnerability analyses and the identification of indicators with early warning prediction models in the event of attacks or incidents. This includes inter-system effects awareness that should imply secure design and construction to prevent cascade failures.

Improving Detection and Identification by updating/developing new sensors- new and innovative sensing techniques considering developments in areas like terahertz, meta or nanomaterials or are required in support to unconventional attacks (e.g. CBRN), post crisis management or search and rescue.

Continuous improvement of detection/sensor equipment –To support the preparation of the contingency and security plans, high resolution space-based sensors, both high resolution optical information and high resolution radar information are also important. Satellite sensors will be able to provide, static area information to setup operation panning. Such sensors will be able to help in characterising representative crowded areas by providing information about the scene geometry and interaction.

Reliable sensor high-throughput /standoff capability and large focus point surveillance in networks - The better performance of sensors in terms of spectral information, spatial resolution and area coverage is required. Still there are limited automatic capabilities for a context specific analysis of data coming from sensors and there is a lack of autonomy of the sensing systems. Increased autonomy is fundamental to reduce and improve the data provided to the users. It will also be important to make use of available sensors that might not, a priori, be connected to the relevant agencies network. This will require development of rules and regulations for when sensor networks belonging to, e.g., private corporations or citizens can be used by authorities. It also requires development of methods and systems for integrating unknown sources into the command and control system.

Strategic(observation means)planning and tactical simulation - For security operations management, depending on the requirements defined by the crisis management team a denser coverage or a general reallocation becomes necessary to ensure proper monitoring of the crisis. There is still a need of new, more powerful strategies to optimize the sensor coverage with respect to the current scenario. New simulation engines to allow the calculation of the optimal sensor constellation in respect to the physical phenomenon under investigation are needed.

Common operational picture generation - Crisis situations will happen both in locations where we have previously deployed sensors and in locations where there are no permanent sensors. It is thus important to be able to rapidly deploy sensors of different types in an area in order to get a situation picture. This deployment can be made by autonomous vehicles who deposit large amounts of tiny sensors, rapidly covering the area of interest.

Required efficient and interlinked communications – The frequency spectrum for radio communications is overloaded and there are no resilient OTH communications. Communications security standards are not available and although SDR is promising, yet there are not standardised adaptive systems for different radio networks. At European level a satellite communications infrastructure to facilitate information sharing in large geographical areas need to be established.

Automatic analysis capabilities adaptive to dynamic situations – different types of sensors can be used individually, or in networks in order to improve the detection and recognition performances through multi-sensor data fusion. Merging different types of sensors (in particular radar and electro-optic sensors) should largely improve false alarm rate and target recognition capability. Some multi-sensor data fusion methods are already well known[2], but are still to be assessed in an operational and dynamic context. It is required to move from a centralised approach to a sensor network enabled system with required intelligence to reach self-reconfiguration in support to decision-makers on situation analysis and autonomous damage assessment.

Support to decision-making and situation analysis – support tools that help humans achieve situation awareness and produce better intelligence reports need to be developed. Mixed-initiative tools for fusion, sorting and filtering of a large amount of data and information from heterogeneous sources, including sensors as well as open source materials and information collected from the web, need to be developed and adapted to the needs of different application areas.

Adaptive modelling and simulation tools - Simulation techniques are only rudimentary developed, require a high modelling effort to provide adequate precision and are computationally too expensive to provide real-time crisis support. Methods are lacking that integrate vulnerability analyses and the identification of indicators with early warning prediction models.

7.2.3 Systemic needs

In order to enable security for the citizen and have competitive market, security systems and policies must be designed to be accepted and trusted by the public. This means that integrity and privacy aspects must be integrated into the technical systems themselves and not only be added later as an after-thought.

2 Known algorithms are not enough so further research is required

Legal frameworks have to be created that allow cooperation and knowledge sharing among different actors. At the European level this will foster inter-organisation cooperation, namely in civil protection operations, by adopting common operational procedures.

At the same time the public needs to be properly informed promoting debate on the policies and systems through specific education and training actions and other forms of long-term trust-building interactions for the citizen. More than adequate legislation, the building of trust in authorities and systems by enabling systemic technical and operational interoperability is fundamental. In support to that the generation of scenario simulation tools (incl. Virtual reality) for rapid assessment during crisis, the creation of information / warning methodologies and the development of specific education and training programmes (virtual live exercises and other simulation-supported training methods) for decision makers, regulators and media can be a step forward.

At a more operational level and in situations of disaster and crisis management, to allow interoperable command and control cooperation for a more efficient international collaboration it is fundamental to adopt standardised procedures of rescuer identity, skills and credentials.

To give response to new threats, advanced tracking and tracing with automatic warning (linked to detailed information on persons and goods) becomes more and more important. This should be supported by adequate information management systems with access protocols to sensitive data as per access rights to guarantee full respect of privacy rules.

Need of tools for a better coordination in the use of existing assets - For security operations management, depending on the requirements defined by the crisis coordination team, a denser coverage or a general reallocation of assets becomes necessary to ensure proper monitoring of the crisis. There is still a need of new, more powerful strategies to optimize the sensor coverage with respect to a defined scenario. New simulation engines to allow the calculation of the optimal sensor placement and configuration in respect to the physical phenomenon under investigation are needed. The aim is to enhance the utilization of such systems and therefore contribute in providing for a certain scenario better utilisation of assets bringing an increased coverage and quality in the data.

Promote collaborative use and multiple use of services, information and data – Considering the proliferation of intergovernmental agencies and security programmes that promote synergies between the civil and military actors, collaborative actions are to be thought of. Adequate protocols for the definition of data policy related to crisis management or peace keeping functions need to be agreed to.

Information / warning methodologies in case of crisis - The behaviour of uninformed or partially informed populations may over complicate crisis situations. A proper communication strategy to the citizens in case of crises would improve crises response along the crisis phases.

Social and psychological aspects must be considered when dealing with communication with the general public due to the fact that, among other aspects, social panic in the aftermath of a disaster may jeopardise public communications infrastructures.

Analysis of novel system of systems approaches like the NEC for civil security applications – There is a need to introduce and implement at European level a common NEC concept. Studies are required to assess the implications of applying the "need to share" concept implicit to NEC both on communications bandwidth or decision making for crisis management.

In support of governance decision making, the generation of comprehensive complex system integration guidelines (architectural, technical, operational etc.) and the creation of a shared conceptual framework for security policy with embedded sound foresight and risk assessment practices are of utmost importance for future security endeavours.

New tools for Common Operational Picture generation together with methods and infrastructure for information sharing will help provide the public with updates/warnings as well as in reporting about noticed unusual /suspicious activities.

7.2.4 Research needs and priorities

MAIN GAPS	KEY RESEARCH TOPICS	PRIORITY
AUTOMATIC ANALYSIS CAPABILITIES ADAPTIVE TO DYNAMIC SITUATIONS	Research should focus on Data and Information Fusion - Automatic network reconfiguration	very high
SHARING OF SENSORS AND SENSOR DATA (META DATA)	Research should focus on Vulnerability modelling and analysis and interoperability issues, including semantic interoperability to ensure that different C2 systems can exchange information	
ESTABLISHMENT OF A CRITICAL INFRASTRUCTURE WARNING INFORMATION NETWORK	Research should focus on: ▶ Standardised adaptive systems for different radio networks. ▶ NEC concepts. ▶ Broadband satellite communications infrastructure. ▶ Satellite based observation systems and telecommunication infrastructure. ▶ Space Situational Awareness and Signal Intelligence	high
DETECTION, LOCALIZATION AND IDENTIFICATION OF DIFFICULT TARGETS IN COMPLEX ENVIRONMENT	Research should focus on Technologies for both radars and EW (electronic warfare) systems as well as multi-sensor fusion.	
ADAPTIVE, SELF-LEARNING AND ANTICIPATIVE TECHNOLOGIES FOR DYNAMICALLY CHANGING OPERATIONAL SITUATIONS AND VARIOUS ENVIRONMENTAL CONDITIONS	Research should focus on: ▶ Software reconfigurable sensors, ▶ Dynamic frequency management, ▶ Co-existence and effective interference suppression of RF systems, ▶ Adaptive beam forming, ▶ Wideband antennas, ▶ Waveform generators, ▶ Power amplifiers, ▶ Wideband high dynamic range receivers, ▶ Adaptive sensor management, ▶ Prediction of target behaviour and intent.	
MOBILE AD-HOC NETWORKS IN URBAN AND METROPOLITAN TO BE DEPLOYED IN EMERGENCY PHASE	Mobile Broadband Wireless Access (MBWA) to route and/or relay packets (e.g. IP packets) between the external networks and the mobile terminals or between the mobile terminals	high

OPTIMIZED COMMUNICATION CAPABILITIES TO AVAILABLE RESOURCES (BANDWIDTH, FREQUENCIES) IN EMERGENCY MODE	Advanced software radio reconfigurable functionalities including cognitive capabilities radio" to sense the surrounding environment and adapt the waveform parameters to available resources, bandwidth requirements, level of interference present, etc	high
SATELLITE COMMUNICATIONS SYSTEM FULLY INTEGRATED WITH THE GLOBAL COMMUNICATIONS NETWORK AND NETWORK CENTRIC COMMUNICATION CAPABILITY	IP based, high-capacity microwave and optical network in space, made of advanced next generation satellites with very high data rate telecommunication connections, including inter-satellite links and including new generation LEO Satellite constellations	very high - short term
SATELLITE COMMS FULLY INTEGRATED WITH NEXT GENERATION TERRESTRIAL NETWORK	Bandwidth/power efficient IPv4/IPv6 satellite on board/ground modems with open standard interfaces	very high - short term
SATELLITE COMMS IN SYSTEM-OF-SYSTEM CAPABILITY	Satellite Constellations and Formation Flying (FF) in the Networked Environment Development of Space based data relay system. Aerial and satellite communications interfaces.	very high - short term
SPACE SURVEILLANCE IN SYSTEM-OF-SYSTEM CAPABILITY	SAR systems Autonomous satellite constellations for earth observation	very high medium-long term
RECONNAISSANCE AND IDENTIFICATION FOR SURVEILLANCE, USING SATELLITE ASSET	Space Based Multi- and Hyperspectral Sensors Technology and Applications Multi-frequency synthetic aperture radars	very high medium-term
EARLY WARNING SPACE SYSTEMS	early warning and ELINT satellite solution (GEO satellite with very large deployable reflectors, mini/micro sat constellations, nanosat disposable constellations)	very high long- term
3D URBAN MAPPING BY SATELLITE	digital elevation models - SAR and optical observation systems	very high - short-medium term
DECISION SUPPORT SYSTEM BY GEOSPATIAL INFORMATION SYSTEMS	▶ geospatial information systems and technology ▶ space-based positioning, navigation and timing	very high - short-medium term
SPACE SITUATIONAL AWARENESS	▶ ground radar and telescope infrastructure ▶ tracking and space-imaging solutions	very high - long term

SPACE ENVIRONMENT AND SPACE WEATHER	forecasting systems for space environment and space weather	very high - long term
DECISION SUPPORT SYSTEMS	Mixed-initiative interaction tools that help humans achieve situation awareness Information fusion to provide situation and threat assessment functionalities	
OPEN SOURCE INTELLIGENCE PROCESSING AND ANALYSIS	Web crawling, including the so-called dark web, to collect relevant data Analysis systems for open source intelligence, including sentiment analysis and text mining	

Table 4: Research priorities for Situation awareness

7.3 The role of space

Space assets and offered services are today indispensable enablers for a wide spectrum of applications to answer societal challenges in fields such as climate change and environment, transport, development and competitiveness in Europe and beyond. Also, new generations of aerial platforms e.g. high-altitude platforms or vehicles including UAVs can make available complementary services to increase the overall quality and accuracy of essential information.

More specifically, air and space-based services can offer large added value and critical capabilities to security-related applications encompassing environmental and weather phenomena, infrastructure (i.e. power, gas and telecommunications) and business safety. In addition, monitoring various kinds of radio transmission allow countering different threats, generating early-warning alerts and carrying out search and rescue, civil security or emergency response.

Nevertheless, space lacks responsiveness which is crucial to answer any security threat and support any operation. The combination of new satellite platforms, new planning approaches, the increase of onboard autonomy, the use of space based relay systems and the appropriate ground based infrastructure with new operations concepts is crucial to increase the level of responsiveness of space based capabilities.

In this context the investment in and deployment of space infrastructure applications and related services is seen to be most promising in the following domains:

TELECOMMUNICATION SERVICES	telemedicine, distance learning, health issues, e-commerce, and multimedia entertainment as well as a communication backbone for humanitarian relief and crisis management operations
EARTH OBSERVATION APPLICATIONS	environmental data, land use management, exploration, natural disaster prevention and management, and treaty monitoring
SATELLITE NAVIGATION, TIMING AND POSITIONING	fleet and traffic management, location based services, search and rescue

Table 5: Most promising space applications until 2030 (according with OECD)

The seamless integration of space applications within wider systems featuring terrestrial sensors (be they land, sea or air-based) will allow to furthermore develop a full spectrum of added value services with unprecedented performance in terms of

all around the globe near real-time data delivery and data continuity. The combination of different data gathering assets and advanced techniques for data exploitation and exchange together with international cooperation between stakeholders (civil and military) present enormous potential to improve missions[3] efficiency.

European flagship programmes such as Galileo and GMES will prove crucial in this respect. The **Global Monitoring for Environment and Security** (GMES) will thereby provide a first set of initial services for land monitoring, atmosphere and maritime data, deriving data from both national (contributing missions) and European-level space assets, i.e. the GMES Sentinels (dedicated missions). Over time emergency-response related services will complete the picture. The overall GMES architecture thereby includes the Space Component, the Service and in-situ Component and the key Data Integration and Information Management component. Synergies and interaction with other European space programmes such as the **European Data Relay Satellite System** (EDRS) will further enhance the availability and quality of GMES services.

The development of Galileo and the use of the **European Geostationary Navigation Overlay System** (EGNOS), greatly contribute to the quantity and quality of the satellite measurements. In particular Galileo will increase the integrity of the GNSS measurements, key factor for the applications affecting **Safety of Life** (SoL). EGNOS and Galileo are very valuable tools to support the prevention and mitigation phase. Positioning and timing capabilities together with continuous and low-cost monitoring of infrastructures and natural phenomena (such as Volcanism, land-sliding or floods) by other means (aerial or in situ), will provide a much needed service to users requiring accurate information to improve the efficiency of **Search and Rescue** (SaR) teams.

Despite the importance of satellite technology in emergency management, to further enhance related capabilities, future work needs to be performed in the areas of Space System Concepts and Data Exploitation techniques. While the former includes more study of mission architectures (e.g. microsatellite clusters, satellite constellations combining civil and defence-related satellites) the latter aims at developing techniques such as the fusion of GEOINT information derived from satellites with other sources or 3D modelling of objects among others.

Figure 3 helps visualising required capabilities in the space domain and the required research at technology development (green) level and product development (blue)

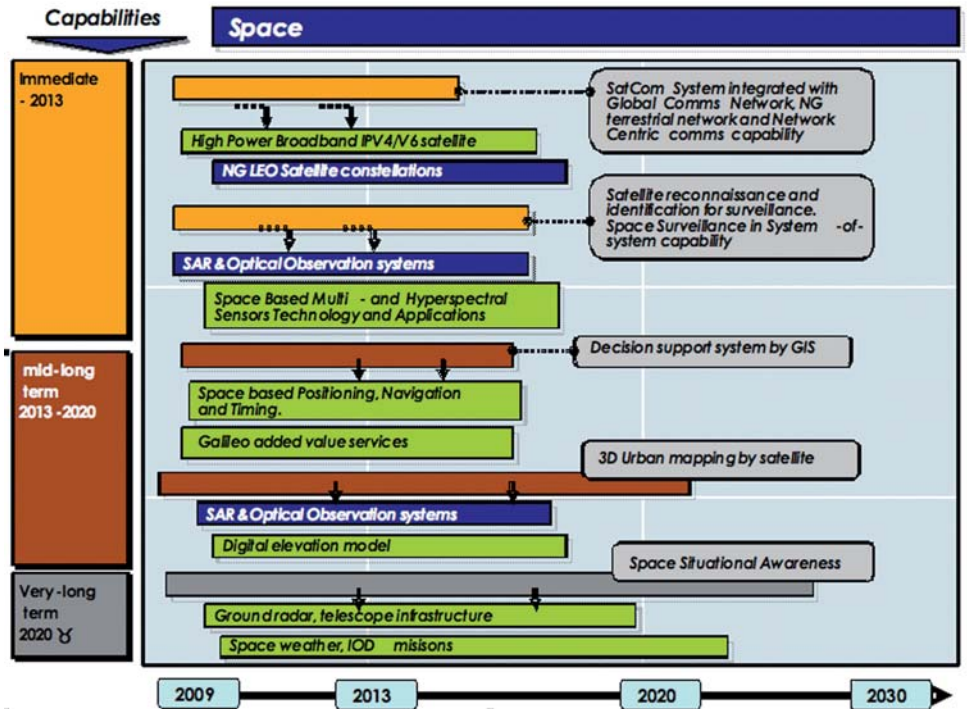


Figure 3: Roadmap for required capabilities and research needs in the space domain

3 OECD Report Space 2030: Exploring the Future of Space Applications, 2004, at pages 117, 119, 121.

7.3.1 Space as infrastructure

The European utilisation of space, for research or services, depends on the capability to safely operate the space infrastructures and any full shutdown of even a part of it would have major consequences for economic activities and would impair the organisation of emergency services as well as the management of crisis phases. Given the increased dependency on space-based services for a wide range of applications and the scale and cost of investment, space assets per se are to be seen as a major critical infrastructure and need to be protected.

Increasing **Space Situational Awareness** (SSA), defined as the comprehensive understanding and knowledge of the population of space objects, the space environment and existing threats/risks, is therefore of key importance to Europe. The European Space Policy states that Europe should protect its space-based capabilities against disruption given that the economy and security of Europe and its citizens are increasingly dependent on them.

SSA can thus be seen as a basis for any future measures (political, diplomatic, regulatory and technical) to guarantee access to space. Any disturbance may not be exclusively related to space debris. The drivers for SSA are possible consequences of interruption of space services.

There is a need to build at European level a common response to protect space assets joining national and EU, both civil and military efforts.

SECURITY AND SOCIETY	Development of an autonomous space situational awareness capability for Europe and integrated specialized space applications and services
RESEARCH INTO DISTRIBUTED CAPABILITIES	Spreading tasks over number of satellites (constellation and formation flying architecture, components and on-orbit networking, automated on-board data fusion algorithms)
INNOVATION	Satellite health monitoring; securing space assets, multi-sensor common operational picture, protection of critical infrastructures

Table 6: Main issues to consider avoiding disruption of space services

An analysis of the space based technologies, sensors, architectures and services for SSA European capability is needed. Initial programs at ESA and supporting activities in the Space FP7 Theme are just starting with the participation of EDA to incorporate the military needs. It is certain the exponential growing of the global market in space systems and satellite –enabled applications therefore, there is a strong need to further develop the SSA infrastructure as in the future.

7.4 Conclusions

This chapter listed a number of challenges and research requirements for improving situation awareness in future conflicts and crisis situations. Their complexity comes from the fact that the citizen is the subject of security operations and proper balance must be found between increased security and social acceptance of it. Technology platforms will enable and largely improve capabilities in this respect but of course cannot replace the human dimension in many respects, (manpower, decision-making, governance, etc)

In order to leverage surveillance of public spaces, indoor environments and vital infrastructure, improved techniques and novel methods need to be developed and deployed. This combines different modalities by fusing data from a wide range of sensors including GPS, CCTV, IR, radar, piezoelectric, THz (which see through different materials), seismic and acoustic sensors. A particular challenge is to separate dangerous objects from harmless. Integrity aspects of using such sensors need to be considered. There is a clear need to improve the sensing capabilities together with a better integration and management of sensors and platform to rapidly and efficiently respond to the security context.

A variety of different platforms are of course needed in order to build proper infrastructure to permit data gathering and further level of analysis and post processing capabilities.

The seamless integration of space applications within wider systems featuring terrestrial sensors (be they land, sea or air-based) will allow to furthermore develop a full spectrum of added value services in terms of all around the globe near real-time data delivery and data continuity. The combination of different data gathering assets and advanced techniques for data exploitation and exchange together with international cooperation between stakeholders (civil and military) present an enormous potential to improve missions' efficiency.

Novel decision support systems (including fusion algorithms and intuitive human-machine interfaces) that help analysts achieve situation awareness find unsuspected connections and get early warning of risks need to be developed and tested. Such systems will lead to faster and better decisions in all of the four application areas (security of citizens, border security, security of infrastructure, crisis management).

Data and information fusion methods and techniques for integrating information from a wide variety of heterogeneous data sources need to be further developed, including interoperable communications, direct handling of legal and integrity aspects. Data integration and semantic interoperability, information fusion and data mining algorithms that increase the security of the society need still being designed to actively protect the integrity of the citizen.

8. Working Group: Identification of People and Assets

Executive summary

Identifying people and assets is becoming more challenging and more important. People and assets are moving faster and faster. Digital services are becoming the norm for all transactions as systems and countries need to interact and exchange information. All these evolutions are completely changing the way we need to define and verify the identity of both people and assets.

In this context how can we maintain or improve security levels while also improving the facilitation of people and asset movements? In this report we present these new challenges and identify the key research domains which will contribute to the solutions.

Other key challenges include the establishment of trust in the user community, the need for faster and more accurate systems and the importance of interoperability and information sharing, associated with a well-defined policy related to the access and interconnection of large-scale databases. This report also shows how innovative solutions (like biometrics) present new opportunities to improve a system's efficiency and its security.

We recommend initiating research in five key domains:

1. **ID theft and credit card fraud**
2. **Use and evaluation of biometrics in identity management**
3. **Identification of disaster victims**
4. **Assets transport tracking and facilitation**
5. **Passenger travel security and facilitation**

8.1 Introduction

8.1.1 Context

This part of the report aims at presenting the issues covered by each work group, the identified threats and challenges attached to them and the requirements and research requirements to overcome them. In this report, we present these conclusions for Working Group 8 (WG8).

8.1.2 Presentation of WG8

Working Group 8 (WG 8) focused on the overall topic of the Identification of people and assets. We focused on a specific problem area with clear challenges, which is a high priority for Europe at present.

WG 8 is composed of 71 representatives from various public and private organisations in most Member States. Its goals are to present the threats on identity management systems currently in place, to establish the missing capabilities to face the challenges of the coming years and finally to define the research needs.

The WG8 members identified 5 major topics of interest:

1. ID theft and credit card fraud:
- Identity management in a paperless world
- Trust in the devices and systems
- Cyber security
- Securing payment through the internet

2. Use and evaluation of biometrics in identity management:
- Trust in biometric systems
- Biometric performance
- Need of liveness/anti spoofing detection
- Data protection
- Biometric revocation
- Certification of biometric systems

3. Identification of disaster victims:
- Use of biometric and biographic fusion for victim identification
- Solutions to manage rescue teams for all Member States
- Mechanisms to temporary bypass privacy protection

4. Assets transport tracking and facilitation:
- Securing multi-modal transport systems in the overall chain
- Challenges in continuous monitoring, tracking and integrity verification of assets
- Integration of travel documents and ID documents
- Detection and tracing of hazardous materials
- Secure Information sharing and collaborative instruments

5. Passenger travel security and facilitation:
- Need for proper change management and planning to build efficiency into the systems
- Move towards automated border control coupled with interoperability and the increased need for sophisticated systems
- Need for a global border control scheme at the EU level
- Entry/Exit scheme and other systems utilising central infrastructures and multiple applications
- Development of required standards in line with user needs and the standardization of tools and methods
- Increasing processing speed and comfort of travellers at the border

In the following two sections we present the threats and challenges and the capabilities and gaps reflecting these topics. In the following section we present WG8's recommendations on research needs and priorities for each of the five points of interest.

8.2 Threats and challenges

8.2.1 Establishing and maintaining trust

8.2.1.1 Complexity of trust in a paperless world

The world has rapidly and largely moved from being paper-based to a digital services world. This move brings with it many challenges and yet citizens expect high and increasing levels of security and trust which they believe they experienced in the paper-based world. In the digital world the absence of written and visual proof that characterizes physical exchanges has given rise to a demand for guaranteed or high levels of identification and authentication of parties and transactions

In 1997, the very first secure electronic identity cards were produced, and called e-ID cards. Many projects soon emerged. In Europe, Finland deployed the first operational project in 1999, Italy started the first experimental emissions on 2001, quickly followed by Estonia, Belgium, Portugal and the UK. France and Germany could follow in 2010. Securing cards is a critical issue because without it, any individual's e-ID universe can be unlocked. The security of all e-Ids, documents or certificates delivered by Governments is critical.

ID theft

The European Union is facing several challenges related to e-ID for e-Services and for e-Travel documents where identification, authentication and signature are mandatory. Identity theft is when an individual's personal information is stolen and used by a second party without the owners knowledge or consent. This is the primary threat to e-ID schemes. Statistics show that identity theft is increasing spectacularly: the latest study from the Identity Fraud Steering Committee (IFSC) of the UK Home Office estimates that identity theft costs £1.2 billion annually to the British economy[1]. In this context, special attention should be paid to data and identity for applications in the public sector as they are designed for longer life cycles and should accommodate evolving security threats.

With a threat of this magnitude, it is clear that the European Union must have a coordinated plan to fight identity fraud. In particular, it is important to reinforce the security of secure tokens, protocols, combined identifications, and both national and international infrastructures.

Certain technical and other challenges must be considered, for example the potential danger associated with contactless communications (which offer a high level of convenience to the user) but may pose their own security threat if the contactless air interface is not well managed and protected. In some un-secure context, there could be a risk of capturing e-ID data without the consent of its owner, and re-use it for non-authorized actions.

Similarly, if e-banking is to truly evolve it is essential to reliably identify parties and authenticate transactions for internet payments[2]. Chip and PIN increase security through "something you have" and "something you know". There is always the risk that a PIN number is compromised.

The next level of security can be reached by using biometrics; introducing "something you are" verifications can enhance the security of any such system.

Cyber criminality

On the Internet trusting the identity of the users and fighting cyber criminality is particularly challenging. The cost of online theft is estimated at $1 trillion per year[3]! Contrary to what happens in the physical world, with the current infrastructures, governments do not really have a means to issue proofs of identity for their citizens on the Internet. Therefore, preventing fraud and identity theft is very difficult. Proving ones identity in the real world can be done by presenting a passport or an identity card but in the cyber world we do not yet have similar mechanisms in place.

A report[4] from Fabrice Mattatia clearly shows the advantages and feasibility of using e-ID cards to solve this issue:

"The increase of identity theft and illegal access to data threatens heavily the trust in the digital world. Passwords fail to protect efficiently online services which create value by handling personal data or privacy information, such as e-government or financial services. eID cards are identity cards supporting a chip with a personal authentication key and a certificate.
Already in use in several European countries, they are a secure and user-friendly means to prove one's identity in the digital world, at low cost, and for all applications. These cards do not increase the threat to privacy, such as tracking, divulgation of privacy data, or the constitution of illegal databases, compared to traditional authentication means."

1 http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf
2 Identity fraud in banking cost 57 million Euros in 2008- APACS UK Payments Association
3 "Cybercrime threat rising sharply" – BBC news article by Tim Weber, Davos 2009
4 "The utility of electronic identity cards for a safer digital world", Fabrice Mattatia, Ann. Telecomm., 62, n° 11-12, 2007

In parallel, with the development of eID cards, the concept of an electronic signature (eSignature) is also emerging. An eSignature can be defined as any legally recognized electronic means that indicates that a person adopts the contents of an electronic message. It is another strong pillar of a trustworthy information society. However, the variety of means by which eSignature can be implemented make its generalization complicated. A European directive, published in 1999, could be used as a starting point to develop new eSignature standards in order to address the crucial cross-border interoperability challenges.

Trust in Internet payments

A large number of credit cards holders claim misuse via ID theft of other means through their credit card. There have been improvements in security in this area with some measures being standardised – for example the use of smart cards and card Pins or password protection. However, these do not prevent the use of cards by unauthorised persons if the user is not very careful with the way s/he types-in the code. The integration of biometrics to grant access to the card information is a solution. Besides, linking the user's credit card and mobile phone may add significant trust.

A key challenge is to provide a next generation payment mechanism, available on internet (but also in any mall or shopping area), based on a PIN code, a signature or a digit sequence, but with strong authentication of the user's identity to ensure trust and security.

8.2.1.2 Trust in biometric systems

What you are vs. what you have

Given the demand for strong identity assurance, biometric technologies have a unique potential, by offering the "gold standard" of true three-factor authentication. The first two factors, "something you know" and "something you have", can be satisfied by traditional username / password / token means – but only biometrics can offer the final third factor of "something you are". This provides a level of control in identity management that has never been reached before by any other technology and therefore, the trust in the identity management systems is dramatically increased both for the users and the authorities. However, we will see that there are areas that remain to be improved if we are to avoid undermining the strength of biometric systems.

Biometric data protection is key to trust

Biometric data protection, acquired by enhancing a system's robustness, is a most crucial requirement for a system to be trusted. There are mainly two classes of attacks, by which an attacker can breach the security of a biometric system or fool the system to gain access to the biometric data of a legitimate user:

- **External attacks:** the attacker tries to fool the acquisition device by showing a fake image (like a copy of a fingerprint of a legitimate user). Such attacks can be prevented with appropriate anti spoofing mechanisms.
- **Internal attacks:** the attacker is able to retrieve the template of a genuine user that has already enrolled onto the system. This can be done by spoofing the system while the legitimate user uses the system or by hacking the database where the biometrics are stored or simply by access not being adequately protected or restricted. The attacker then injects the template directly into the matching algorithm. This solution is more complex to implement as the attacker needs to interfere with components within the system perimeter.

Due to such threats, biometric data of citizens must be protected to a high level. This issue is addressed by the Personal Data Protection legislation but further measures or standards for secure deployment are required. A strict application of the Directive is very important since stealing or spoofing of biometric user characteristics, may lead to a "permanent" fake identity ownership or identity theft. We need improved security to protect the biometric data used in our systems. Some people are considering user behaviour as a kind of biometric identification.

The building of user profiles deduced from user behaviour in his/her interaction with an application may provide meaningful information to detect abnormal user operations and thus, potential identity theft. It is a major challenge in the mid-term to build and evaluate appropriate counter-measures.

Research should focus on evaluating performance and robustness of counter-measures related to internal and external attacks and, if required, as well on profiling

Tuning of biometric systems

The decision errors of a biometric verification system are measured in terms of:

- False Acceptance Rate (FAR): the expected proportion of transactions with wrongful claims of identity that are incorrectly confirmed. A transaction may consist of one or more wrongful attempts dependent upon the decision policy.
- False Rejection Rate (FRR): the expected proportion of transactions with truthful claims of identity that are incorrectly denied. A transaction may consist of one or more wrongful attempts dependent upon the decision policy.

There is inevitably a trade-off as attempts to minimize the false matches of a system tend to decrease the frequency of true matches. System designers often have to adjust threshold values to get the best combination of true and false performance measures, and sometimes these adjustments are also available to customers who want to fine-tune their own biometric deployments.

Other performance indicators such as Failure To Enrol (FTE, percentage of people not able to enrol in the system) or Failure To Acquire (FTA, percentage of people not able to have their biometrics captured for matching) can also be measured and tuned in each system. If the requirements in terms of quality of the samples captured are too high, the FTE and FTA will be extremely high. But on the other hand if these requirements are too low the system will not be secure.

While it is important to be able to adapt a system's performance specifically to a given application and environment, this can also be dangerous, especially in Border Control scenarios. In Europe for instance, we can imagine that different countries deploy systems with different performance in terms of any of the indicators mentioned above. For this reason, and to maintain a good level of trust for the overall European system, it is important to have a mean to uniformly assess this performance. Certification of the systems is one of the solutions to achieve this goal.

Certification of systems

It is challenging to define and compare security levels of different biometric identity management systems. As we just mentioned, different attacks can be carried out against biometric systems and by design the systems can achieve different performance levels. One possible approach could be to introduce a certification mechanism or a conformance mechanism. This would allow interoperability and trustworthiness through connected service providers. It is also important to define quality requirements targeted to different applications where biometric systems are required. This is of particular concern as these systems interact with people's privacy and can lead to judicial penalties.

A good example of this can be found in large-scale applications where the choice of the acquisition devices is one of the most critical issues. For example, the 10-print (4-4-2) fingerprint capture devices that will be used for the European Visa Information System (VIS) project require implementing the ISO/IEC 19794 series standard. This provides a common level of quality and mutual trust between all the participants in the project.

8.2.1.3 Trusting assets

The opportunities and challenges mentioned above equally apply to assets. With better performing technologies, but also an increased complexity of the exchanges of assets, establishing trust of physical assets is at the same time becoming more feasible but also more complex.

The best example of the challenges that have to be faced can certainly be found in multimodal freight transportation, which is a complex, distributed and unbounded network linking geographically-scattered nodes through broad and diverse flows and infrastructures covering direct air/sea/road/inland/waterway/railway connections. In such a scenario, as in any complex networked system, the weakest point always determines its overall resilience and exposure to risks.

Here are some of the challenges to be addressed to enhance trust in this context:

- Authentication, authorisation and organisational/institutional control/ruling providing guarantees for all actors involved.
- Customs control and procedures addressing inspection requirements and technological solutions for monitoring, tracking and automatic control of freight and carrier at the crossing points, during transport and the effective interaction of the authorities with the stakeholders towards a greater efficiency.

8.2.1.4 Citizens' trust in identification systems

A key link in the chain of trust is the users' trust in identity systems. With identity systems managing very sensitive and private data for millions of people (especially for government systems) we must ensure that the systems are secure and well defined to protect against key threats such as identity theft..

One of the often overlooked factors in trust is communication and it is important that the users of any identification system are provided with clear explanations of how their data is going to be used and the purpose of such use. It is well established that the public's concerns with regard to biometrics are around a lack of knowledge of the technology and mistrust of organizations that deploy and manage biometric applications. Most people are unaware of what biometric systems can and cannot do and draw no distinction between non-intrusive and potentially intrusive implementations —rendering it difficult to make informed decisions about a particular case.

For all these reasons, training for users and operators is crucial to the success of the new systems. If the training and communication around new projects is not done properly, people will not trust the systems and therefore not use them or potentially use them improperly which could lead to security breaches.

8.2.2 Identification management in a faster moving world

8.2.2.1 Fast identification of travellers

Many of today's border management organizations and processes are not structured or ready to meet the new challenges with which they are faced. Consistent and strategic coordination across border management agencies is often lacking and information is fragmented or maintained in information silos. As a result valuable information is not always available to the decision makers to whom it could make a difference.

Therefore individuals are able to cross borders without being subjected to the appropriate level of scrutiny.

Tragic events such as the September 11 attacks in the United States and the bombings in Madrid and London are stark reminders of the potential consequences of a single mistaken decision. Managing all of these challenges in a cost efficient manner, while communicating adequately to the public and conveying a commitment to protect privacy, are the key challenges for today's border management professionals.

Border control typically presents the following characteristics:

- Operated at the border station, without mobile equipment
- Processed when the traveller arrives at the border without proactive controls
- Control stations are connected to police databases, but do not use all capabilities given by Passenger Name Records (PNR) and Advanced Passenger Information System (APIS) data

Our purpose is to show the opportunity of a reasonable investment, in architectural terms, to move the border controls from reactive to proactive: people are flying and are expected in a few hours, therefore one has time to process the controls and to select who should be controlled more accurately.

Such proactive systems will require a connection to the information systems of airlines (through companies operating flights or through a special secure connection). This way, border control authorities would browse data concerning people following arrival, and select only those who need a more precise control at the border after having queried their national databases and the Schengen Information System (SIS or SIS II). All other passengers can cross the border easily and quickly.

A new global scheme could integrate **three levels of identity controls:**

- **At origin/in transit:** the details of the traveller are collected and sent to the destination. This will help focusing the efforts on travellers most susceptible to being a threat to the destination country. Furthermore, with this approach it will even be possible to deny the boarding of travellers who would be denied entry at the destination.

- **At border of destination country:** these checks are the only ones currently done. However, thanks to the first level of checks before or during travel, and by giving the police mobile devices to check and control identities at the gate of the plane, this new scheme gives a real proactive and discrete dimension to the police's action and gives more satisfaction to all the people who are no longer obliged to take their place in the queue at the border. The checks at the border also should be carried out not only to record the entry of the travellers but also their exit (Entry/Exit scheme).
- **Within the destination country:** to have a complete control over the individuals entering and leaving the country, it is crucial to also perform identity control within the borders. With the control of entries and exits at the border, the authorities will have a precise knowledge of the people who should be within the territory at any given time. Therefore it is important to be able to perform checks anywhere in the country (with the help of mobile devices) in order to be able to find the people who did not leave the country when they were supposed to or the ones who entered the countries through illegal channels.

Coping with increasing numbers of travellers

Increasing movement of people is a further challenge[5]: "Migratory pressure, as well as the prevention of entry of persons seeking to enter the EU for illegitimate reasons, are obvious challenges facing the Union and, therefore, also its policies on borders and visas."

Technology developments and scientific progress in areas such as biometrics are paving the way for new solutions to meet these challenges. Biometrics help strengthen identity solutions by integrating physical or behavioural characteristics (for example, fingerprints, facial structure, iris structure, signature and gait) with biographic identity information. Biometric technology is also being integrated into identity credentials such as travel documents (for example e-passports), visas and smart cards to reduce the threat of a criminal or terrorist assuming a fake identity or committing identity theft—a much simpler process if mere biographic information is required for validation.

The combination of biometric technology, high storage capacity chips, secure transmission technology and new authentication tools supports border management agencies in making decisions about identity and risk and strengthens the processes to rapidly facilitate known, low-risk travellers while improving security.

It is notably possible to perform automatic identity verification using electronic passport and automated gates: in such scenarios the gate has the ability to read the passport biometric information, capture the biometrics of the traveller, perform the identity verification, check the authenticity of the document and connect to watch list databases.

Coping with increasing numbers of unknown immigrants

Many non-EU citizens enter EU borders not only with temporary authorisations, like those for business or tourism, but also reach EU coasts by boat to Southern Europe without any identification documents and cannot be stopped in crowded illegal immigrant detention centres. Inevitably, the result is that a multitude of unknown immigrants move inside EU without any knowledge about them, representing a large gap in the overall security system related to border control. This could be partly addressed by issuing on arrival a temporary biometric e-ID, allowing them to move inside the EU territory, carrying out periodic checks while waiting to reconcile their identity with valid ID documents from their origin state. This can also allow following them in their process toward legal naturalisation in one the EU member states avoiding any gap from their first entry into the EU territory. In fact, in most known cases, their first request is to apply for asylum.

Benefits for the border control agencies

The benefits of a new traveller identification scheme as mentioned in this section are multiple:

- **Increased capacity:** the time required for each transaction is reduced while the level of security is increased. With the usage of automated gates the floor space required is also reduced.
- **Increased predictability:** with proactive management the variability in terms of the workforce required to perform the control can be better handled.
- **Increased security:** by using biometrics and automation the level of checks is kept the same. Border guards can focus on higher value-added activities.

---

5 "Preparing the next steps in border management in the EU" - Commission communication

- **Lower costs:** with automated gates and other automation tools, the cost per transaction can be reduced by as much as 90%. This has a direct impact on the citizens as tax payers' money is used more efficiently.
- **More pleasant experience:** with a reduction of queues the first image that the country gives to the visitor is improved.

Reducing risks of security breaches

If border guards have personal data at their disposal only when they face the person who wants to cross the border, how could two officers, for example, perform thorough identity checks with 400 people presenting themselves at the same time? Proactive controls give them time to select who they want to check with more interest and who can cross the border more easily.

It is also quite impossible to fight terrorist organisations efficiently without proactive management of border checks and controls. Proactive controls are the only way to introduce a dimension of individuality in each control and to perform complete database checks.

8.2.2.2 Fast response in case of disasters

Potential impact on citizens increases due to population growth

Here, we mainly focus on natural disasters: flooding, hurricane, tsunami, etc. Terrorist acts should remain minor, even if they have major image impact. Furthermore, climate change will increase the number of natural disasters. Additionally, population density grows in cities, increasing a disaster's impact on citizens.

In the event of a disaster, it is necessary to provide information related to the identity of the victims. The link between a person and his identity has to be re-established. The period of time included between the disaster and the restoration of identity is uncertain. It produces doubts, a bad image of crisis management and delays additional support to victims and their families.

Preventing spread of epidemic diseases

Epidemic diseases require, by nature, a very fast response. Rapidly establishing a list of victims is crucial to stop the spread of the disease. It either helps defining the danger zones or helps to contact a person who has been in contact with someone who is affected.

If we take the example of Chikungunya, as soon as victims are identified, there is an immediate effort to destroy the vector around the suspected affected area. A potential link with future victims is always established on the basis of individual interview. There is no exploitation of surveillance capabilities to identify relations and links faster.

Other agents could be smallpox, SARS[6], and H1N1. Such agents are extremely contagious and affected victims could be treated if they are contacted in time.

8.2.2.3 Continuous monitoring and control of containers

The challenges to precisely monitor the location and content of containers are becoming more and more complex and diverse. This is particularly true, as we have to look at the system as a whole. Therefore, the monitoring system must be:

1. **Multinational**
2. **Multi-cargos (different products are transported)**
3. **Multi-technological**
4. **Multi-actor (various stakeholders)**
5. **Expandable/interoperable: to not to establish a monopoly, but rather to follow an approach that can be extended to establish new «smart» procedures, new standards/data flow and new technology.**

There are mainly two types of risks that can be classified as follow:

1. **Infrastructure risks:** The terrorist has the objective to damage or destroy transport elements in order to disrupt the transport supply chain. The transport elements are in this case the terrorist's target.

6 Severe Acute Respiratory Syndrome virus

2. **Supply chain risks:** The terrorist has the objective to misuse the transport supply chain as their means to create damage or fatalities. The transport elements are in this case not the target but the means (used to transport weapons or as weapons themselves, in particular if we consider dangerous freight).

8.2.3 Interoperability and information sharing

8.2.3.1 Interoperability of systems

As we invest in new technologies and systems, it is vital to ensure they achieve their full potential. To that end we need to move beyond the "stove-pipe systems" and ensure the systems can work together in an interoperable fashion. These changes which our national and international systems are undergoing are groundbreaking. Our current lack of planning and information sharing must be addressed so we can improve efficiency in our systems and massively improve the current lack of user satisfaction.

If we deal with these key management issues at an early stage we can build security into a system from the start rather than making alterations when we realise the problems.

Traditionally, identity systems were established for one purpose and there was little or no information sharing. However, new systems, for example border and immigration systems which are now at the vanguard of national, regional and global security need to share and exchange information in a quick and reliable manner. Achieving this will enable systems to process travellers more efficiently on fast track programmes and an early detection of persons of interest.

Information sharing falls into three main categories:

- Cross-programme: Within a given agency, there may be a need to share information between projects or programmes (e.g. between visa issuance and asylum systems).
- Cross-agency: Within a government, a need generally exists to share information between departments or agencies (e.g. between border control and law enforcement).
- International: Allied nations, regional pacts, or bilateral agreements frequently necessitate the exchange of data between countries.

Interoperability is crucial to the success of any data exchange. Interoperability requires many elements to be successful: technical, architectural, interface, formatting, security and last but not least policy. In particular, a traceability and control of database access and interconnections should be well-defined starting with the system conception.
Certification of the systems is one means to achieve better interoperability or the development of standards as has been done in recent years with the ICAO standards on passports. However, one needs to be vigilant as these now interoperable systems need to be protected against their own inherent vulnerabilities. Ultimately, a lack of system interoperability will limit these new systems and undermine the sophisticated purposes for which they are required.

As far as standards are concerned our continued failure to agree on certain matters and put in place all required standards (for example fingerprint template interoperability) continues to hold up our ability to exploit and maximise our use of available and new technologies. Also it hinders innovation and R&D as developers still do not have roadmaps for all requirements as yet.

8.2.3.2 Tracking international movement of assets

There is no single system governing all the international movements of assets; in fact, freight transport is characterised by complex interactions among multiple actors, industries, regulatory agencies, modes, operating systems, liability regimes, legal frameworks, etc. Actors involved are numerous, disparate in nature and activity, operate on tight margins, and, as a result, represent more of a security risk than their larger counterparts further down the chain (i.e. large airport, port and maritime transport operators).

Cross-network optimisation of security measures is extremely difficult. Each component of the system has tended to seek to optimise its own operations and, in some cases, ensure that these are compatible with the next link in the chain. However, it is a well-known tenet in logistics management that the aggregation of individually optimised links leads to a suboptimal logistics chain. Un-harmonised or inexistent security practices, incompatible operating and information management systems,

uncoordinated regulatory frameworks and unclear security continuity protocols among the different links in the transport chain – and especially at its outer edges – all represent security vulnerabilities that stem from the lack of a coordinated approach to securing the container transport chain.

8.2.3.3 Cooperation between Member States in case of disasters

Identity Management of rescuers is essential to provide appropriate support (doctors, fireman, etc.). When multiple Member States collaborate on dealing with a disaster, each Member State is in charge of a non-overlapping zone because coordination of support is not interoperable. Due to discrepancies with identity and skills management, it is difficult to transfer rescuers from one zone to another.

Collaboration among rescuers will also become more and more important as it is estimated that disasters and victims impacted will increase in the forthcoming twenty years. Member States of the European Union should collaborate more and more to provide assistance to victims. Assistance could be located within the European Union or in various places around the world.

8.2.3.4 Business models

Finally it is worth noting that the points raised above, with its accompanying extensive list of requirements, will have a financial impact on those who are purchasing, designing or implementing these new systems. The issue of cost is often avoided or shied away from, resulting in a lack of appropriate financial planning, inefficiencies and cost overrun as well as security being viewed primarily as a cost.

However, this is not always true and as some innovative schemes in recent times have shown that security cannot only be seen as a business or service that consumers want to buy (for example citizens in the US and the Netherlands voluntarily pay for a scheme that enables them to be fast-tracked through certain airports) is a service that provides security and pays for itself, but also a service that can reduce costs by tackling overstaffing and providing automating border processing. It is important therefore that we understand the potential cost impact of these changes as well as the potential savings and related opportunities, and consider appropriate business models for these new systems.

8.3 Capabilities and gaps

8.3.1 Technology maturity for people and asset identification

8.3.1.1 Biometric systems performance

Current FAR/FRR and possible improvements

The most important threat on any biometric system is the danger to grant unauthorised access, due to false positive identification (FAR). Another important threat is the denial of access threat, due to false negative identification (FRR). As we already mentioned lowering the FAR leads to an increase of the FRR and vice-versa. However, certain biometric traits do lead to better overall performance than others. For instance, among the two biometrics used in e-passport (face and fingerprints), fingerprint recognition is clearly recognized as more secure.

Technical improvements of capturing devices and matching devices should be encouraged as they can lead to better performance. For example, the usage of very high definition cameras to capture the face can help analysing the structure of the skin. Fingerprint capture and matching technologies could be improved in a similar manner, by the processing of additional details.

Multimodal fusion

A unimodal biometrics system uses a single biometric trait to verify/identify an individual whereas a multimodal biometrics system uses several traits together to achieve superior performance or can apply to situations where one or more of the available traits are needed for the identification.Thanks to the advances in fusion techniques, multimodal biometric systems have many benefits such as:

- Being more fit for purpose - some biometrics work better for a given function, application, or environment than others
- Improve accuracy – fusion of a number of biometrics or other can reduce error rates that one security mode can exhibit
- Increase security. Use of multiple biometrics, or a biometric with another type of authentication (e.g., smartcard), increases the number of authentication factors, and thus makes potentially successful attacks more difficult to implement. This is also one of the countermeasures against sensor spoofing
- Improve efficiency. When acceptance of some of the available traits is achieved in a faster way
- Increase user comfort by faster, easier and more accurate checks

With the generalisation of Extended Access Control (EAC) in biometric e-passports, it will be possible the advantage of the modalities available (face and fingerprints) and, depending on the system context, use either one or both at the same time through multimodal fusion.

Liveness detection

Liveness detection is a key mechanism to prevent spoofing using fake biometric samples (picture of a face, latent fingerprints collected on a sensor, etc.)

Liveness detection techniques can be classified into three main categories[7]

- Intrinsic properties of a living body. The system measures physical properties (like elasticity), electrical properties (like resistance) or visual properties (like colour)
- Involuntary signals of a living body. The system captures the signal every living body emits. Such signals can be perspiration, blood pressure or pulse for example
- Bodily response to external stimuli. This possibility is also called the challenge-response technique. The challenge can be voluntary (requires the user's cooperation: he is asked to perform an action) or involuntary (reflexes such as pupil dilation or the knee reflex of the user are tested)

As a single protection mechanism cannot prevent all possible attacks, a good liveness detection scheme should combine few of them and use a fusion algorithm to provide an output on the "liveness probability" of the sample.

Of course, a more traditional and yet very powerful way of fighting against external frauds is the surveillance of the system by an operator. This probably remains the most efficient liveness detection system.

However, as more and more biometric systems are built to avoid requiring a human presence, the liveness detection techniques will become more and more crucial to the success of biometric deployments.

In most systems, the anti-spoofing capabilities are not yet very powerful. Biometrics vendors should be encouraged to develop these techniques and the anti-spoofing performance should become crucial criteria when implementing new biometric systems. Human surveillance should be considered as a transitional solution as long as the anti-spoofing techniques are not fully satisfactory.

Revocable biometrics

With the development of biometrics a certain fear of "losing" control of one's identity has appeared. The argument is that the objectives of the systems can change and then the biometric data can be used for an additional purpose (different from the original), so the systems should also be able to guarantee the usage, share or cession of biometric data. An enhancement will be that when biometric data is collected, it is to associate the usage.

An important question which has not yet been answered is whether biometrics can be revoked, i.e. if a person needs to change identity or finds that his/her biometric data has been compromised, what can be done to revoke that person's biometrics. This question will assume even greater importance as biometrics are diffused and become part of everyday life.

7 "Biometrics Liveness Detection", Accenture Biometrics Technologies Whitepaper 2009

Behaviour analysis

One possible way to prevent identity theft or misuse of biometric traits is to be able to measure the user behaviour to derive the coherence with previous uses of the services, and thus the potential presentation of a biometric credential by an intruder. User behaviour may also be used to detect a user acting under unexpected conditions that may be forced by a kind of kidnapping act: the stress, the face contraction, etc. could be used. Abnormal behaviour needs to be extended to vehicles and assets in general where the person is always involved in the process as a driver or a controller.

But some difficulties exist and require further work:

- First, these practices may be against the Personal Data Protection Directive, and study of legal implications and limits should also be an issue of research
- Second, there is no standard methodology to evaluate the security of a behaviour detection system

Standardisation Status

Standards are critical to the proper and robust development of the biometrics and identity management market place and technologies. Contrary to common perception there are many standards already in existence for many technologies. However some key cross technology areas remain to be properly addressed as for example security, interoperability and performance. This standards harmonization will be key to the success of future biometric systems' operations.

The need for enhanced security technologies drove and accelerated the development of identity related standards. With regards to biometrics, in addition to the ICAO standards, relevant biometric, ID/smartcard, and security standards have been developed in ISO (i.e., JTC1 SC37, SC17, and SC27). Although there is still a long way to go towards achieving interoperability in terms of technical specifications, it is important to note that these standards exist and they should be promoted and developed.

Extended Access Control (EAC) requirements

With the EAC process, the time needed for reading the chip in the e-passport is estimated to be 6 to 9 seconds for 40 Kb data read. It would be interesting to break down this time:

1. Is the maximum communication speed reached by the reader?

2. Are there waiting times (calculation of the keys, data encryption)? Is it possible to count and measure these? How long do they take? Is it possible to reduce these? If so, how?

3. BAC reading seems to be very smart. Has the difference of reading time with the EAC control been identified: availability of certificates? Latency time between two readings? Calculation time for the keys? Exchange data's encryption time? Are these times attributable to the reader, to the chip, or to both of them?

At border control, time is money and the EAC process execution time is a critical factor. It would be interesting to answer these questions, especially for airport administrators. In addition, it is important to assess if the considered technical solutions (RSA key, elliptic curve) will be able to reduce the time of border control on complex airport platforms such as Heathrow, CDG, Frankfurt, Schiphol and so on.

Of course, the main reason for introducing biometrics is to increase security and the sense of security. Although increased efficiency in law enforcement does not directly improve security, it can be argued that the use of biometrics acts as a deterrent to criminal, illegal or anti-social activities. In this respect, overblown claims about the performance of biometrics may actually prove helpful.

Fingerprints consist of particularly sensitive personal data. Their access, for any check or verification operation needs to be strongly secure. Therefore, even though we want to reduce the reading time, it is critical to maintain a high level of data protection. This is achieved by having for each Member State an infrastructure of keys management and cryptographic mechanisms.

A Certificate Policy (CP) is put in place to achieve trust and sufficient interoperability between the Country Verifying Certification Authorities (CVCAs) and Document Verifiers (DVs) of different Member States for the EAC-PKI to operate.

This Certificate Policy is established in accordance with Article 5.5.3 of the Technical Specifications on Standards for Security Features and Biometrics in Passports and Travel Documents issued by Member States, set out in Commission Decision C(2006) 2909 of 28.06.2006[8]. The Certificate Policy only concerns the use of certificates to control access to fingerprint biometrics on Extended Access Control enabled passports and travel documents for the purposes of border control. This provides a common set of minimum requirements upon which each Members State shall base a National Certificate Policy for use of certificates for border control purposes.

A National Certificate Policy must, as minimum, meet the standards of this common Certificate Policy but may place further restrictions on the control and usage of certificates within that Member State. A Member State must not require a DV in another Member State to adopt restrictions above those in this common Certificate Policy as a pre-requisite of issuing a certificate to that DV.

Security and scalability with Match-On–Card

A new type of middleware for biometric identification is emerging in the form of software embedded on smart cards. These applications offer a lot of opportunities especially in terms of scalability of the system. In these systems the user is "carrying" part or all of the application. One approach which will gain momentum in the coming year consists of Match-On-Card (MOC). In these solutions, the matching is done on the embedded software itself. This solves part of the privacy issues and facilitates interoperation among applications. Furthermore, as the enrolled sample or template does not have to be retrieved from a central database this solution is also faster.

Match-on-Card has the privacy advantage of storing the fingerprint template within the card, making it unavailable to external applications and the outside world. In addition, the matching decision is securely authenticated internally by the card itself. It has the security advantage of being far more secure than matching on a PC or server, as the fingerprint never leaves the secure environment of the card and no biometric data ever has to be transmitted over an open network. It has the interoperability advantage of being an open system: the MOC process does not require any special capabilities of the biometric or smart card reader. It is also fully scalable, offering a good solution to remote authentication without the need for a large infrastructure. This means there is no limit to the number of possible users when rolling out Match-on-Card. It also reduces the security requirements on the infrastructure itself. Furthermore, there is no need for network resources or server processing, and the need for human presence during authentication is reduced. For all these reasons, MOC is cost effective.

By adopting Match-on-Card, organisations have a secure way of adding fingerprint security to smart cards, to replace or supplement the traditional PIN/password approach found in Web based security. Match-on-Card makes it possible for biometric technology to be used in non-government applications, as it does not require strong certification of the matching infrastructure.

Government cards using biometrics Match-on-Card present several advantages to the private sector. They offer stronger security than PIN-based cards, and private sector organizations can accept government-issued Match-on-Card cards for local identity verification without having to connect to government systems, thus protecting privacy.

The technology could also be deployed with many benefits to open systems. For example, Belgium's electronic ID card is used to identify the cardholder for many Web based applications, including chat rooms (so that the two people talking to each other are of a similar age, rather than an adult preying on a child, or a child pretending to be over 18 to access adults-only chat rooms); for retail applications such as eBay, where strong security is needed when purchasing an item; for digital signatures for credit and tax payments; and for voting.

8 Not published in the Official Journal - available on http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm.

Currently, Belgium's ID uses a PIN, and biometrics could be introduced with Match-on-Card. With such a system, any third-party organization can ask the card for the identity of the cardholder using a simple Application Programming Interface and reusing the tokens provided by the government. And registered traveller cards issued by an airport and accepted by other airports throughout the world could benefit from a Match-on-Card based card that could be used for check-in, security access, boarding and baggage control, as long as there is trust established between the issuing and the accepting authority.

In the health care sector, which often involves both public and private partners, there is a growing trend towards issuing smart cards to patients so they can enjoy more convenient and secure access to services. Security could be further improved by the addition of Match-on-Card, ensuring that only those entitled to treatment receive it.

MOC can also be performed with multiple biometric traits, enlarging the potential application fields and scaling different strengths of the identification systems.

8.3.1.2 Portable devices for identity verification

Usage for proactive border control

The success of biometrics at border control will depend largely on the method of implementation. The face has been chosen by the ICAO and EU as the primary biometric identifier. But face recognition is currently one of the less accurate biometric technologies. It suffers from technical difficulties with uncontrolled lighting and it therefore may be necessary to install the face recognition readers in booths where lighting conditions are carefully controlled. Measures, such as this one, may lead to improvements in accuracy but also to an increase in costs.

Multimodal systems are those which combine more than one biometric identifier. As we already mentioned, it is currently planned to use face and fingerprints in EU border control systems as EAC becomes more and more widely used. Research initiatives have been launched on the application of multimodal biometrics in mobile communications (e.g. mobile telephones and other devices). However researchers need more test data and there is still much work to be done.

How to manage certificates?

Managing certificates in a mobile environment is very complex. But it is very important to investigate the possible solutions as most of the data stored in the electronic documents will soon require a certificate infrastructure to be read (with the generalization of EAC). So we need to find solutions to the following issues:

- How to allow a constant access to the database of certificates with embedded devices
- How to make different public keys, issued by all Member States, available for all fixed and/or mobile receivers in the whole Schengen area
- By what means does the software "know" what certificate to ask for from the server?
- What are the means of conservation (even temporarily) of certificates in embedded devices?

Usage in situations of crisis

The challenge, in a situation of crisis, is to collect the maximum amount of data from victims as the set-up of victims' lists is essential to manage the rescue effort. The collection of information has to be done efficiently even though a lot of victims may be unconscious or shocked by the disaster and most of them will have lost their identity documents.

Therefore, it is crucial to use, not only alphanumerical data as is primarily the case today, but also data collected from all kind of sensors, like biometric data (face, DNA, fingerprint or reader to assess (like mobile phones), as well. The system should then be able to identify the victims using limited information from one or more of these sources.

A legal aspect of this challenge is also to create circumstance mechanisms that bypass privacy protection for the purpose of victim identification (it is not yet the case for post-mortem identification, but is should also be the case for ante-mortem identification).

The need for more resistant sensors/capture devices is also very important to be able to improve crisis management. Most of the current portable devices are not resistant enough to be used in harsh conditions.

8.3.1.3 New practices and technologies to be used for tracking assets

Securing assets throughout the entire delivery process is a complex problem. The most natural approach is to secure containers as these are used in all modes of transportation.

In order to improve the security at all levels, more than one technological solution may be implemented, which however must be developed in a collaborative fashion in order to secure the seamless support of long, trans-national and global supply chains. Not only the technological dimension, but also the organisational dimension must be addressed.

The potential technological solutions to be developed are:

- Integration of travel and ID documents providing an appropriate level of security and greater efficiency of the overall supply chain, including interoperability with existing systems and other systems outside the EU.
- RFID-based systems for assets, containers and related seals, in addition to the associated management processes in small areas, able to be de- and re-activated on demand and by using multi-protocols.
- Intelligent sensing solutions (including GNSS[9]) allowing continuous monitoring and tracking of the load unit and its content in large areas taking into account the whole spectrum of influential parameters for commercial, legal, and transport continuation purposes.
- OCR[10] systems for the localization and recognition of the standard ISO-codes of containers and for the identification of truck/lorry licence plates and railway wagon codes.
- Advanced technology for detecting and tracing hazardous materials, like plasmonic, photonic, or Quartz crystal microbalance technologies.

8.3.2 Better planning

8.3.2.1 Moving towards automation of border control and other key application areas

The border control domain faces increasingly sophisticated requirements and demands with the ongoing implementation of new procedures and processes and new and more efficient technologies to ensure that legacy systems and processes are appropriately updated or replaced.

One of the key factors in the successful achievement of this goal is better long-term planning and consideration given to change management vis-a-vis these new systems. Failure to plan and build efficiency into systems from the start will result in major user satisfaction and management issues.

This gives more weight to process efficiency and provides for overall cost savings. But at the same time, ensuring that the law enforcement requirements and civil security initiatives are respected remains the principal objective.
Customer service and fraud reduction business cases increasingly leverage technologies enhancing both security and convenience, such as improved x-ray scanners, RFID and biometrics.

Biometrics, for example, can be used to:

- Expedite pre-vetted, registered travellers or users (for example employees) through inter alia border control points or fast track lanes at border crossing points.
- Help reduce fraud prevention within high risk caseloads such as refugee and asylum processing.
- Help reduce fraud prevention in critical processes such as immigration and citizenship.
- Provide effective and flexible watchlists which enable greater efficiency and thorough security processing.
- Process the majority of travellers through automated e-gates.

Many of these systems/solutions will be expensive, although not prohibitively.

9 Global Navigation Satellite System
10 Optical Character Recognition

We need to develop appropriate business cost models to manage how such matters will be paid for: who will be the service provider and hence will governments, airports or the citizen end up footing the bill? There are a number of projects and jurisdictions where we can and should learn lessons from, such as our own EU systems. As already stated, once the initial cost is overcome, these systems can drastically reduce operational costs. This important aspect should also be detailed in the related business cases.

In summary some of the key capabilities and gaps are as follows:

- Lack of effective planning and the need to factor in Change Management from the start
- Need to consider appropriate and new business models focused on efficiency and cost reduction
- Develop new and required standards for key identity management matters such as interoperability and other matters

8.3.2.2 Deployed infrastructure are not using all electronic security features deployed into secure ID documents

People may hold secure electronic identity documents while the legal infrastructure is neither adopted nor deployed. E-Passports are a good example: they are already deployed in Europe even though border controls are not able to verify such an electronic document. The verification is almost always visual. Over 60 countries have started issuing e-passports, and there are around 100 million e-passports in circulation, but less than 10 countries[11] effectively use readers able to read the data from the chips.

The potential reasons for this situation might be that countries wait for the EAC and are put off by the slow reading times (7s for older chips). That's why it is important to concentrate the effort both on the generalization of EAC and on the system's performance.

The potential reasons for this situation might be that countries wait for the EAC and are put off by the slow reading times (7s for older chips). That's why it is important to concentrate the effort both on the generalization of EAC and on the system's performance.

A similar situation can also be considered with e-ID cards. Many countries in Europe have already started to issue e-ID cards but these cards are not used as widely as they could.

The reasons for that are probably similar to the ones mentioned for the e-passports with the addition of the lack of interoperability among countries. Establishing a standard, or using an existing one like EAC, is necessary.

8.3.2.3 Better usage of API/PNR and ESTA

As already mentioned, in the future global border control scheme, we need to move the border controls from reactive to proactive. This can be achieved via a connection to a secure information system (through companies operating flights or through a special secure connection), so that passengers will be checked by the authorities during the flight, and only those who need a more accurate control at the border will be actually and physically checked. Solutions such as Passenger Name Record (PNR), Advanced Passenger Information (API) and Electronic System for Travel Authorization (ESTA) already exist and should be more widely used to achieve this goal.

In the travel industry, a PNR is a record in the database of a Computer Reservation System (CRS) that contains the travel record for a passenger, or a group of passengers travelling together. The concept of a PNR was first introduced by airlines that needed to exchange reservation information in case passengers required flights of multiple airlines to reach their destination ("interlining"). For this purpose IATA defined a standard for the layout and content of the PNR.

The border control authorities could use the PNR to perform detailed checks and risk profiling on all the travellers as the PNR long before their actual arrival in the country.

The APIS is a system established to enhance border security by providing officers with pre-arrival and departure manifest data on all passengers and crew members. The information in the APIS is recorded when the passenger boards the plane. With better use of APIS, part of the border control could be moved to the point of departure of the passenger so that those who would anyway be denied entry at their destination would not even obtain authorisation to board the plane. It is also interesting to note that industry is supportive of capturing API and PNR data.

11 Edgar Beugels, Frontex, presentation at Security Document World Conference, London 2009

The Electronic System for Travel Authorization (ESTA) is another means by which we could increase the proactiveness of border control. It can be seen as a lightweight visa for travellers entering a country with a visa waiver status. The idea of the system is that airline passengers register with the destination government in advance of their travel. Once screened, passengers are subject to reduced screening as their records will be kept on file for few years. This solution reinforces the level of security for third country nationals and also facilitates the control of most travel as details can be checked in advance. The EU is planning to possibly introduce such a system. The US has introduced their ESTA system in January 2009.

8.3.2.4 Differentiate various types of traveller at the points of controls

Travellers will be able to cross the border more efficiently if they are in possession of highly trusted and secure documents and/or if they complied with pre-registration schemes (like ESTA).

Whenever possible when a passenger arrives at border control carrying the proof of identity the controls should be faster. This has the advantage of motivating people to comply with all possible security requirements and as a result help the authorities to focus on the people who represent the highest threats.

8.3.2.5 Coordination required for effective implementation of EAC

While there has been some focus on national certification systems, a lot of work still remains on international aspects of creation, distribution, exchange, update, and revocation of EAC certificates.

There is a risk that without any coordination at the European level, the system will not get a chance to develop itself, and real interoperability shall remain a chimera for a long time. If this happens, flaws in systems addressing the fight against terrorism and illegal immigration, which should be always based on the MRZ reading and on the single Basic Access Control (BAC), will remain.

Furthermore, industrial partners who have invested for years significant technological and financial efforts to provide real interoperability between the Member States in the EAC protocol would not understand if their efforts were not supported by strong political will.

8.3.3 Importance of uniform legislation

8.3.3.1 Legal discrepancies create weakness points

Legislation in the physical world

Some identity documents are less secure than others. Without very strong cooperation and harmonisation among the Member States, low security identity documents could be used in some countries when they are refused in others. Such legal discrepancies could facilitate terrorism activities. No matter how strict the laws are in a given country, if a single Member State is more permissive then it is the entire security of the Union that is weakened.

Legislation on the Internet

The Internet is growing inexorably all over the world in all directions and in all areas: messaging, e-commerce, electronic data, files, photos and videos, newspapers and forums. To oversee the billions of electronic communications of all kinds, States have undertaken a legal revolution by signing a large number of international conventions on copyright, trade and the electronic signature, cybercrime, data protection, patents, etc. However, the Internet continues to remain outside the legal, judicial and criminal sovereignty of the states.

As stated in a report on data breaches[12], the cyber criminal operates with several distinct advantages:

- Higher yield—vulnerable systems hold information on tens of thousands of victims.
- Less target resistance—when breached, systems tend not to fight back and many do not keep a record of what happened.
- Low target sensitivity—it often takes system owners weeks or even months to discover a breach. This allows the criminal to harvest information over a longer period of time.
- Easier escape—when they are detected, it is significantly easier for the cyber criminal to run and disappear.

12 "2008 DATA BREACH INVESTIGATIONS REPORT" – Verizon, 2008

This situation is due to the lack of a global international organisation setting the rules of the internet.

Knowing this, the terrorists will always try to attack the network from the countries where the laws are the most permissive. By complying with a weak law in a given country they can "legally" threaten the rest of the world.

As reported by Tim Weber in an article for the BBC «the internet is a global network, it doesn't obey traditional boundaries, and traditional ways of policing don't work[13]» . Therefore, it is extremely important that we study the possible solutions to protect ourselves and develop global uniform legislation.

8.3.3.2 New border management issues

Coping with an enlarged area of freedom

The number one challenge is coping with the border management of an enlarged area of freedom within which there are no internal borders :

"The dismantling of the EU's internal border controls is one of the greatest achievements of European integration. An area without internal borders, which has expanded from seven countries in 1995 to 24 countries at the end of 2007 – a unique, historic accomplishment –, cannot function, however, without shared responsibility and solidarity in managing its external borders[14]."

Managing asylum in a fair manner

Another important challenge for the EU is to standardise the asylum application procedure across Europe.

It is considered that harmonisation of procedures will lead to greater consistency across Europe in handling asylum applications and consequently the system will become more efficient and operate more swiftly[15]:

"Establishing a minimum level playing field throughout the European Union by introducing guarantees for a fair and efficient procedure will commit Member States to reduce the differences in national systems and align their systems on the basis of these standards."

The UK Home Office is prioritising the introduction of procedures for the pro-active determination of asylum applications and the expedited removal of those without a valid claim to remain in the UK:

- Fast-tracking asylum decisions, removing those whose claims fail and integrating those who need protection
- Ensuring and enforcing compliance with UK immigration laws, removing the most harmful people first and denying the rights and privileges of residing in the UK to those there illegally

Insider Threats

We need to consider and factor in the non-obvious populations into the systems we are building. The majority of our new systems are focused on travellers whether they use a passport only or also in addition to a visa. As has been recognised in other jurisdictions we need to consider the threat posed by internal populations.

The US, UK and Australia are already introducing programmes which manage or examine the internal threat posed by the regulated workers and populations such as the police, the x-ray screeners in airports, etc. There is a stereotype of the individual who poses the greatest potential threat.

Along the same line, it is also important to have a common agreement on the number of fingers that will be used for biometric enrolment in registered traveller programs and other similar systems. This needs to be decided by Member States in cooperation with the European Commission.

13 "Cybercrime threat rising sharply" – BBC news article by Tim Weber, Davos 2009
14 "Preparing the next steps in border management in the EU" - Commission communication
15 Impact Assessment associated to "Preparing the next steps in border management in the EU" - Commission communication

8.3.3.3 Privacy protection

Need to comply with the Data Protection Directive

As we already mentioned, biometric models of citizens may not be used anywhere without an adequately high level of data protection. This is addressed by the Personal Data Protection legislation and therefore a common legal framework is in place for all Member States. However, as with any directive, differences in the actual implementation in the Member States law should be assessed. Furthermore, all the Member States should really take the appropriate actions to effectively ensure a proper protection of privacy as stated in their laws.

There is also a need to find a trade-off between interoperability of biometric databases and the principle related to the mandatory ban to interconnect specific databases. In practice, this means that users who have accepted to be enrolled in one application would be introduced as authorised users in another application, without any explicit consent, impersonating this consent on the behalf of the user.

The collected biometric data should be used only for the use technically and legally associated with the data at the enrolment stage, and the threat of misuse of this information should also be addressed.

Privacy Enhancing Technologies

The EU Commission itself has classified biometrics as a privacy enhancing technology and it is understood that the Commission would wish biometric technologies to be developed more towards the preservation of users' privacy[16], an opportunity that has often been downplayed in discussions on these technological deployments. For example, a securely-designed access control system using a fingerprint or iris recognition biometric can offer a better solution for a medical database system, for example, than traditional techniques. In this way, a biometric identifier can be a positive measure to improve the privacy of the individual.

A promising new area of privacy enhancing technologies that have not yet really come to market are tools to de-identify information in databases. These include tools to selectively "scrub" data so that just enough data is removed to ensure that it is non-identifiable (including removing entries that might identify an individual because they describe characteristics that are likely unique to that individual). In addition, research is underway on techniques for adding randomness to data before it is added to a database in such a way that individual data is not reliable but aggregate data remains useful.

8.3.3.4 Information sharing for assets tracking

Administrative harmonisation is crucial for transnational transport chains, in order to accelerate cargo movement particularly at border crossing points. Solutions must be developed to share information for vessel/cargo tracking. This information must be accessible to all relevant stakeholders.

Special attention should be paid to customs control and procedures. With an iterative approach we could clearly understand the inspection requirements for automated control of cargo at the border crossing points and during transport. It is also important to facilitate the interaction between the authorities and the stakeholders.

The complexity of transportation systems makes information sharing particularly challenging. However, advanced technical solutions (such as the ones described in section 13.2.2) can help us to build efficient automated information sharing systems as long as the requirements and needs of all stakeholders are harmonised.

8.4 Research needs and priorities

8.4.1 Technological needs

8.4.1.1 Faster and more secure identity checks

The goal would consist of being able to process a complete ID check and control including database queries in less than 10 seconds. This could be achieved mainly by enhancing the speed of biometric (EAC) controls at the border and during checks in the field: this would enhance security for all parties.

16 Europe Information Society, Privacy Enhancing Technologies
http://ec.europa.eu/information_society/activities/privtech/index_en.htm

8.4.1.2 Improve trust in biometric devices

We need to have robust technologies that make systems or solutions much harder to spoof or fool by building in enhanced security measures such as liveness detection and anti-spoofing measures such as heartbeat detection. Ideally we would need to be able to create biometric models specific for a given need and to ensure proper policy management so that issued "identities" can be updated, revoked and reissued. The research should aim at enhancing the accuracy and robustness of biometric devices.

To reach this goal, many potential solutions should be explored:

- Development of secure biometric acquisition systems
- Evaluation of non zero effort attacks (internal and external) on biometrics systems
- Development of new and innovative biometric sensors able to operate under critical conditions that are typically found at a disaster scene
- Acquisition devices and system certification
- User behaviour and postural recognition, promoting "person identification" beyond biometric traits and avoiding identity theft
- Create biometric model-specific to a use
- Investigate multi-biometric traits application benefits and increased performance

8.4.2 Systemic needs

8.4.2.1 Combating identity theft

No coherent approach to address this threat is currently in place. It requires a concerted effort involving significant advances in processes and technology. The current lack of solutions costs companies, countries and citizens billions of Euros in fraud and theft and undermines global and financial security. The problems come from a lack of joint approach, a lack of trusted authentication and enrolment processes, and an ongoing and increasing lack of trust.

In order to efficiently fight these frauds, systems and technologies should perform mutual recognition between regional, national and/or European systems. Standards and retro-compatibility management should also be developed and agreed at the Union level.

Privacy management of stored data should also be handled appropriately. Systems and architectures should allow the management of different electronic ID in different contexts (public vs. private, region vs. Europe, etc.). Finally, on the legal aspects, responsibility and liability matters for fraud should be addressed at national and international levels.

The solution to overcome these challenges would be:

- Development of agreed processes and standards
- Use of strong authentication processes and technologies
- Development of secure enrolment processes and technologies
- Solutions to provide for secure on-line transactions (secure payment on the Internet based on eID and banking smart cards)
- Education and training for all stakeholders and users on the threats and preventive measures
- Harmonise the security level of all identity documents; i.e. have the same requirements in term of technical requirements and proof (security evaluation criteria and security targets)
- Harmonise national legislation between all EU Member States for all applications where eID is mandatory (travel, e-Services, driving licenses, eHealth, etc.)

8.4.2.2 Mobile identity checks

As mobility of people is becoming a central factor of behaviour and life, the use of new identification technologies to support and improve law enforcement should contribute to ensuring the security of society. In the same manner, the growing need for flexibility generates a need for appropriate technologies and processes to achieve the required security level.

Mobile ID devices may be used for a variety of situations where a stationary check point is neither possible nor practically feasible. Common applications include: flexible immigration and border control needs in non-stationary environments, identification and verification in law enforcement applications, access control for buildings, computers, and networks in flexible application environments.

The main challenge is to define the interoperability needs and related criteria for checks and controls at the borders and in the entire Schengen Area.

We should foster the realisation of mobile checks and controls, and prepare the generalisation of EAC checks and controls on mobile devices everywhere within the Schengen Area.

8.4.2.3 Intelligence-led border management

In synergy with the use of mobile devices, it is important to implement secure data transfers in order to optimise the use of PNR and APIS data and to process proactive ID checks and controls at the border.

Currently, border control is performed at the border control booth, without mobile equipment. The control is executed only in a reactive way when the traveller arrives at the border point. No proactive controls are operated. Control posts are connected to police databases, but do not fully use all capabilities given by PNR and API data.

Border guards, via a better and systematic analysis of PNR and APIS data, could beforehand select persons who have to be more thoroughly checked, at the gate of the plane (or the boat) with mobile devices connected to databases through a secure network. Such controls will be more efficient, faster, and more precisely oriented to screen wanted persons (national, SIS or Interpol alerts).

8.4.2.4 Disasters and emergencies management

In the event of a disaster, it is necessary to provide as soon as possible information related to the identity of victims. The period of time between the disaster and the restoring of identity management is generally uncertain and creates discomfort and uncertainty. It produces doubts, a poor image of the crisis management on the part of governments and delays the execution of additional support actions to victims.

To improve crisis management the following solutions should be developed:

- Software mechanisms to build up an identity service based on heterogeneous information (biographic and biometric).
- Develop identity management production that can deliver credentials to victims.
- Standardisation of rescuer identity, skills and credentials to allow interoperable command and control cooperation.
- Electronic wall-mechanism to supervise disaster border zones to manage access rights and to protect victims from unauthorised reportage.
- Build robust, portable and autonomous tools to digitally collect victims' information on-site and in real time, including information sharing via a secured network.

8.4.2.5 Harmonised global border control

In the domain of border control there is currently a lack of change management, planning and system interoperability. As a result new systems are limited and will ultimately not be fit for the sophisticated purposes for which they are required. Furthermore, it hinders innovation, and R&D professionals in the domain still do not have roadmaps for all requirements.

These challenges should be addressed by developing the following:

- **Automated border control** to leverage the increasing number of electronic travel and ID documents and to manage the associated technical and legal complexities.
- **Move the border controls from reactive to proactive** through a connection to a secured information system (through companies operating flights or through a special secured (wireless) network connection), so that passengers will be checked by the authorities during the flight, and only those who need a more detailed control at the border will actually be physically checked.

- **Mobile devices to check the identity of persons** should be developed and deployed at European level **throughout the countries** and not only at border crossing points.
- **Need to manage the threat posed by the regulated workers** and populations such as the police and the x-ray screeners in airports. We are currently too focused on the more visible populations – passport and visa holders. Failure to secure these new populations is a major gap in our security as we ignore a potential major threat.
- **Develop standards required to ensure true interoperability** of secure documents and systems.
- **Architecture -** Require architectural support and clear interface specifications including data formatting and security for the new systems and use central infrastructures for multiple applications – removing redundant and/or isolated "stove-pipe" systems (SOA).
- **Policies –** Develop appropriate policies and procedures for the handling of exchanged data.
- **Support best of breed technologies -** Examine new software approaches such as, notably, SOA for service/component reuse, scalability, interoperability, flexibility, and maintainability.
- **More secure systems -** Examine use of multimodal biometric systems to ensure that systems are fit-for-purpose, improve accuracy, and increase security.
- **Efficiency versus accuracy trade-off –** Examine benefits for efficiency promotion in terms of expected time, strength of the systems and accuracy of the biometric check.

8.4.2.6 Improved assets tracking

An important effort has to be invested to increase the security of physical assets transportation. The complexity of the networks involved (multimodal, multinational, multi-technological and multi-actor) requires the use of very sophisticated technologies.

We believe it is necessary to invest in the following domains:

- Innovative tracking devices (e.g. RFID-based systems) for assets, containers and related seals.
- Intelligent sensing solutions using state of the art technologies (including GNSS) allowing continuous monitoring and tracking of the load unit and its contents.
- Integration of OCR systems for the localisation and recognition of the standard ISO-codes for containers and for the identification of truck/lorry licence plates and railway wagon codes.
- Advanced technology for detecting and tracking hazardous materials.
- Develop a family of portals for logistics monitoring and management, fully interoperable and interconnected supporting standardised software and hardware communication interfaces and information flow.
- Need for a single system governing all international movements of assets.

8.4.2.7 Harmonised EAC certificates management

The goal is to build a common structure on the example of the Schengen Information System (SIS II) or VIS, which should be operated and run by one or two voluntary Member States (one principal site, and one rescue site). Define in particular common rules for the creation, distribution, update, exchange and revocation of certificates between the EU Schengen Member States. Define rules of governance of the system, for example based on the cycle of European Presidencies. This solution should have the benefit to involve all Member States in the process, independent of their size or influence.

It is also crucial to propose a Certificate Policy specifically for the use of certificates to control access to fingerprint biometrics on Extended Access Control enabled passports and travel documents for the purposes of border control.

8.5 Conclusion

The identification of people and assets is a very broad topic that spans across many domains. We believe it is a topic of great interest for the ESRIF. The WG8 report has been designed in alignment with the ESRIF Report - Part 1. Our conclusions are aligned with the key messages of the ESRIF, particularly as regards the notion of security by design, interoperability and trust.

The key points we would like to reinforce are the following:

- Without any coordination at EU level, no effective implementation of EAC controls at the borders and controls within the Schengen Area can be attempted.
- We need to create a new scheme and approach for border controls that is integrated and interoperable and thus improves performance, accuracy, efficiency and convenience, by deploying automated systems and enhancing proactive work and mobility at all border crossing points.
- Trust is the key of the edifice; trust of citizen in deployed policies, trust in ID credential issued (notably for crisis management) and trust in biometric devices deployed.
- Speed and convenience for all ID checks and controls is an effective means to ensure that security investments are in line with business rules, because at the border, "time is money".
- Security investment is a means to protect more certainly and efficiently the ID credentials of citizens, so investments in security are at the same time investments in privacy protection.
- To promote appropriate design and discussion with stakeholders for new systems oriented to "person identification" in a broader sense and to promote efficiency with multimodal biometric techniques and appropriate user comfort and acceptance, in line with actual and expected future standards.
- In a globalised and insecure world, tracking goods and assets by technological means is necessary to efficiently prevent terrorist attacks and malicious organised fraudulent activities.
- We need to support and invest in research, evaluation, development and use of best of breed technology such as biometrics, SOA and related technologies.

9. Working Group: Innovation Issues

9.1 Introduction

ESRIF builds on two ambitious objectives, namely to make Europe a more secure place in which to live, enhancing the security of the citizen and making European society more resilient to cope with security related challenges, and to create the market conditions and related incentives, mechanisms and instruments for a competitive European industry.

The economic situation has dramatically changed since the inception of ESRIF. Europe is right now facing threats of economic uncertainty and social instability due to the current economic crisis. At the same time, it has become clear that security has become a relevant dimension **in almost all areas of daily life. Security is** not only about border security or critical infrastructure protection; it also affects civil society domains such as food, agriculture, health, diversity and the financial sector. For this reason, ESRIF suggests that the European Union takes up **security as a lead market**, stipulating innovative research and the creation of jobs and at the same time providing new business opportunities.

The European Union should **reach out for competitive leadership in selected elements of the security market by 2015**. These selected elements should reflect the operational needs and the specificities of European society, such as Europe's unique approach to data protection, diversity and the need for multi-cultural, multi-lingual solutions emphasising the need for integration.

This certainly requires a clear articulation of the demand and **joint commitment** of governments and end-users, including the sharing of benefits and risks with industry in order to exploit the results of research, moving research developments from their early stages to tested pre-commercial products ready for commercialisation. In addition hereto, a **culture of innovation is a key to success**. Given that the Lisbon Agenda considers European competitiveness in the global marketplace a top priority, European innovation[1] capabilities need to be enhanced. In line with the renewed European Commission action plan on the Lisbon Partnership for Growth and Jobs[2] an **integrated approach to research and innovation is seen as essential.** ESRIF strongly recommends to improve the conditions for commercialisation and exploitation of the research results, bearing in mind the huge potential of using public procurement to encourage innovation by providing a 'lead market' for new technologies.

With these objectives in mind, ESRIF WG 9 studied the criteria and conditions for the creation of an innovation-friendly security market and for the strengthening and dynamic integration of RTD resources and competences to make optimal use of Europe's knowledge base. It assessed and proposes the implementation of concepts and instruments such as a **European Security Label, pre-commercial procurement and innovation ecosystems.**

1 Innovation = capacity to valorise new R&D results into marketable products, processes and services.
2 COM (2006) 30 final, Communication from the Commission, The new partnership for growth and jobs, dated 25 January 2006

9.2 Challenges

Already in its intermediate report on mid term challenges and in line with the tasks given in the ESRIF Terms of Reference, ESRIF WG 9 identified a number of challenges to be further explored and analysed with representatives of all stakeholders during the course of its work.

9.2.1 Challenge to map competences

For the strengthening of its security structures and infrastructures, Europe can rely on strong in-house technological and industrial competences. In order to understand and value the European Security Technological and Industrial Base (STIB), it is an important first step to map these competences, covering all relevant technology, system and service areas, all types of technical and industrial players and all EU-27 Member States. Such a mapping will allow the identification of the strengths and weaknesses of the STIB and will support the policy makers in defining the research, technology and development priorities for the EU, strengthening its technological capacity, and developing new competences where deemed necessary for the security interests of the EU and the Member States.

In this context ESRIF WG 9 took into account the work done in the PASR-2006 supporting activity STACCATO, in particular on the Taxonomy and the Competence database and to use these inputs as a basis for further elaboration. As further activity, ESRIF WG 9 took up the task to consider, among others, the value of regional conferences for encouraging industries, SMEs, research institutes as well as academia to register and to define their competences in the competence database.

9.2.2 Challenge of networking

However, it is not sufficient to describe the competences of the STIB in isolation. A broader value lies in pooling and clustering these competences to maximize the synergy, complementarity and cross-fertilization between different technologies, players, stakeholders and services.

In this context, the ESRIF WG 9 considered it important to, among others, explore and assess the potential value of Centres of Excellence in the security domain.

9.2.3 Challenge of an appropriate legal context and framework

The security market is drawing on the requirements of the defence market and at the same time has to comply with regulations, processes and specifications of the civil market. In addition, it is strongly governed by national rules and regulations, which could require a European harmonisation.

It is important to understand the different rules, conditions and regulations that govern the security market. In order to achieve this, ESRIF WG 9 took up the task of analysing already existing rules, conditions and regulations and – in a second step – performing a gap-analysis to identify which new rules and regulations are required and which existing rules needed to be modified or abolished.

9.2.4 Challenge of standardization processes and standards to organize the market

The market for security solutions in Europe is highly fragmented and this fragmentation hinders the STIB in exploiting its overall potential and accessing market opportunities in a more effective way. There is a need to make a thorough analysis of the security market conditions, looking more closely to the demand side, and in particular to consider the role of standards and standardization as processes for organizing the market.

ESRIF WG 9 identified the importance to address these issues and in particular to explore the value of a European Security Label.

9.2.5 Challenge to reach out to end-users

The end-user community is much dispersed, fragmented and consists of a large variety of stakeholders, be it public institutions and agencies, ministries, policy makers or be it private users such as transportation companies, electricity distributors, critical infrastructures, etc. It is difficult to identify the end-users and even more a challenge to convince the end-users to support in general the work of ESRIF and more specifically concrete research projects.

ESRIF WG 9 set the objective to engage as many stakeholders as possible in the work of its activities and to interact with other ESRIF WGs to optimize stakeholder representativity.

9.2.6 Challenge for new business models

Security-related research activities are very valuable, but in order to ensure maximum take-up of the research effort, the research part should not be considered in isolation. It is important to tailor the technological solutions to the operational requirements and user needs in the field, as described above, and it is necessary to develop the required market mechanisms to ensure and enhance the development of security-related industrial products and services.

Since the security market differs significantly from the civil market, ESRIF WG 9 underlined the importance of analysing and defining the specificities of the security market and, with this objective in mind, of looking at, among others, relevant examples such as the EDA common reference for procurement.

9.2.7 Challenge to identify model cases to describe the concept

There is a large amount of relevant study material to analyse and assess in all aspects of the work of ESRIF WG 9. Many theoretical concepts have been developed in innovation policy, in legal frameworks, in market analysis, etc. ESRIF WG 9 adopted the methodology to take, in a first step, stock of the effort made so far in the EU, in individual MS and also beyond the EU in the US, Japan and others. In a second step, based on this assessment, ESRIF WG 9 planned to make suggestions on which existing tools/ methodologies / practices are useful for an EU approach and on how to move forward.

In addition to this theoretical and methodological work, ESRIF WG 9 believed it important to undertake a number of concrete activities. In particular, ESRIF WG 9 emphasised the necessity to launch a number of implementation cases, so-called "model cases", to describe and demonstrate the value of the theoretical and methodological choices made. These model cases can be related to one or more of the key issues. E.g. to illustrate the processes for networking, a concrete networking activity could be launched, such as the creation of a network of trusted airports.

9.3 Needs

The challenges identified in the intermediate report provided good guidance for the work of ESRIF WG 9, but the detailed analysis of the many issues at stake identified a much wider range of needs to be addressed. ESRIF WG 9 did not do this detailed work in isolation. Valuable input came from dedicated workshops with specialists and experts on innovation policy, education and training, legal frameworks, insurance companies, etc. In addition, ESRIF WG 9 verified its findings against key reports such as those by the Aho Group.

9.3.1 An innovation-friendly security market

In order to create an innovation-friendly security market, Europe would need:

- Investment planning and setting of targets and objectives based on a demand driven and harmonised approach
- Good governance through EU wide harmonised regulation
- Ambitious use of standards
- Structuring the market through harmonised public procurement
- Fostering a culture which celebrates innovation

9.3.1.1 Investment planning, setting of targets and objectives

The creation of a harmonious European security market and the engagement of the supply side to invest in research, new technologies, new innovative products and services, require clear commitments from the end-user community, the buyers, the policy makers and the regulators.

Articulation of the demand

Security research and innovation aims at being user-oriented and driven by given threats and requirements. The end-user community must be able to articulate its needs for operations in the field and their envisaged investment planning. Understanding user needs and developing mechanisms for translating these needs into technical requirements and service

specifications are crucial in this process. Adequate interfaces need to be set up; exchange mechanisms between the end-user community and the research and industrial community are to be developed. Human Factors tools geared towards analyses of systems and operations are required. This certainly asks for a permanent interaction between end-users and providers to define, redirect, adapt, tailor, and optimize operational use of the technologies, and to take account of the changing threats and related security challenges.

Prioritisation of Expenditure

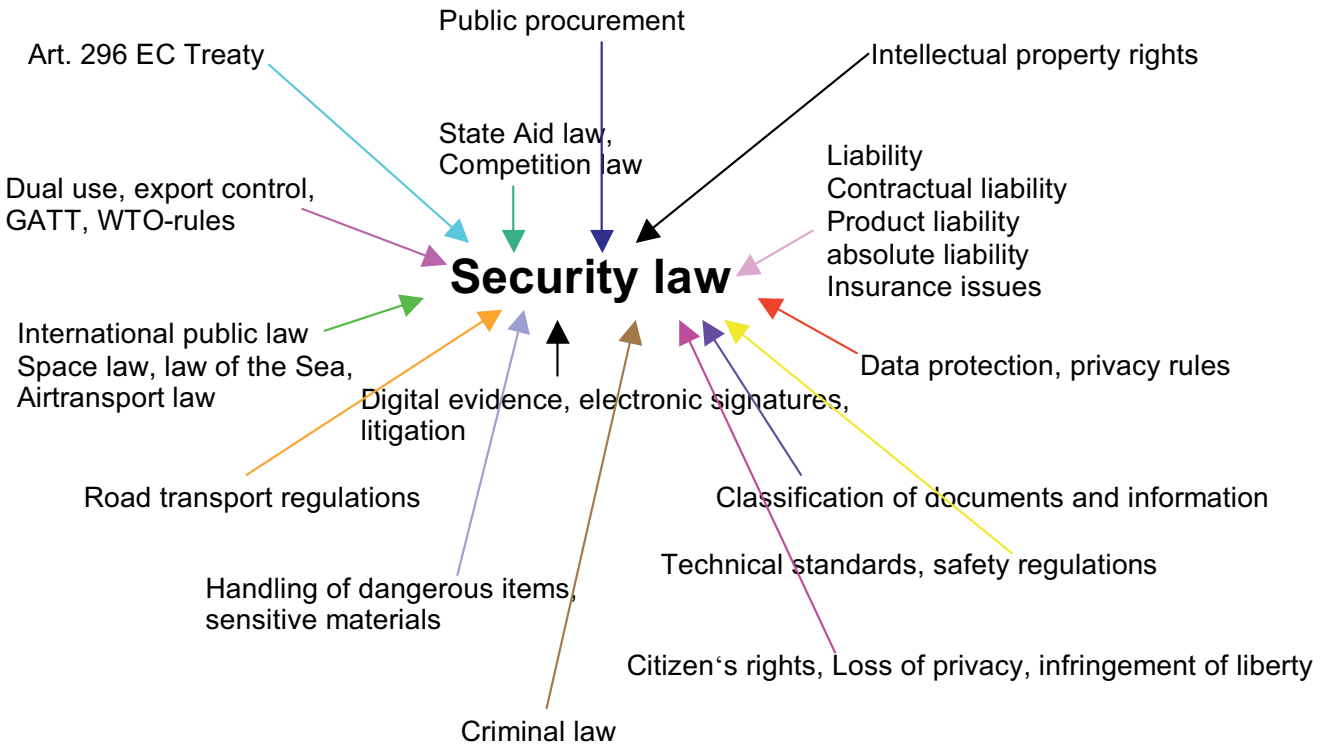
While articulation of the demand is essential to address core issues of concern to the end-users, there is a further need to adopt a risk based approach to prioritise investments. For instance, in order to increase resilience in the case of a man-made or a natural crisis there should be a process to identify and prioritise risks, understand the threat, the vulnerability and the potential impact so as to invest resources in an appropriate and cost-effective manner.

Europe should use risk modelling methodologies derived e.g. from the insurance sector to draw up (insofar as possible) a complete set of incident scenarios and prioritise its security research and innovation expenditure to improve resilience and to inform the allocation of crisis management resources.

9.3.1.2 Harmonised regulation and legal framework for security

The creation of a harmonious European security market and the engagement from the supply side required a related stable legal context as reference, both at national and European level. Such legal framework will contribute to an improved understanding of the principles governing the security market. Since this market still is highly diverse, dispersed and fragmented, a common regulatory framework for security technologies and security research in Europe will allow industry to better focus its new industrial developments in view of the user needs and market requirements.

The legal framework for security is a complex interaction of rules, conditions and regulations not only related to security, but, as summarised in the diagram below, also coming from other policy requirements such as transport, energy, privacy, etc.



Not only this interaction between different policy domains is characterizing the legal frame for security. Also the large variety of national practices and the diversity across the EU Member States in translating and implementing EU rules, conditions and regulations into national law contribute significantly to the complexity. Moreover, there may exist national, European and International legislation, legal frameworks and treaties that would not allow for any exchanges of information or expertise, as for instance in the case of CBRNE matters.

In order to improve the understanding of the state of play for all stakeholders in specific security-related situations, it is important to have an overview of all these elements and their interaction. A database with legislation in force in the EU might contribute significantly to this understanding and would facilitate the process of identifying potential gaps, conflicts, averse effects, of the rules, conditions and regulations in use.

ESRIF WG 9 held hearings with experts, e. g. the European Representative for Data Protection. It became evident that any new solution must take into consideration aspects of privacy and civil liberty rights from the beginning of the design of new security measures. This concept of privacy by design or data protection by design is a core characteristic of Europe's unique approach to privacy and data protection. The balancing between increasing security and enhancing security measures on the one hand and preserving the fundamental rights of citizens for privacy, justice and freedom on the other should be the driving force for any investment in security. As such, the concept of privacy by design or data protection by design should be an inseparable part of the wider concept of security by design, described in the key messages of ESRIF.

ESRIF WG 9 also noted that other countries introduced new legal measures for providers of security solutions, e. g. in the aspect of liability (the US Safety Act). It is suggested to assess both the need and the value of establishing an EU equivalent in order to enhance the competitiveness of EU industry.

9.3.1.3 Ambitious use of standards

The market for security solutions in Europe is highly fragmented thereby preventing EU industry from exploiting its overall potential and accessing market opportunities in a more effective way. There is a need to make a thorough analysis of the security market conditions, looking more closely at the demand side, and in particular considering the role of standards and standardization as processes for organizing the market.

Dynamic standardisation

The European Commission[3] identifies dynamic standardisation as an important enabler of innovation, contributing to the development of sustainable industrial policy, unlocking the potential of innovative markets and strengthening the position of the European economy through more efficient capitalising of its knowledge base.

State-of-the-art standards provide a level playing field, which facilitates interoperability and enhances competition between new and already existing technologies, products, services and processes. They generate trust in the performance of these new technologies, products, services and processes and allow their benchmarking through reference and validation according to standardised methods.

In this understanding, new standardization concepts must be developed which are capability driven, focusing on the level of performance of security related solutions rather than on the level of technical equipment specifications. This is important to enrich the market and to allow a broad range of industries to come up with solutions that are compatible and interoperable, and at the same time allowing flexibility to adapt to individual customer needs.

If specific areas are identified where new standards or standard-like initiatives are required, they should be approached with an innovative mindset, as described also in the Aho Report.

"Specification of functional performance or standards, which allows suppliers to produce any configuration of technology they feel can meet the need."

3 COM (2008) 133 Final, Communication from the Commission, Towards an increased contribution from standardisation to innovation in Europe, dated 11 March 2008.

"This will require technical and competitive dialogues between purchaser and supplier", as well as a set of guidelines and workshops for new public procurement approach and evaluation.

The Aho Report wording is important as it opens up the solution options and the opportunities for alternative innovative solutions which do not exist today, such as process driving innovation and new thinking.

European security label

The European market needs basic criteria upon which to base decision making, regarding the acquisition and implementation of security products, services and their integration. Citizens need to be informed and reassured that the security measures, provided by public and private organisations, are compliant with and use (exclusively) products and services that respect European specified criteria. They must be assured that an adequate and recognised level of security has been established for their protection and well-being.

The present market for security is particularly fragmented in Europe. Stakeholders and investors lack confidence. A structured security market, enabled by the introduction of a European Security Label, will increase confidence and trust through a transparent, auditable and sustainable approach to addressing security. This will be a catalyst for investment by the European security industry and attract new investors to the security sector, introducing a new business model supported by Public-Private Partnership. This is closely linked with the importance of a strong European competence in the field of standardisation and certification.

The introduction of a European Security Label would constitute a common reference point for suppliers, end users, customers and society in general. Customers, end users and suppliers alike would experience a heightened perception of security, with all related benefits, from the knowledge that products and services have gone through the process of being evaluated and achieving the European Security Label.

A European Security Label would provide the frame for a dynamic standardisation process, defining the what, when and why of a security process without defining how it is to be achieved and setting out measurement criteria around the performance levels of different applications. As such, it will also drive innovation, in particular because the best solution must include, among others, human factors and operator/end-user issues and the incorporation of citizens rights, including privacy by design.

9.3.1.4 Structuring the market through harmonised public procurement

In order to ensure maximum take-up of research effort, it is important to consider research activities and their related technological solutions in a system of operational requirements and user needs. In this way, security-related research will be an important enabler towards more efficient and effective operational capabilities in security-related tasks and missions, and it will enhance the competitiveness of the European security-related industry.

There is a need to consider the entire innovation chain, including the involvement of public and private end-users, competence mapping and networking, interaction and integration of supply and demand and of education and training.

Innovative Public Private Partnerships

By promoting the connection between security research and security policy making, research and public-private partnerships have a key role to play in protecting society.

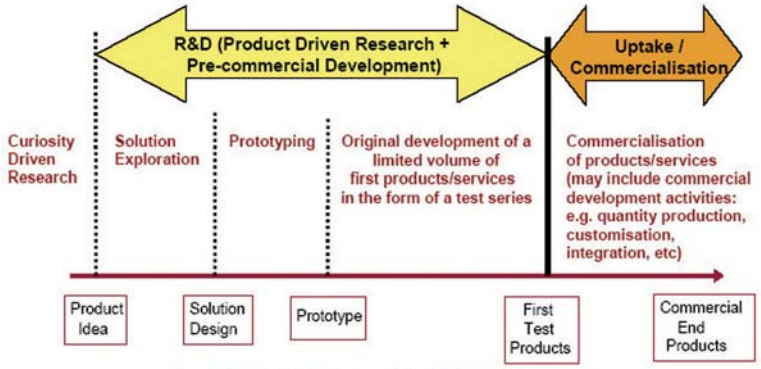
Public-private dialogue is crucial in increasing the security of infrastructure and utilities, fighting organised crime and terrorism, by preparing for, preventing, managing and helping restore security in a crisis, plus analysing related political, social and human issues.

There is thus a need for a harmonised European approach to address these matters, providing a means for the market to recognise and implement effective and efficient security solutions.

Role of Public Procurement

The European Commission[4] already emphasised the importance of public procurement in reinforcing the innovation capabilities of the EU whilst improving the quality and efficiency of public services. It also underlined the insufficiently exploited opportunities in Europe of pre-commercial procurement. The Aho report also underlined the urgency to develop an explicit strategy at European level to use public procurement to drive demand for innovative goods and services.

The European Commission[5] further developed this concept and defines pre-commercial procurement to be the Research and Development (R&D) phase before commercialization, as in the table below.



Typical Product Innovation Life Cycle

The Communication in particular sees value in exploiting the potential of pre-commercial procurement in addressing important societal challenges, such as affordable health care, climate change, energy efficiency and security of energy supply, food security, security of supply with fresh water, impact of natural disasters to critical infrastructure, etc.

In these areas, pre-commercial procurement provides excellent opportunities to ensure that capacity to deal with the societal challenges is enhanced whilst supporting investment in development of research results into prototyped solutions. As such, this role of the EU or national governments as procurers of R & D or "first buyer" of innovative demonstrators can be a catalyst for innovation and a major driver to reinforce the competitiveness of European industry in the markets concerned.

Following the European Commission's recommendations, ESRIF WG 9 emphasises that pre-commercial procurement of innovative security solutions should be promoted and the potential role of the EU as a "first buyer" explored.

It is furthermore recommended to undertake a number of initiatives, such as the revision of public procurement rules and procedures to stimulate the market and pre-commercial procurement of innovation. For this reason, ESRIF WG 9 suggests considering the creation of an EU wide harmonised public procurement scheme. As one example, the standard handbook for defence procurement, established within CEN, could be taken as a reference.

9.3.1.5 Promoting competitiveness and European excellence

The security market is an emerging on, but is nevertheless highly innovative, with a large, growing potential when adequately responding to customer needs. At the same time, Europe can rely on a strong scientific, technological and industrial base and the security market depends more than other markets on the creation of favourable framework conditions through public policy measures. Given these characteristics, the security market provides promising opportunities for a European lead market initiative and ESRIF WG 9 suggests that the EU reaches out for competitive leadership in selected elements of this market by 2015.

---

4 COM (2006) 502 Final, Communication from the Commission, Putting knowledge into practice: A broad-based innovation strategy for the EU, dated 13 September 2006

5 COM (2007) 799 Final, Communication from the Commission, Pre-commercial Procurement: Driving Innovation to ensure sustainable high quality public services in Europe, dated 14 December 2007

9.3.1.6 Fostering a culture which celebrates innovation

Partnerships between research, industry and end-users are seen as an important enabler to stimulate innovation in the security domain. For such partnerships to work efficiently, it is important to build on a well-organised knowledge base and to establish market conditions, mechanisms and incentives that foster innovation. One example in this context could be field laboratories.

Independent testing for technology validation

Technological developments are moving fast and the security relevant product portfolio is very wide. In this labyrinth of technologies, first responders, fire brigades, customs officers and other operators in the field are not always sufficiently aware of the technology potential and technology readiness to support their operations and can therefore not access those potential products and services. Therefore, there is a need for independent validation of technologies. The result must influence the R&D prioritisation in order to enhance the fast implementation of innovative solutions.

Field labs for validation

The result of the complete innovation chain, starting from R&D will be systems and solutions which should enhance safety and security, e. g. first responders. However, before implanting such new solutions, Field labs are needed for the validation (verifying whether it is fit for purpose), i.e. realistic environments for the demonstration, validation and optimisation of innovative systems for security tasks or meeting points where end-users, security authorities, industry and the research community can have access to the technological solutions relevant for their daily work.

Encourage SMEs

SMEs account for 67% of Europe's private sector employment and represent 99.8% of all European enterprises[6]. They suffer more than large companies from administrative and regulatory burden, lack of access to finance, taxation, insufficient access to public procurements and research funding, unfair or too strong competition, etc. This is not specific for the security domain, but ESRIF WG 9 does believe that future EU research and innovation initiatives should be designed so as to alleviate SME problems and to grow SME participation in EU RTD. Specifically for security research how to stimulate and optimise SME involvement in projects, targeting 25% by 2011, could be explored.

In addition, security is an extremely broad domain requiring input from most industrial sectors and expert disciplines. Many SMEs that would normally not operate in the security arena have relevant skills for security applications. This is an 'untapped potential'. Dedicated initiatives should be undertaken that would encourage more SMEs to enter exploitable high-tech niche security markets. As such, Europe will drive investment in knowledge and innovation and thereby enhance its competitiveness. A further benefit is that this action will improve the competitiveness of large European enterprises by broadening and deepening the pool of potential partner SMEs. ESRIF recommends to launch a structured initiative to identify exploitable demand by public and private security end-users and to entice non-security SMEs into these niche markets and, to a lesser degree, to encourage existing security SMEs to diversify. It is noted that for SMEs the large enterprises are legitimate end-users.

9.3.2 Capitalisation of Europe's knowledge base

In order to strengthen and dynamically integrate R&D resources and competences to make optimal use of its knowledge base, Europe would need:

- Mapping of technological and industrial competences,
- Innovation ecosystem,
- Exploiting the value of instruments such as technology platforms or joint initiatives for security,
- Education and scenario-based training.

6 http://ec.europa.eu/enterprise/entrepreneurship/docs/sme_pack_en_2008_full.pdf

9.3.2.1 European Security Technological and Industrial Base (STIB)

For the strengthening of its security structures and infrastructures, Europe can rely on strong in-house technological and industrial competences. These competences cover a very wide range of research, technology, development, manufacturing and service expertise, including very specific detailed areas, such as biotechnology and biosensors as well as very generic domains, such as technology and systems integration, interoperable communications, C4ISR, etc. Also the technological and industrial landscape displays a large variety and geometry, covering SMEs as well as large multi-nationals, basic research in technical universities as well as in service support companies, regional/national expertise and more established, integrated European networks of excellence, etc.

In order to understand and value the European Security Technological and Industrial Base (STIB) and to take targeted action to reinforce and strengthen its potential, it is an important first step to map these competences, covering all relevant technology, system and service areas, all types of technical and industrial players and all EU-27 Member States. Such a mapping will allow the identification of the strengths and weaknesses of the STIB and will support the policy makers in defining the research, technology and development priorities of the EU, strengthening its technological capacity, and developing new competences where deemed necessary for the security interests of the EU and the Member States.

9.3.2.2 Innovation ecosystems

The competences of the STIB should not be considered in isolation. A broader value lies in pooling and clustering these competences to maximize the synergy, complementarity and cross-fertilization between different technologies, stakeholders and services.

Networking brings important competitive strengths for business. It helps to close the gap between business, research and resources and as such brings knowledge faster to the market. Successful networks, such as ENFISI (European Network of Forensic Science Institutes), EURAMET (European Regional Metrology Organization) and GMOSS (Global Monitoring for Security and Stability) enhance productivity, attract investment, promote research, strengthen the industrial base, and develop specific products or services and become a focus for developing skills.

But for highly demand-driven sectors as security, it is not sufficient to just bring the knowledge community together. The knowledge triangle must be structured around a strong interaction between supply and demand. The end-users of the security solutions in the field must be engaged in the innovation process; they must steer and drive it, to ensure that the security solutions are adequately tailored to their specific needs.

Innovation ecosystems encompass more than knowledge inputs. They incorporate all relevant factors and stakeholders that generate value to customers. They enable participants to work across enterprise boundaries, focus on customer value creation, respond quickly to shifts in market demand, accelerate the transition from research to production and be more adaptive to change.

Important in this context is the recent inauguration of the European Institute of Technology and Innovation (EIT). EIT is an integrated partnership of science, business and education, embodying excellence in all of its initiatives. It is intended to be a key driver and a new model for innovation in strategic interdisciplinary areas, where there is the potential to generate innovative solutions and commercial advantages with a major impact on Europe's competitiveness. Its mission is to grow and capitalise on the innovation capacity and capability of actors from higher education, research, business and entrepreneurship from the EU and beyond through the creation of highly integrated Knowledge and Innovation Communities (KICs). The development of specific KICs for dedicated security-related domains may be a stimulus for innovation in the emerging security market.

9.3.2.3 Technology Platform / Joint Technology Initiative "security"

In order to ensure a systematic and consistent approach to security research and innovation fully serving the ESRIF objectives, ESRIF WG 9 believes that there is a need for a transparent mechanism dedicated to the ESRIA and at the level of the implementation of the ESRIA, as well as for the monitoring and updating of the ESRIA taking into account the progress and changing priorities. ESRIF WG 9 is convinced that the concept of the European technology platforms and the Joint Technology Initiatives are useful instruments to serve this purpose.

The **European technology platforms** aim at providing a framework for stakeholders, led by industry, to define research and development priorities, timeframes and action plans on a number of strategically important issues where achieving Europe's future growth, competitiveness and sustainability objectives is dependent upon major research and technological advances in the medium to long term. They play a key role in ensuring an adequate focus of research funding on areas with a high degree of industrial relevance, by covering the whole economic value chain and by mobilising public authorities at national and regional levels.

Joint Technology Initiatives are going further than European Technology Platforms by offering a framework for realising particularly ambitious research and technology agendas. They are of such a dimension and scale that existing funding schemes are not adequate to achieve the desired objectives. They require high public and private investment at European level. For that purpose, they bring together all stakeholders (not only EU but also national) around commonly agreed agendas. Such an integrated approach promotes the generation of new knowledge, enhances the uptake of the results of research into strategic technologies and fosters the necessary specialisation in high technology sectors which determine the EU's future industrial competitiveness.

Both instruments are very valuable in the context of security. Europe should consider launching initiatives of European technology platforms and Joint Technology Initiatives in dedicated security-related domains.

9.3.2.4 Education and scenario-based training

As emphasized in the key messages of ESRIF, education and training can contribute significantly to the overall acknowledgement and recognition that security is a common responsibility of all stakeholders, i.e. security officers, policy makers, regulators, law enforcement, emergency services, civic society, industry, RTOs, academia, media, and the citizen. Therefore, education and training need to be oriented and specifically tailored towards all of these players.

Education and training programmes

Specific programmes should reach out to a wider public, to raise awareness of threats, risks and vulnerabilities, to improve the understanding of the processes and procedures put in place to tackle the challenges that these threats, risks and vulnerabilities bring, to debate the acceptability of technological solutions, etc.

Policy and decision makers must be addressed, to emphasise the complexity of security related tasks, measures, processes, to support decision making, etc.

There is a need to support the regulators, to enhance the understanding of the impact of regulations, to avoid conflict and promote harmonisation of regulations and their implementation, to support interoperability, etc.

And there is also the need to involve the media in the security process, to underline the important and responsible role of media in communicating disasters and crises, to develop a specific Public Private Partnership with the media for this purpose, etc.

Curricula for security

ESRIF promotes the concept of security by design: Security must be embedded in the technology and system development from the early stages of conceptualisation and design. For the topic of education this means that the education of researchers and designers in future should reflect these needs, including the promotion of multi-disciplinarity, through specialised curricula for security.

Joint training centres

Training for security functions and tasks is much diversified, with a large number of small public and private operational training centres (often) under direct control of local authorities or a specific public service and a poor exchange of expertise between local training centres, training centres from different services and across nations. It is believed that individual training centres could benefit significantly from having access to experiences, lessons learnt and best practices of colleagues in other regions or nations or even other disciplinary domains. Therefore, it is suggested to create a multi-layer, border crossing infrastructure

for training and education for security functions and tasks. Such infrastructures would provide a platform for and facilitate inter-service and cross-border training. ESRIF WG 9 recommends to build on existing experience and to establish links with existing networks for professional training like CEPOL on police training and education.

Advanced training concepts and scenario based training

Most training is still focused on formal training environments. Given the complexity of many security related tasks, training could significantly benefit from virtual realities and gaming environments. New training methods should be explored, for instance use web technologies to increase informal learning, improve communities of practice, extend existing virtual reality and gaming environments with strong didactics, train instructors/ trainers/ developers/designers to use other learning environments/tools, better include operational lessons learnt into learning environments (and vice versa).

In addition, training based on scenarios hardly exists in the civil domain. Scenarios would provide realistic contexts and environments for example complex crisis management operations, such as CB incidents in a metro station, or incidents with explosives, etc.

9.4 Priorities

ESRIF WG 9 has taken a holistic approach to broad-based innovation, i.e. engaging all stakeholders. It is important to tailor the technological solutions to the operational requirements and user needs in the field and it is necessary to develop the required market mechanisms to ensure and enhance the development of security-related industrial products and services. Only then, security-related research will be an important enabler towards more efficient and effective operational capabilities in security-related tasks and missions, and it will enhance the competitiveness of the European security-related industry.

It is very difficult to prioritize actions in such a holistic concept, since initiatives need to be taken at all levels to really move forward. It is important to consider the entire innovation chain, including the involvement of public and private end-users, competence mapping and networking, interaction and integration of supply and demand, education and training, etc.

This was well supported by the ESRIF community. Most of the issues raised by ESRIF WG 9 have been incorporated into Part I of the ESRIF report: chapter 2 has dedicated key messages on innovation, industrial policy, education and training, chapter 3 identifies in the ESRIA a number of concrete standardization needs and training requirements, chapter 4 emphasizes the importance of standards, validation, certification, market incentives and legal frame and chapter 5 supports in its recommendations the ESRIF WG 9 suggestions for a European security label, pre-commercial procurement, lead market initiatives in security, the creation of knowledge centres, etc.

9.5 Conclusions

In summary, ESRIF WG 9 proposes to:

- Reach out for competitive leadership in selected elements of the security market by 2015
- Establish a rolling process aiming to co-ordinate and harmonise end-user needs and requirements
- Use risk modelling methodologies derived from the insurance sector and elsewhere to prioritise investment
- Develop a stable legal context as a reference
- Improve the understanding of the complex interaction of different rules, conditions and regulations
- Promote the concept of Privacy-by-Design / Protection-by-Design as strongly intertwined with the concept of security by design
- Explore the value of a European legal framework that would take proper account of liability
- Develop a dynamic standardisation policy
- Launch a European Security Label
- Enhance public private dialogue and innovative PPP to jointly address security challenges and to enhance security
- Promote pre-commercial procurement of innovative security solutions

- Explore the potential role of the public dimension of the EU as a "first buyer"
- Share the benefits and risks of translating research into marketable solutions
- Create field labs for validation
- Set ambitious targets for SME involvement/participation in RTD projects
- Map the capabilities of the European knowledge base
- oster the networking and clustering of the knowledge base and the creation of innovation eco-systems providing a platform for systematic interaction between supply and demand
- Explore the value of launching Knowledge and Innovation Communities (KICs) in dedicated security domains
- Develop a transparent mechanism for the implementation and updating of the ESRIA
- Launch education programmes for policy makers, the citizen, media and others
- Create curricula for security
- Promote scenario-based training
- Enhance the establishment of joint training centres

10. Working Group: Governance and Coordination

10.1 Introduction

This introduction describes the organisation of WG 10 and its work programme and packages.

The ESRIF Terms of Reference requires ESRIF to undertake **"continuous analysis of the future capability needs of the security demand side".**

Further "ESRIF should contribute to increased transparency and **joint planning of Security Research and Innovation programmes / activities in Europe,** with a view to enhanced co-operation."

The WG10 Terms of Reference requires the group to examine:
"the co ordination of security research strategy and implementation between the European Union and Member States and relevant institutions or organisations, such as: ESA, EDA, NATO."

WG10 adopted a four-phase programme of work, following a set of five clear principles, and conducted a thorough analysis. The summary of the programme and the results of the analysis are presented in the WG10 report.

WG10 has implemented its terms of reference to undertake its data collection, analysis and assessment, and to reach its conclusions and recommendations. WG10 performed its activities according to the following programme:

- Assessment and mapping of current policy and practice regarding research, including coordinated activities, for the four vertical mission areas (February 2008-April 2008)
- Test current governance and co ordination systems for fitness for purpose against long term scenarios (May 2008-August 2008)
- Identify policy/structural/cultural issues surrounding the gaps identified (September 2008-December 2008)
- Research co ordination recommendations as a function of 4 mission areas at both EU and national levels (January 2009-April 2009)

In conducting its work, WG10 observed the following Principles:

- The Governance system must add value above and beyond what Member States can deliver on their own
- The Governance system will be responsible for overseeing the ESRIA, its implementation, and what happens to it
- Governance system will have to monitor the ESRIA, in line with the preservation of the ESRIF vision
- The Governance system will need to ensure that Member States agree with and support the aims and objectives of the ESRIA as we move forward
- The Governance system will need to secure the agreement, sponsorship and funding of the EU

10.2 Analysis of the Situation

Many Member States have created dedicated Security Research Plans. The large majority of these plans contained requirements in one or more of the four vertical areas indicated by ESRIF:

- Security of the citizen
- Security of critical infrastructure
- Border security
- Crisis management

This confirms a common perception of the issues of our society. Moreover, almost all the Member States have put in place a specific national Governance structure for the definition of the objectives of the research plan. This confirms European agreement for the need to maintain co-ordination of security research plans.

Members States employ different approaches for the management of the Security Research Plans ranging from the establishment of dedicated National Authorities to the extension of the role of existing structures. The variety of implementation approaches represents an issue for ESRIF, which can be overcome by stimulating partnerships among Member States and creating a European network of actors capable of successfully executing projects in a coherent frame. Critical to this is the identification of the correct level of intersection between EU/Member State initiatives.

10.2.1 Mapping and Assessment of current policy and practice regarding research

10.2.1.1 Explanation of methodology

The findings were gained through a structural qualitative comparison of the eight available national research programme documents from EU Member States (Austria, France, Germany, Netherlands, Norway, Spain, Sweden, UK; documents are specified in the 4th ESRIF plenary report PowerPoint presentation of WG 10) and security research relevant work programmes of supra-national organizations/agencies (European Commission/FP7 Security Research; European Commission/other FP7 themes and other programmes; European Community agencies such as FRONTEX, EMSA or ENISA; other agencies and international organisations such as EDA/OCCAR, ESA, Eurocontrol, NATO). Relevant research programme documents were partly analysed in full text, partly in the form of selected excerpts thereof provided by the Sherpa, and partly in the form of own translations (were no English programme document was available).

A comparative matrix was then designed for the Member States and also for the supra-national organizations'/agencies' security research programmes (see annex IV - WG 10: National Matrix (annex 3) and European Matrix(annex 4)). For each member state or supra-national body, it was marked on that matrix if and how the four EU FP7 vertical mission areas for Security Research (security of citizens, security of critical infrastructure, border security and crisis management) are reflected in its own security research programme. Transversal security research activities, cutting across two or more of these mission areas, were identified and noted in the matrix together with examples.

10.2.1.2 Cross-national Comparison of Security Research Themes according to the FP7 Vertical Mission Areas

The National Matrix reveals differences within Member States, mainly in the sense that Member States tend to set clear priorities within the four mission areas, mostly with cross-cutting themes that combine FP7 mission areas 1 (security of citizen) and 2 (security of critical infrastructure): In the case of Austria, it is the theme of public authority measures (especially communication) that links the mission areas "security of the citizen" and "security of critical infrastructure"; in Germany it is transport; in the Netherlands it is the energy supply chain, as it is in Spain, together with biotechnology. Biotechnology is also the theme that overarches FP7 mission area 1 and 2 themes in the Swedish security research programme, along with CBRN (Chemical, Biological, Radiological, Nuclear) detection and critical ICT (Information and Communication Technology), based on network solutions. In Norway it is information security, especially in terms of secure access to information and secured accessibility of information. Only France and the UK were found to keep FP7 mission area 1 and 2 topics relatively separate in their security research (funding) policy.

10.2.1.3 Security Research Themes in Programmes of International Organisations/Agencies

International (European) organisations and agencies (see annexed European Matrix) seem to be split on research topics in mission area 1 (security of the citizens), 2 (security of critical infrastructure) and 4 (crisis management) topics, whereas they converge in mission area 3 (border security) topics, especially maritime surveillance and UAVs. Development of and orientation on common (international) standards is an area of convergence in the field of transversal issues. Potential synergies for joint programmes and budgets should consequently be explored in these areas.

10.2.1.4 Research Governance and Management of Transverse Issues

As a fifth row in the National Matrix, a comparative assessment of national provisions for security research into transversal issues, for standardisation and (international) interoperability in security research or use of research results was added.

In Austria, transversality is confined to the national dimension and governed by the compulsory inclusion of humanities and social science aspects in all funding proposals handed in under any programme line of the national security research programme. Management of transversal issues happens on a regular basis in the framework of a steering committee with representatives from all relevant ministries that is regularly convened by the Ministry of Transport, Innovation and Technology as owner of the national security research programme. In France, transversality is also confined to the national dimension and governed by the joint issuing of the current edition of the national security research programme by the National Research Agency, the General Delegation for Armament and General Direction of the National Police. In Germany, the objectives and contents of the security research programme were defined jointly, involving the ministries of research, science and business.

The National Security Strategy and Work programme of the Netherlands contains among its objectives the establishment of international security networks and deems the national approach to be aligned of that of other nations and organizations. At the national level, the programme seeks to grasp contributions from the national government, local governments, the business community, social organisations and citizens. The national security programme is explicitly seen as an interdepartmental responsibility, however with overall coordination in one ministry (Interior and Kingdom Relations). Norway, concentrating on information security, seeks to contribute to international development of standards with its security research activities, which are governed by the Information Security Coordination Council. In Spain, the focus is on national innovation by dedicating research to cross-cutting themes, mainly in the field of critical information and communication infrastructure. Programme governance rests with the Inter-Ministerial Commission for Science and Technology. In Sweden, the Emergency Management Agency governs security research and seeks international linkages in order to support industry participation in foreign (mainly U.S.) security research programmes. The UK seeks to explore transversality in order to strengthen bonds with U.S. government authorities, especially in terms of science and technology cooperation for critical infrastructure protection and homeland security as well as cooperation on combating terrorism that also shall include academia.

As for governance in the sense of operative research programme management, the analytical picture is patchy: In half of the countries analysed (Austria, Germany, Netherlands, UK), the lead in security research (programme) management rests with a certain ministry (in two cases Interior/Home, in one case Science and in one Transport, Innovation and Technology), in some it rests with an inter-ministerial commission (Spain) or with different agencies and authorities from the security sector (France). In other countries, the lead is assigned a national emergency management agency (Sweden) or a coordination council consisting of members from ministries, directorates and government agencies (Norway).

10.2.1.5 International Instances of Coordination

International instances of coordination, as already mentioned, are not reflected in all Member States' security research programmes. Austria and France concentrate on domestic coordination and innovation. In a similar vein, Germany stresses that the European programme is not a substitute for Member States' national programmes with their own focus and concentration on specific security requirements. In the Netherlands, in contrast, the need to line up with security research programmes and practice of other states and organizations figures prominently. Norway underscores that standards for information security, the thematic focus of its security research programme, will be set by international standardisation organizations, and Norway should actively participate in this work in order to affect the development of these international standards that will (have to) be nationally applied. Spain seeks to foster national innovation in security research also by improving the coordination of participation in international projects and facilitating national experts' access to international projects. Sweden explicitly aims to facilitate participation in US security research programmes, along with improving conditions for participating in the EU's security research programme. The UK stresses the sharing of experience and solutions with international partners, again the US in the first place, as an important approach to strengthen national security in terms of combating terrorism.

10.2.1.6 Mapping the European Security Research Landscape

Inferential reasoning on the basis of this precedent analysis revealed three common dimensions (factors) along which the eight analysed Member States' security research programmes can be adequately compared and differences as well as "distances" between Member States marked. These three dimensions (factors) are:

1) Thematic thrust (main subject area/s for security research).
2) Leading concept of crisis management (prevention/preparedness vs. reaction/response).
3) Transversal mode: Management of cross-cutting issues and interoperability by standardisation (orientation on same external norms and practices, e.g. from FP7) vs. coordination (common/shared internal norm-setting and focus on efficient domestic alignment of relevant actors).

10.2.1.6.1 Thematic Thrust

The majority of Member States' security research programmes focus on one leading theme that typically comes from an analysis of specific national requirements or shortcomings.

In the case of Austria, this is critical infrastructure protection (with the inclusion of social and cultural aspects). In the Netherlands it is climate change, as well as in Spain, together with nanoscience. In Norway it is the role of private entities in critical (mainly information) infrastructure protection, including critical ICT social infrastructure. Network-based solutions in security affairs (with respect for ethics, integrity and human rights) are the main theme in Sweden, and the UK focuses on permanent cooperation with (also non-EU) partners in the fields of conventional crime/violence prevention and protection against terrorist attacks. What makes the French security research programme stand out in its thematic thrust is – in addition to critical infrastructure protection – again an emphasis on conventional crime and violence as well as on crisis management in a broad sense, independent from the source of origin (such as natural, manmade and others). In Germany's programme, civil security research, or research on civil protection, is the leading theme.

10.2.1.6.2 Leading Concept of Crisis Management

While a clear concept of crisis management is not apparent in all national programmes, it is evident that tangible results for practical crisis management are a cornerstone of the European security research panorama. In the Austrian programme, the focus is on governance of capability building for crisis prevention rather than on operative crisis management: Generation of knowledge and technologies which are necessary to attain the goals of Austrian Security Policy (comprehensive approach) and contributing to increasing security and people's situation awareness. In France, crisis management in terms of incident response is emphasized, but the additional focus on conventional crime/violence as well as on protection of vital infrastructures and networks gives the programme also a preventive dimension. In Germany, with its security research programme following a generic civil protection approach, capability building for prevention and capability building for response are equally emphasized. The Netherlands focus on prevention in the sense of mitigation, or specifically, comprehensive vulnerability reduction (including the reduction of climate change triggered crises, of potential for interethnic confrontation and the assurance of electricity supply). Norway focuses on cultivating a culture of security in the sector of critical information and communication technology, thus also prevention is at stake. Security research in Spain centres on (mainly technological) innovation for resilience and response purposes, whereas crisis management as a term does not figure as a topic or strategic activity. From the Swedish point of view, security research should contribute to crisis management in the sense of civil protection and emergency management, which tends to make in response-focused. In the UK, security research contributions to crisis management focus on preparedness and prevention, primarily in the face of terrorist threat.

10.2.1.6.3 Transversal Mode

Management of cross-cutting issues and interdependency in security research happens at the level of a designated ministry in half of the examined Member States (Austria, Germany, Netherlands and UK). This group of countries is however split in itself: Whereas Austria and Germany follow a coordination approach and have a national focus (pluralistic approach, inter-agency networking), the Netherlands and the UK practice standardisation. That is, they are lining up their programme and research governance with international (Netherlands) or foreign (primarily U.S.) standards (UK). Two countries (Norway and Spain) practise an inter-ministerial level of security research governance, represented by an inter-agency commission. However, whereas Norway follows a transnational standardisation approach, Spain relies on national level (inter-agency) coordination for managing transversality in security research. France has a unique locus of governance: the National Research Agency, which follows a coordination approach. In Sweden, the Swedish Emergency Management Agency is responsible for security research governance, thus the

locus of governance is the first-responder level, and the method is standardisation – as in the UK case with a focus on foreign national (US) standards perceived as best practice.

There is a breakeven between the governance method of standardisation and the governance method of coordination. Four of the members states at stake here (all from the northern parts of Europe: Netherlands, Norway, Sweden and UK) are managing transversality by coordination (inter-agency), four (all from the more southern parts: Austria, France, Germany and Spain) do so by standardisation (internationality).

The following matrix systemizes the findings in search for a European security research panorama. For each country, the "load" of each of the three dimensions (factors) is marked on a bivariate basis:

DIMENSION (FACTOR)	"VALUE"
Thematic thrust	society-related vs. technical themes and subjects
Leading concept of crisis management	prevention vs. reaction preparedness vs. response
Transversal mode: Method of governance of cross-cutting issues/interdependency	coordination (national, e.g. inter-agency) vs. standardisation (international)

The strongest columns in the matrix are technical themes (5.5) and prevention-orientation in research for crisis management (4.5), whereas coordination and standardisation are equally strong (4). Thus, on a general level, it can be said that EU Member States' research programmes in sum favour technological solutions to security problems (or at least focus on technological as opposed to societal security issues) and aim at increase preventive efforts, rather than the capabilities to respond to crisis events. However, there is no all-European preference on a specific mode of governance for security research, apart from the north-south divide mentioned above, with northern European countries practising (international) standardisation and the others (national inter-agency) coordination.

	THEMATIC THRUST		CRISIS MANAGEMENT		METHOD OF GOVERNANCE	
	society	technology	prevention	reaction	coord	standard
Austria						
France						
Germany						
Netherlands						
Norway						
Spain						
Sweden						
UK						
filled boxes	3	5.5	5	3	4	4
no. of cases with which "X" is combined in the above lines	X		2.5	0.5	1.5	1.5
		X	3	2.5	3	2.5
			2	2	X	
			3	1		X
main quasi-correlation patterns						

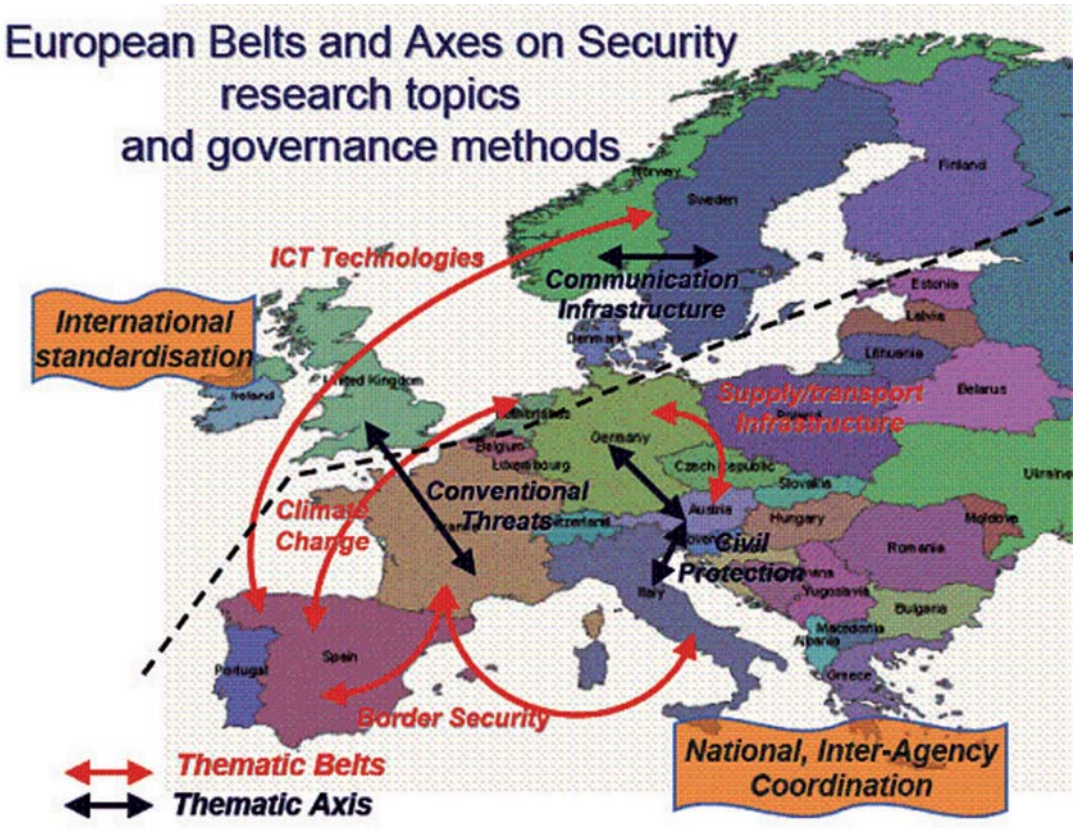
A comparative counting (lower half of the above matrix) of the filled boxes reveals a couple of illustrative associations ("quasi-correlations") on an ordinal scale level (sums of ticked boxes):

Both technology-centred and society-centred member state security research programmes clearly tend to focus on preventive crisis management/disaster prepared¬ness. The association between society-centredness and prevention is however stronger as compared to technology-centredness and prevention, which are only slightly tighter associated than technology-centredness and reaction. Society-centred research themes for the slightly most part go together with (international) standardisation as method of (research programme) governance, whereas technology-centred research themes slightly more often are associated with (national, interagency) coordination as governance method than with standardisation.

Read the other way round, a coordination approach to security governance goes together with a slightly stronger focus on reactive crisis management or disaster response, whereas a standardisation approach strongly goes together with prevention/preparedness. Efficient reaction to crisis and disaster response as research topics are typically governed by (national) coordination, so an inter-agency approach is more often applied here than an international standardisation approach. Preventive crisis management and disaster preparedness obviously are by the majority of the analysed states seen as themes that especially require internationalization in security research or at lest orientation on common (international) standards. Preparedness thus has a certain potential of becoming a European security research theme, whereas response will tend to remain a national security research theme.

10.2.1.7 "Belts" and "Axes" of Security Research Topics

As a further step towards picturing a comprehensive panorama, it can be concluded that there are four bows/belts of European security research thematic governance emerging: The technology (especially information and communication technology) bow from Spain to Sweden and Norway, the climate change bow from Spain to the Netherlands, the border security belt from Spain to France and the transport and supply chain infrastructure protection axis from Germany to Austria. Similarly, Sweden and Norway could be said to represent a communication infrastructure thematic axis. France and the UK may be seen to form a conventional threat/violence thematic axis. The southern half (in italics) of the countries addressed in this study rely on (national, inter-agency) coordination as the primary governance method, whereas the northern half follow an (international) standardisation approach.



10.3 Findings & Gaps

This section presents the real situation of "Governance and Co ordination" based on the assessment of Member States' policy and practice.

The ability (or lack thereof) to develop a shared understanding of Security, to overcome traditional national interpretations and frameworks for assessing security problems and solutions, and the existence (or lack) of a political cognitive construction (conceptual frame of reference) of a common European security space is the strongest political/structural/cultural factor that explains for a country:

- The potential (negative and positive) for a comprehensive approach at the national level
- The lack of potential for a comprehensive approach at the European level
- The success or failure in overcoming the lack of a comparable set of security strategies and approaches to security governance (co ordination vs. standardisation), including the improvement of co ordination of national security research and foresight activities with European-level research programmes
- The success or failure in overcoming the split in thematic thrust (society vs. technology), with a tendency to favour technological solutions to security problems)

These findings support the assumption that the development of a shared understanding of the concept of security is generally at the core of security research governance and co ordination. It also means that security research governance and co ordination founded on structural similarities can be disrupted by lack of a shared understanding of the concept of security or, for example, different strategies to give political meaning to technical questions of security.

10.3.1 Cultural Factors associated with Security Research Governance Gaps

10.3.1.1 Scope & Objective

This study provides an analysis of national cultural/structural/political factors which are associated the following status and gaps in EU Member States (including one non-member but FP7 participating state) security research governance; the identification of these is among the findings of previous analyses undertaken in the framework of ESRIF Working Group 10:

- Maintaining European security is complex and requires a comprehensive approach both at national and European level
- EU Member States' governments do not have a comparable set of security strategies or priorities to address adequately the current security challenges Europe faces
- National security research and foresight activities are not adequately coordinated with the European-level research programs resulting in gaps and overlap between activities
- There is a split in approaches to security governance (coordination vs. standardisation) and a majority focus on technical solutions to security problems

Political factors, even beyond typical political culture, are often associated with cultural factors: National perception styles determine which issues are seen as security relevant and where legislation and/or development of national capabilities to meet challenges is necessary; culturally embedded norms affect countries' approaches to the development security solutions (national, pooled or common European capabilities); culturally rooted values attached to the concept of the nation state determine to which extend national research policy is open to international standardisation or is in contrast concentrated on national coordination of relevant domestic bodies and agencies; etc.

10.3.1.2 Methodology

The methodology applied here rests on the "cultural theory of risk" (e.g. Mary Douglas/Aaron Wildavsky: Risk and Culture (Berkeley, CA et al.: University of California Press, 1982). This theory assumes that different perceptions and disputes about risk and security can be linked to competing worldviews: conceptions of risk, security and solutions to security problems vary according to the organization of political and social relations. Risks and security threats are selected as important because this reinforces established interpretations and relations within a culture, thus reproducing the symbolic foundations of a community. Among other "texts"

and "artefacts", security research programmes can therefore be taken as an indicator of security cultures, thus fitting the present analysis were well into the context of precedent security governance analysis conducted within ESRIF Working Group 10.

The subsequent investigation of cultural factors in this sense rests on a theoretically based differentiation between four groups of such factors, in addition to the cultural theory of risk. This differentiation represents state of the art in strategic security studies/strategic culture and is adapted here to cover the whole thematic spectrum of security research. The four groups of factors (arranged in four models) are then empirically investigated along four dimensions of gaps/need for coordination in security (research) governance according to the findings just listed above. The analysis is conducted on a country basis, considering the countries covered in precedent ESRIF WG 10 work: Austria, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and the UK. These countries were selected as being those EU/FP7 participating countries which have national security research programmes in place. In a follow-on step, the county-related results are aggregated so to gain insight on the general relevance of each of the four groups/models of cultural factors in respect of the earlier identified gaps and needs for coordination. A basic decision is made between whether a cultural factor can be expected to have a positive or negative effect on narrowing gaps and meeting needs for coordination.

The empirical results are listed in detail in the attached analytical matrix sheet and reported in this paper in sum (see annex IV, WG 10 annex 1).

10.3.1.3 Four Models of Cultural Factors in Security Policy: Values, Knowledge, Symbols and Repertories of Action

Social science approaches to cultural factors in political processes typically assume that culture is not a factor strong enough to explain similarities between countries that have strong structural differences, such as constitutional foundations, political system and system of government. Culture is rather seen as a factor that explains why countries that have certain structural factors in common still behave differently or why countries react differently to the same structural forces they are exposed to (such as international terrorism, IT security threats or the need for common security capabilities). An illustrating example is the question of why countries that follow society-centred security research programmes focused on prevention have different approaches to coordinating their national approach to counterterrorism with the EU strategy or follow different definitions of terrorism.

There are four different understandings of cultural factors in politics and policy (such as security research policy) development. These trains of thought represent models from the broader field of cultural analysis in political science and have been successfully applied to analysis in the framework of "strategic culture" research. In fact, the most substantial contribution to a cultural approach to comparison of national security strategies comes from this field of strategic studies. The basic structure of that approach can be per analogiam transferred to grasp cultural determinants of security research governance, definition of security research themes and potential for European coordination present in EU Member States. The present analysis thus carries strategic culture analysis further to grasp the whole of the thematic spectrum of security research in Europe.

A (chronologically) first school of thought *(model I)* understands culture as the ideational representation of foundational decisions about basic *normative values* (e.g. democracy, European integration, justice liberty and security), which shape the normative arena in which political decisions then take place. Seminal authors are Gabriel Almond and Sidney Verba. For example, a certain normative concept of civil society present in an EU member state may prevent that state from participation in international security (research) coordination, especially in the field of technical solutions to security problems, because this runs counter to that state's conception of liberty and self-determination of its people.

A second school of thought *(model II)* sees cultural factors as *cognitive* forms by which members of social communities make sense of reality, attribute meaning to facts as well as save and reproduce *knowledge* and their interpretation of the world. A seminal author is Clifford Geertz. This concept may be especially useful explaining the variety of research themes present in EU Member States' security research programmes and the interpretation of cultural factors as part of the security problem vs. part of the solution. For example, immigrant cultures may be interpreted as the cause of social radicalization processes that mount up to threats to internal security (such as in France or the Netherlands); differently, a user security culture may be interpreted as a social firewall against IT security offences (as it is the case in Sweden).

A third school of thought *(model III)* conceives of culture as *common symbols* of a (national or even transnational) community on

which members of a society orient their action and which are a kind of software for operating interfaces between actors (e.g. EU Member States) and overarching structures (i.e. European institutions for security research coordination and governance). The cultural key to the functioning of such interfaces is seen a system of symbols that is flexible enough to reflect and adapt to new threats and challenges. A seminal author is Robert Wuthnow. For example, a country that has a security culture centred on prevention and foresight as the symbol for security will have normative difficulty to engage in security research coordination centred on response/reaction and to accept topics such as civil protection as elements of a European security (research) agenda.

A fourth school *(model IV)* conceives of culture as *action* repertories, that is individual (or proprietary), experience-based strategies associated to individual attributions of meaning and normative convictions. This concept is strong in explaining how existing strategies and courses of action may determine which policy goals are developed or met, rather than strategies and courses of action being allotted to defined goals. A seminal author is Ann Swidler. Applied to security research governance analysis, cultural factors defined in terms of action repertories may best explain why EU Member States adapt differently to similar security threats and may also implement commonly defined security capabilities plans and research coordination strategies in divergent ways. Coordination for example may be implemented by Europeanization (development of or adherence to common standards on the EU level) or by a national joined-up interagency approach.

The four approaches/models can be classified along to two axes, as shown in annexes as
Table: *Four models of analysis of cultural factors and examples from the field of security research governance*

Culture as a factor in the perception/definition of threa

vs.

Culture as a factor in the response to threat.

and

Cultural factors influencing the thematic thrust of national security research programmes (e.g. prevention/preparedness vs. reaction/response; technology vs. society)

vs.

Cultural factors influencing the national approach to security (research) governance (e.g. national inter-agency coordination vs. international standardisation).

WG 10 findings have, as noted in the introduction, revealed the following gaps and need for coordination:

- Building potential for a comprehensive approach at the national level
- Building potential for a comprehensive approach at the European level
- Overcoming the lack of a comparable set of security strategies and approaches to security governance (coordination vs. standardisation), including the improvement of coordination of national security research and foresight activities with European-level research programmes
- Overcoming the split in thematic thrust (society vs. technology), with a tendency to favour technological solutions to security problems)

10.3.1.4 Assignment of Evidence for each of the Four Big Cultural Factors (models I-IV) per country to the Four Identified Gaps/Challenges

In matrix 1 of the attached analytical sheet (annex IV, annex 2), these identified gaps and coordination issues are associated with cultural factors according to the four models identified above. Within each model, evidence for each of the four big cultural factors (model I-IV) per country is assigned the four identified gaps/challenges listed on a country basis. This country-related information comes from the precedent comparative country analysis reported in the "Mid-term Threats and Challenges" paper as well as from preliminary results of the collaborative project "Changing Perceptions of Security and Interventions" (CPSI) from the FP7-SEC-2007-1 call.

"+" in front of an entry in matrix 1 means that the respective political/structural/cultural facture is conducive to meeting the respective challenge/narrowing the respective gap.

"-" in front of an entry in matrix 1 means that the respective political/structural/cultural facture can be expected to exacerbate the respective challenge/broaden the respective gap.

The matrix can form a basis only for tentative results, as the present empirical material does not allow for making assignments for all countries in every box. However, as the subsequent analysis is based on an aggregation of country entries in the matrix, the results can be expected to be sufficiently reliable to make statements about the aggregated effects of each of the four big cultural factors (according to model I-IV): We can determine by that method to what extent a cultural factor accounts for the existence of a gap or coordination issue or for the overcoming of such a gap or coordination issue. Put differently, we can provide an answer to the question if the respective cultural factor is part of the problem or part of the solution, or of both – as we will see will also be the case.

To approach this question, matrix 2 (annex IV, annex 2), produces on overall assessment of evidence for the four big cultural factors, integrating the country-related "+/-"-entries from *matrix 1 above*. In the left four columns of matrix 2, in each box the countries that have "+" entries for the respective gap and cultural factor in matrix 1 (meaning that there is evidence that in this country, the respective cultural factor can be expected to help close the gap/solve the coordination issue) are listed. In the right four columns, the countries that have "-"-entries (meaning a negative effect of the respective cultural factor on the respective gap) are listed.

The number of listed countries is then counted per line (per gap), and counted in sum in the last line of matrix 2.

The most visible result is that *model II* (knowledge/interpretation) has most evidence *for both favourable and adverse effects on the identified gaps,* except one case both per gap and in sum. Ability (or lack thereof) to develop a shared understanding of the concept of security, to overcome traditional national interpretations and frameworks for assessing security problems and solutions, and the existence (or lack) of a political cognitive construction (conceptual frame of reference) of a common European security space is the strongest political/structural/cultural factor that explains for a country :

- The potential (negative and positive) for a comprehensive approach at the national level
- The lack of potential for a comprehensive approach at the European level
- The success or failure in overcoming the lack of a comparable set of security strategies and approaches to security governance (coordination vs. standardisation), including the improvement of coordination of national security research and foresight activities with European-level research programmes
- The success or failure in overcoming the split in thematic thrust (society vs. technology), with a tendency to favour technological solutions to security problems)

These findings support the assumption that the development of a shared understanding of the concept of security is generally at the core of security research governance and coordination. However, it not only means that structural divergences between Member States (such as different modes of research governance or different thematic thrusts and implementation perspective – e.g. technological vs. social solutions to security problems) can be overcome by shared meaning. It also means that security research governance and coordination founded on structural similarities can be disrupted by lacks of a shared understanding of the concept of security or, for example, different strategies to give political meaning to technical questions of security.

Only as far as positive potential for a comprehensive approach at the European level is concerned, more evidence was found for model IV (action repertories) (see annexes),. This suggests that common (or at least compatible) practices of cooperation of a group of countries can lead to a harmonization and Europeanization of security research policies even when no shared understanding of the concept of security and no common interpretation of security threats and challenges exits.

Model IV (action repertories) is at the same time the only model with a majority of evidence for positive effects on gaps and coordination issues, whereas all the other models (normative values, knowledge and interpretation, common symbols) are in sum associated with evidence for the negative effects of the cultural factors which they assume.

The second noticeable result therefore is that in t*he majority of the gaps and coordination issues identifies, cultural factors are a part of the problem:* They for the most part account for the existence and widening of gaps and for lacks of coordination. This was found to be the case for:

- Lack of potential for a comprehensive approach at the European level
- Failure in overcoming the lack of a comparable set of security strategies and approaches to security governance (coordination vs. standardisation), including the improvement of coordination of national security research and foresight activities with European-level research programmes
- Failure in overcoming the split in thematic thrust (society vs. technology), with a tendency to favour technological solutions to security problems)

Just as remarkable, there is one sector of gaps/coordination issues in which *cultural factors are – on an aggregated level – a part of the solution, helping to narrow gaps and solve coordination issues:* The development of *a comprehensive approach to security research (governance) at the national level.*

10.3.1.5 Country-related Findings

Germany is the case in which cultural factors in sum have by far the most negative impact on managing security (research) governance gaps/challenges. *Italy and Sweden* are the countries in which cultural factors have the most positive impact. In the case of *France*, summarized cultural factors impact is neutral. *See matrix 3 and matrix 4 (annex IV, annex 2)*, for the results behind this country sum-up.

The *Netherlands and* Norway are cases where cultural factors according to *model II* (knowledge/interpretation) best account for both reduction and production of the identified gaps, thus both countries best represent the aggregated results noted above. In the political culture of the Netherlands, security is interpreted as a task of the level of the state organization as a whole, including societal stakeholders. This limits the scope for Europeanization, but at the same time, Dutch security research is guided by the interpretation of security as a sector that requires an alignment of the own national approach with that of other states and organizations. In Norway, the interpretation of security as information security is prevailing, which limits the scope of the country's research approach, but on the other hand, there is the political interpretation that solutions to (information) security problems need to rest on international standards/standardisation. Norway follows multidimensional, multifunctional approach – not only confronting threats to citizens and infrastructure but threats to values of the nation, from democracy, health and territorial integrity up to economic security and cultural values. On the other hand, Norway's interpretation of security follows strictly the concept of internal security the "riket" (kingdom). Therefore, in both the Netherlands and Norway, political/cultural factors positively affect compatibility of national security strategies or priorities with challenges and (search for) solutions present at the European/international level. At the same time, they limit the scope for defining common European themes for security research.

Italy, Sweden and the UK were found to make up for a common case in which cultural factors in sum have positive effects (which is also the case in the Netherlands). Additionally, in this three countries, factors according to model II *(knowledge/interpretation)* – as just discussed for Norway and the Netherlands for their negative impact – clearly have a positive main effect: They reduce divergences in the national security strategies, provide scope for a comprehensive approach both at the national and the European level and for reconciling split approaches to security governance in the context of a shared understanding of the concept of security. This is mainly due to these countries' culture of network-based approaches to security-policy making (including comprehensive knowledge management with inputs from different sectors of politics and society). There are accordingly national preferences for network-type to solutions to security threats, technological exchange and exchange of security information at a national level – and also at an international level, at least as information referring to developing standards or "security labels" is concerned. For example, Italy has the public perception of internal security and public safety as national tasks, at the same time political culture is open towards a Europeanization of the security sector due to long experience with internationally acting organized crime.

At the same time, cultural factors according to *model I (normative values)* were found to account for amplification of gaps in two (Sweden and UK) of these three countries. This is a case were value-based approaches to security do not reinforce

a common European idea of security research but lead to the development of separate national thematic references for security research (coordination). It could be argued that Sweden and the UK are countries in which questions that are in public opinion and policy framed as security questions are very close related to the normative foundations of statehood, reflecting threats to the idea of the state as a collective security provider (Sweden: integration of information from different sources for first-responder emergency actions; UK: responding to citizens' fear of conventional crime/violence and terrorist attacks), thus resulting in a predominance of national themes, however mirrored by an interest in implementing these themes along with emerging European/international standards, as well as making use of international knowledge and practices.

Austria and Spain represent cases in which the effect of *model-I and model-II* cultural factors is just opposite – and in which cultural factors in sum have a negative effect on security (research) governance. Normative values were found to contribute to reducing gaps, as both countries have a public culture that fosters the idea of making public choices on the basis of pluralistic assessments and with a view of the functioning of the social/political system as a whole. Styles of developing knowledge and interpretation (giving political meaning to facts) were found to have in sum an amplifying effect on gaps in both countries. In Austria, the tradition and structure of consocialism and consensus democracy limits the potential for developing shared European understandings on security problems and agree on a common interpretation of the value/seriousness of security challenges; the interpretation of security as a task of the level of the state organization as a whole limits the development of internationally comparable security strategies. It can also be expected to limit the social acceptance of international solutions for security problems, not (re-)designed to national needs. In Spain, normative ideal of security based on and contributing to innovation does not open up space for a promotion of comprehensive international solutions and convergence of security (research) strategies, as it is mainly interpreted in national terms of science and technology. At the same time, Spain typically uses EU institutions to promote its own agenda and to seek support for own positions. This tendency is however limited by mistrust against other security cultures rooted in the countries politicals culture, which is marked by an aversion against "security", resluting from remembrances of repressive security state in charge of public order.

France and Germany are cases in which *model-III* cultural factors *(symbolism and associated practices)* were found to reduce gaps. National characteristics of security lead to the perception of security problems as having a generically transnational and international character. Security is at the same time seen as a symbol of preserving the values acquired by the society as a whole. In France, security has become a symbol for crisis management in a broad sense, independent from the source of origin. In Germany, security has become a symbol of preparedness and ability for defence of the nation against threats from without and from within. Both need additional legitimacy from higher-ranking, international values, such as democracy, rule of law and European integration. This background of political culture explains the potential for establishing comparability between national and European security strategies and call for a more comprehensive approach on a European level. It however needs to be added that in the case of Germany, model-III cultural factors were also found to have exacerbating effects on gaps. This has to be understood in the first place as an effect of the German idea of a protective state (in the wake of the enlightened-absolutist public policy tradition of *"gute polizey"* in the 18th century), responsive to the specific security requirements of its citizens.

Model-II cultural factors, relating to *knowledge structures* and styles of interpretation, were found in France and Germany to in sum cause/widen gaps, just as they were in Austria and Spain. France's "sûreté" tradition/culture e.g. causes on overemphasis on the societal (as opposed to the technical) dimension, thus limiting potential for convergence of security research on a European level and causing incompatibility with the majority of national and European security (research) strategies with their focus on technical solutions to security problems. Germany's interpretation of security as a task on the level of the state organization as a whole/as a government matter in the sense of civil protection sets constraints on a comprehensive approach both on a national and on a European level. It also limits acceptability of coordination with other national and European-level research programmes, or at least the perception of such coordination as useful for solutions to security problems on a national scale.

10.3.1.6 Association of the Four Cultural Factors Identified Gaps/Challenges

Summarized oval all countries analysed *(see matrix 4, annex 2)*, cultural factors have the strongest evidence of positive impact on (developing) a comprehensive approach at the national level; they have the strongest evidence of negative impact on splits

in thematic thrust (such as society vs. technology-centred security research). They have almost neutral impact on (developing) a comprehensive approach at the European level.

Knowledge and interpretation (model II) – styles to make sense of facts as they are rooted in national political culture and reinforced by political structure are the strongest factors for better and for worse. They in sum have most country-related evidence and almost equally often account for the existence of gaps and the potential to overcome gaps. Factors related to knowledge and interpretation are most often associated with negative effects on all four types of gaps under consideration here. In particular, they hamper the overcoming of international splits in thematic thrust. They have not however a comparable main effect when it comes to overcoming gaps, playing the strongest positive role only in overcoming lacks of comparable sets of security strategies and approaches to security governance.

Cultural practices (model IV), e.g. experienced-based (vs. model-type) strategies of coordination and consensus-making about domestic security (research) policy alternatives, more often account for overcoming gaps than for the existence of gaps. They in fact have the least negative effect and at the same time the second strongest positive effect *(behind knowledge and interpretation)* on gaps. In particular, they increase the potential for a comprehensive approach at the European level. This reinforces our assumption that common or compatible practices/repertories of action between states can help streamline national approaches to security (research) governance or streamline national and European approaches even in the absence of common normative values and a shared symbolic understanding of security on a common (European) scale. The EU should therefore support cross-national compatibility of security capabilities as well as support standardisation and certification procedures through EU and national bodies.

Normative values (model I) (security as a societal, a technical, a European etc. value) and *common symbols (model III)* (e.g. are security threats symbolized by ICT, by crime or by natural disaster etc.?) in most of the cases account for the existence of gaps. In particular, they hamper the development of a comparable set of strategies and approaches to security governance and integration of research. Our assumption therefore is that a lack of common normative values between states as well as a lack of a common symbolic understanding/framing of shared normative values (e.g. counter-terrorism) reinforces gaps even if a common basis of knowledge exists between states.

In an overall picture across all countries studies, *political/structural/cultural factors typically increase the potential for a comprehensive approach at the national level.*

However, *political/structural/cultural factors typically limit the potential for a comprehensive approach at the European level, for overcoming the lack of a comparable set of security strategies and approaches to security governance (coordination vs. standardisation) as well as for overcoming the split in thematic thrust (society vs. technology).*

10.3.1.7 Policy Recommendation

EU action to enhance, support and coordinate security (research) policy of Member States should take into account that the development of a common "culture of security" as for example advocated in the European Security Strategy (ESS) – thus activating cultural factors in the process of policy implementation – will not necessarily facilitate harmonization of national security (research) policies. In the majority of the countries considered here, security continues to be a national cultural value. Common symbols and values representing security on a European level may (still) lead to divergent national responses. They need to be preceded by a process of convergence of national practices and instruments for security (research) governance; even more as Common symbols and values representing security on a European level may (still) lead to divergent national responses, and cultural factors have the least impact on the gap type "comprehensive approach at European level".

Enhancement of nationally driven initiatives for standardisation and certification, including support for already operating multilateral strategies may be therefore a more effective choice for EU action. The EU should accordingly support cross-national compatibility of security capabilities as well as aggregation and integration of standardisation and certification procedures practised by national bodies through proprietary repertories of action. This is enforced by the observation that they were found to have the least negative and at the same time the second strongest positive effect on gaps.

10.3.2 Analysis of Security Capabilities v. Defence Capabilities

10.3.2.1 Introduction

In the EU civil community, the objective of the Security R&T is to develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as acts of terrorism and (organised) crime, natural disasters and industrial accidents while respecting fundamental human rights including privacy, to ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security, to stimulate the cooperation of providers and users for civil security solutions and to improve the competitiveness of the European security industry and to deliver mission-oriented results to reduce security gaps.

In the Defence side, the mission of EDA is to support the Council and the Member States in their effort to improve the EU's defence capabilities in the field of crisis management and to sustain ESDP as it stands now and develops in the future. For this purpose, the four functions and tasks allocated to the Agency are the development of defence capabilities in crisis management, the promotion and enhancement of European armaments cooperation, the strengthening of the European Defence Technological and Industrial Base (EDTIB) and the enhancement of the effectiveness of European Defence Research and Technology (EDRT).

10.3.2.2 Defence R&T

It emerges from many experts debates that different conceptions of Defence R&T exist in Europe. The debates have revealed that if those different conceptions coexist, it is partly due to the various motives of carrying out Defence R&T:

- Evaluate technologies in order to meet with capabilities needs (improve its contractor capability)
- Develop technologies in order to fill the capability gaps and to support the competitiveness of DTIB (improve the capacities to provide products)

Different discussions also took place about the European R&T strategy under preparation by EDA, its relation with the CDP and its implementation, in particular the existing R&T project management tools (cat. B projects, JIP) or potential new tools. It is noted that beyond the 22 priorities identified by EDRT, other subjects of interest exist (even if they lead to more difficulties for co-operation). A better recognition of capabilities considerations and the development of an analytical approach could be an axis to be considered.

Some EU actors, particularly industries, have raised the issue of the necessity for dialogue with all stakeholders (industries, laboratories, universities, regions) and of transparency. This has been notably presented as a manner to optimise the investments (maximise the outputs) and to attract funds from other stakeholders than Member States and the idea of a common agenda has been raised in many discussions.

In addition to outputs maximisation, the increase of R&T devoted resources issue is raised in many contexts, with the possibility of a target for R&T devoted part in the defence budget and the setting of a fund devoted to facilitate technological exchanges.

Last but not least, it is noted that the technological capabilities of the new European Union

Member States (hold by companies, laboratories, research institutes) remain up to now unrecognized and the interest for developing knowledge on these capabilities is widely recognized.

10.3.2.3 Dual R&T and Security R&T

A general consensus is found in the EU stakeholders on the interest for developing as much synergies as possible between defence R&T and civilian R&T, and particularly security R&T. The debates are on the question of improving the use of civilian research for defence purpose and vice versa. All are convinced that basic R&T is mostly generic, not specifically civil or defence. Furthermore, the perimeter includes not only civil and defence, but also space (where ESA could be an example of possible duality).

For the moment, improving synergies between civilian research and defence research for defence purpose is quite difficult since we have borders between the different pillars. However, the Lisbon treaty gives hope that these borders will progressively disappear allowing more cooperation between EDA, EC and ESA, especially for high TRL.

Regarding the content, is possible to consider two main categories of research subjects, first technologies and components where Europe suffers from gaps creating dependencies for civilian sectors as well as for defence sectors and, second, downstream applications interesting both defence and security.

Current Member States Security Research could have commonalities with the principal conclusions emerging from this initial CDP as the need for persistent intelligence to support modern knowledge-based operations in complex environments, including full spectrum awareness, robust networks and appropriate architectures and the requirement for adaptive and co-ordinated inter-agency structures in order to support a comprehensive approach to EU crisis management operations and with some of the Initial Tranche (IT) of 12 selected actions:

- IT #1: Counter Man Portable Air Defence Systems
- IT #2: Computer Network Operations
- IT #6: Intelligence, Surveillance, Target Acquisition and Reconnaissance Architecture
- IT #8: Chemical, Biological, Radiological and Nuclear Defence
- IT #10:Counter-Improvised Explosive Device (C-IED)
- IT #12: Network Enabled Capability

Various approaches can be used in order to favour synergies, the search of the best possible top-down (capability pull) and bottom-up (technology push) compromise, notably systematizing the exploitation of civilian research for defence ends (with the identification of necessary defence complements), at the institutional level, the search for a better co-ordination between the EDA R&T action and the FP7 Security Theme (and, possibly, in a programme explicitly seeking synergies between security and defence R&T in the future FP8), for example by setting up mixed funding.

However, it seems difficult, presently, to go further. Nevertheless, a discussion on what could be the situation within FP8 between the EC, the Member States, the European Council and the European Parliament would be welcomed.
A strategic role is seen for EDA into the identification of shortcomings between military capability requirements and outputs expected from on-going developments, both civilian and defence ones. This would help identifying R&T projects in order to fill these gaps. However, it was noted that EDA should not duplicate efforts by spending resources to play a role on security R&T activities.

Cross-cutting technologies are in a difficult situation since one can note that they receive less and less support. A dialogue between EDA and other R&T stakeholders (EC, ESA, etc.) would be useful to decide which side is financing identified cross-cutting key technologies in order to share the funding burden while avoiding unnecessary duplication. Another role for EDA could be the information sharing between Member States for technology watch issues.

10.4 Solutions and Priorities

This section suggests all the actions that will allow European governance and co ordination on Security Research and Innovation.

Standardisation must play a vital role for the combined operational effectiveness of the Security Policies of Europe/Nations/Regions. Implementation of standards will help to:

- Achieve the required levels of interoperability
- Accomplish common strategic, operational and tactical tasks more effectively
- Understand and execute command procedures

- Employ techniques, materiel and equipment more efficiently

Given the split in approaches to security governance (co ordination vs. standardisation) and the majority focus on technical solutions to security problems; it seems advisable for the EU to support international compatibility of security capabilities as well as support standardisation and certification – with a European level of reference – through EU and national bodies.

10.4.1 Interoperability & Standardisation

The European Security & Defence Policy (ESDP) is increasingly important to the objectives of Interoperability and Standardisation. The ESDP will improve the EU's ability to confront existing and emerging 21st-Century security threats, particularly in joint civilian-military operations and crisis management measures ranging from intelligence-driven crisis prevention actions to security sector reform, reform of the police and judiciary and military action.

The existing relationship between NATO and the EU needs to be improved, making them ever more integrated, reducing duplication and creating permanent joint structures of co operation, while respecting the independent nature of both organisations.

The experience of EU operations demonstrates that the lack of a permanent planning and command capability for EU operations has become a capability shortfall. Given the civilian military focus of the EU, EU Operational Headquarters (OHQ) would not duplicate anything that exists elsewhere.

The challenge for both the EU and NATO is to make use of the same national pool of resources (both personnel and capabilities). WG10 calls on the Member States to ensure that their limited resources are applied to the most appropriate capabilities for tackling the difficult challenges of today, avoiding duplication of work and fostering coherence.

This rationale can be applied to the Security Capability Plan for each Member State in order to improve the Security Capability in Europe. Member States, having diff erent and sometimes divergent traditions and views, should fi nd a common understanding and adopt a common vision for the future European Security Capabilities.

In the following the idea of a common security capability plan for the EU is put forward. It is clear that this can only be a long-term goal, given that even within some Member States such a common security capability plan does not exist today. It is also clear that this is a very challenging and ambitious goal.

In the EU Security context, the NATO defi nition of "Force Interoperability" calling for "the ability of the forces of two or more nations to train, exercise and operate eff ectively together in the execution of assigned missions and tasks" (AAP 6) could be translated in to:
"the ability of the resources of one or more PMS and of one or more EU Agencies/Institutions to train, exercise and operate effectively together in the execution of the tasks/missions foreseen in the Common Security Capability Plan (CSCP)." [2]

10.4.1.1 Defining Interoperability

ISO-IEC provides the following definitions of the levels of standardisation:

Commonality (highest level)	"The state achieved when the same doctrine, procedures or equipment are used".
Interchangeability (middle level)	"The ability of one product, process or service to be used in place of another to fulfil the same requirements".
Compatibility (lowest level)	"The suitability of products, processes, or services for use together under specific conditions to fulfil relevant requirements without causing unacceptable interactions".

Interoperability has many facets, and the following table presents the most important.

Concepts	Concepts are drawn in CSCP, which establishes the European Security aims and tasks, defines its place and role in the structure of European Agency/institution, and sets linkages with National Resources.
Doctrine	Common doctrine as the guiding element of all activities
Tactics	Common tactics would further support interoperability.
Logistics	Interoperable logistic support will enhance interoperability and increase the "stability of the interoperability building"
Communication	Common terminology and language are important, as misunderstandings can create problems, sometimes fatal. Harmonisation of terminology, protocols and information exchange structures help to prevent such problems.
Materiel	Common materiel and materiel processes & procedures would further support interoperability.
Training	Training for joint operations will improve interoperability and thus enhance the entire operation.
Standardisation	The level of standardisation in these essential areas determine the level of Interoperability within multinational operations.

Certification

Certification refers to the issuing of written assurance (the certificate) by an independent external body (e.g. the International Standards Organisation, ISO) that it has audited a management system and verified that it conforms to the requirements specified in the standard. The development of standards should start with the identification of an interoperability shortfall generating a Standardisation requirement. Depending on who identifies the shortfall, either the Top Down or Bottom Up procedures could be initiated.

- Top-down: a mechanism (for instance a stable framework) in charge of CSCP identifies the problem
- Bottom-up: Problem identified by an Agency/EU structure

The same phases, identification, validation, ratification and implementation have to be coordinated in both procedures.

A mechanism (for instance a stable framework) should be in charge of the development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability and/or commonality that are necessary to attain the required level of interoperability or to optimise the use of resources, in the fields of operations, materiel and administration.

Given the split in approaches to security governance (co ordination vs. standardisation) and the majority focus on technical solutions to security problems, it seems advisable for the EU to support, at least in a first phase, transnational compatibility of security capabilities, as well as of support standardisation and certification – with a European level of reference – through EU and national bodies.

10.4.2 European Commission Models for Research Management

WG10 examined the European Commission paper "Towards Joint Programming in Research: Working Together to Tackle Common Challenges More Effectively – Impact Assessment" (Reference {COM(2008) 468 final SEC(2008) 2282}). This presented four candidate approaches to the management of joint research programmes, covering the entire range of research. It therefore considers those common themes of research management that are found throughout all research.

WG10 therefore is confident that its proposals benefit considerably from the thinking that was invested in this paper, it drew significantly on the four approaches when identifying what is clearly the most appropriate solution for security research, while not precisely aligning with any one of the four different options.

The following sections present WG10's recommendations for the governance and co ordination of security research programmes in the EU.

10.4.3 Common Security Capabilities Plan/Independent Adequate Framework

Before implementing an R&T plan it is necessary to develop an R&T strategy based on:

- Needs defined by the public and private end users in that case of "policy driven" research
- A shared global vision
- Capabilities priorities

This can be done by work to define and prioritize "capabilities" in a capability development plan. The aims of such work are:

- To make the global vision more specific and thus more useful
- To identify priorities for capability development
- To bring out opportunities to pool and cooperate

The CDP can (and should) be used as an important tool to guide R&T investments, but the CDP is not a work addressing only R&T:

- The CDP focuses on needs for capability improvement in security task terms, and not in technologies or R&T task
- The CDP does not focus exclusively on equipments or R&T: the outputs can be global technological needs for a better efficiency but also a better organization, a better use of existing resources etc. Not everything that is proposed by the CDP necessarily has an R&T component

Due to its importance (in particular the definition of R&T priorities), this capability development plan can be prepared by an "Independent Adequate Framework" populated by experts from Member States, Agencies/Institutions dealing with operational issues, through a constructive dialog between that structure and the "research world" (public laboratories and industry).

If we compare with the work done by Member States or EDA on the same topic "capabilities development plan", the main difference is not on the final objectives but on the participants: for the security domain a lot persons in charge of security missions (for example some surveillance tasks, some critical infrastructures) come from the private sectors and capabilities and have to participate in that independent structure.

The CDP is not a multinational investment plan. It is linked to the EU security missions and to security missions of EU Member States, and the private sector. It is an important difficulty to take into accounts the priorities and capabilities required by other sides.

One key factor is to differentiate when there are capabilities gaps to solve if it is due to:

- A research gap
- A development gap (to de differentiated from a research gap: this gap is often a "money gap"
- A resources gap (money, people,)
- An organization gap
- Etc.

Depending on the answer, a technology priority can be given.

Work in the border land capability development / R&T management development is needed to make that guidance concrete. The composition of such an adequate framework must have some people with a good technology level.

There also must be a dialog between this capability framework and

- A parallel equivalent R&T structure in charge of the R&T implementation
- Public labs and industry in charge of R&T execution

Annual workshops, ideas boxes can be a tool for this dialog. For industry, ASD organization can help.

For such a work there is a lot of existing competencies, in particular in European security agencies. Some agencies like Europol, ENISA, FRONTEX, EDA or IPSC have a lot of competencies in the main security missions (security of the citizen, critical infrastructures, border security or crisis management). Other European agencies can contribute; as can the Member States. We do not have to "reinvent the wheel".

European Agencies/Institutions coverage along the 4 mission areas *(not exhaustive)*	**"Independent Adequate Framework"**				
	EUROPOL	**ENISA**	**FRONTEX**	**EDA**	**IPSC**
Security of the Citizens (WG1)	I			I	I
Security of Critical Infrastructures(WG2)		I		I	I
Border Security (WG3)			I	I	I
Crisis Management (WG4)				I	I

At the end the capability development plan must get political approval at the right level.

The capability development plan (CDP) must be a continuous task to implement each year, due to the evolution of threats, of technologies etc.

After starting work, for one or 2 years, creating an initial CDP, an annual upgrading has to be done. The network / framework has to be defined with 2 geometries: one for the initial work, another to annually upgrade the CDP.

The capability development plan is not the final goal. There is also the Security Research Plan (SRP) and other actions necessary and strongly linked to R&T in security, including:

- EU bid detailed standard aiming to interoperability, to be successively promulgated
- EU Institutions/Member States to agree on a list of EU/National CoE capable to certify adherence to standard, utilizing at the maximum possible extent the existing ones even improving their efficiency and updating

The integrated package of CDP, SRP, Standards, CoE's will be the basis of the chapter on governance of the ESRIA.

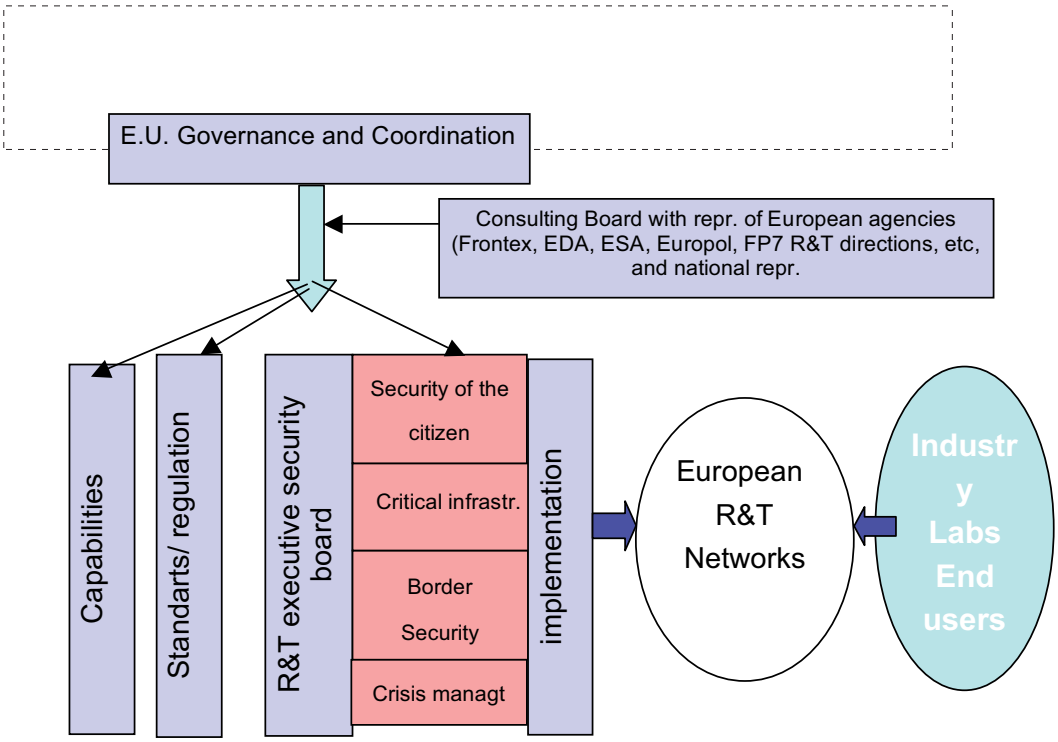
10.4.4 Implementation of Governance

A specific mechanism has to be defined for the governance of the ESRIA following the Lisbon treaty and keeping in close loop the representatives of each stakeholder.

We suggest the following guideline to define it:

- For each of the four missions, monitor coherence between all actors of security research following ESRIA
- Stay in contact with Technological and Industrial Base with a structured dialogue
- Use / take into account existing co ordinations [regional, national or inter governmental] in some fields example crisis management. Separate operational coordination to governance coordination
- Parallel Implementation between capabilities and R&T work

These are shown in the following diagram :.



Administrative coordination of of European R&T programs and some national programs or joint multinational program with additional European fund "could help".

For R&T a network with six topics: the four missions of security, plus cyber security (on topics strongly linked to security), plus a topic on transversal or underpinning technologies " could help".

An executive board and an implementation management is also envisaged.

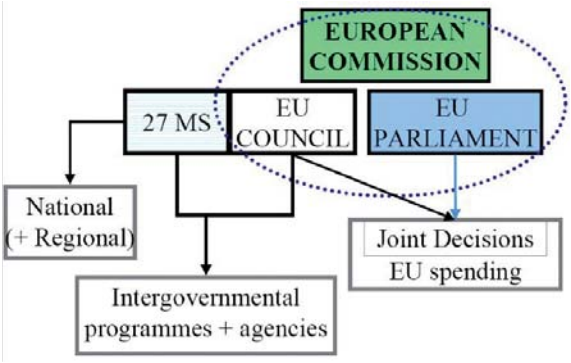
Demonstration platforms or technology platforms where people from labs, from industry and from the end user community (policemen, firemen) can work together for a final product strongly linked to the end user applications would be a right way to go on.

A strong Governance and Coordination is therefore needed to implement in parallel:

- R&T programmes
- Capability development plan and capabilities priorities
- Technical works on standards and certification tasks

10.4.5 Funding

WG10 also took into account the origin of the budgets: the budgets in security Research drive the coordination needs.



In the above figure it can be seen that the origin of the budget can come from each Member States (with a national and/or regional origin), from intergovernmental programmes and /or agencies, or for EU spending. Some programmes can have two or more origins.

10.5 Conclusions

WG10 unanimously agreed the following conclusions and recommendations.

10.5.1 Conclusions & Recommendations: General

The European Union should support:

- Compatibility of security capabilities among Member States
- Multilateral cooperation in international organisations and through partnerships with key actors
- Standardisation and Certification within a European reference system, co ordinated by the EU and implemented through national bodies
- Extensive use of interoperability between security and defence, (achieved through the "securitisation of the military markets" rather than the "militarisation of the security markets": Gilles De Kerchove)

10.5.2 Conclusions & Recommendations: Funding

WG10 considers that a Technology Investment Fund should be set up at EU level. Such an investment scheme should cover a number of key technologies that will deliver:

- Capabilities to protect critical European energy, transport and ICT infrastructure. This is mostly nationally owned infrastructure, therefore investment by the EU should be in the form of a grant subject to certain conditions, such as clear EU added value and interoperable technology
- Capabilities to protect the EU's external borders (including the relevant maritime surveillance). The same conditions should apply as for critical European infrastructure
- Capabilities to protect Galileo and GMES/Kopernikus ground & space infrastructure. As this is a truly European owned infrastructure, investment by the EU should be 100%.

(The above is in accordance with WG10's proposed vision on co ordination of ESRIA, as presented in Brussels 14 January, and amended according SEC(2008)2281 and SEC(2008)2282 on Joint Research Programmes

10.5.3 Conclusions & Recommendations: Governance & Co-ordination

WG10 supports ESRIF's opinion that Europe will need over the coming years to develop a **Common Capability Based Planning Process and possibly, ultimately a Joint Security Capability Plan (JSCP).**

The Common Capability Based Planning Process will be prepared by an "Independent Adequate Framework" populated by experts from Agencies/Institutions dealing with operational issues even through a constructive dialogue between that structure, public laboratories and industry (extensive use of inter-operability between security and defence), such as to translate capabilities in technologies and to facilitate prioritisation of efforts.
This **JSCP** has to get a political approval at the right level.

A mechanism (to be identified/ created) is necessary to update and maintain JSCP. The proposed Governance structure should act in accordance with the following principles:

- Central role for EU Governance and Coordination in accordance with Lisbon treaty keeping in close loop representatives of each stakeholder.
- For each of the four missions, monitor coherence between all actors of SR following ESRIA.
- Stay in contact with Technological and Industrial Base with a structured dialogue
- Use / take into account existing co ordinations [regional, national or inter governmental] in some fields example crisis management. Separate operational co ordination from governance co ordination.
- Parallel Implementation between capabilities and R&T work.

In the meanwhile, public and private stakeholders alike, both at EU and national levels will need to proceed to the systematic identification of available and required capabilities. In specific sectors, relevant agencies can play an important role. At EU level, current developments in EDA and FRONTEX could be seen as examples of good practices which might be considered by other agencies.

11. Working Group: Human and Societal Dynamics of Security

11.1 Introduction

Throughout Europe serious rethinking about security is underway. Traditional security concerns are combined with revised notions of the consequences of living in Risk Society. Several types of antagonistic threats, natural and man-made disasters are likely to be faced in Europe over the foreseeable future. States are developing novel practices for dealing with security challenges from abroad, at home and not least within its inter(national-do)mestic sphere. The trans-boundary character of the novel threats of the future will affect both the security challenges faced and our abilities to meet them in effective and legitimate ways. Research based knowledge and innovations in technology are needed to underpin reform efforts in this field. For a variety of reasons, an emphasis on societal security will be central to the success of this effort.

The concept of societal security has several dimensions. Its successful management requires a coordination and integration of a range of different professional traditions of safety and security at home, abroad and in-between. Organisational and mental barriers will slowly erode across jurisdictional, sector based and professional boundaries. This dynamic has been experienced in many other spheres of European integration, including in areas with traditionally firm nation-state jurisdictions.

11.1.1 Cross-cutting themes that need coordination across the work of ESRIF

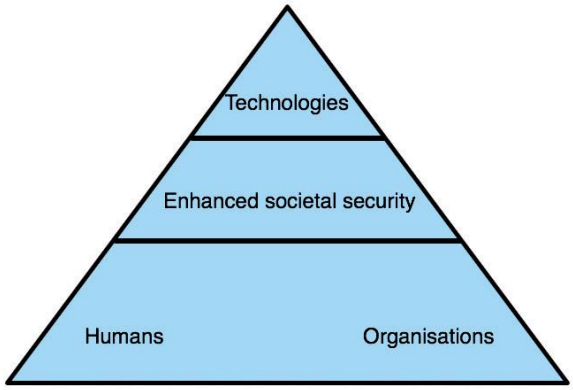
The ESRIF working group on Human and Societal Dynamics of Security (WG11) focuses on important societal related research that cuts across the mandates of all working groups. Technology can only be part of the effective response to security threats and must be applied in combination with organisational processes and human intervention. Solutions shall need to be multi-dimensional taking into account the different experiences and approaches to life across Europe.

The ESRIF research agenda aims to build new knowledge and technology about responses to mid term and long term threats and challenges to European security. The working group also aims to infuse the other suggested research and technology development programmes of ESRIF with human and societal aspects to help guide the development of both proposed technologies and resulting policies. For this second purpose, a Transverse Committee has been established under the leadership of Ms. Sadhbh McCarthy.

This group played the central role of identifying common interests, aims and premises for the work of the ESRIF. It developed themes that link together the many aspects of security research in European societies. It clarified shared social, cultural and political foundations and articulated the wide interests of various stake-holders in security innovation. These settled on a shared set of ambitions for the advancement of European values in a new security environment. The group formulated a number of ESRIF key messages that have been adopted in the Final Report. Also, the ESRIF priority research topics, presented by the eleven working groups, were clustered and linked to these key messages in order to ensure the coherence of the Final Report.

Among the cross-cutting concerns raised by this group has been the question of the affordability and usability of proposed security solutions. These can best be understood as a triangle of mutual dependency between advancing Technology, the possibilities and restraints of Human factors and increasing Organisational complexity. In order to enhance societal security all three dimensions must be integrated and scrutinised together well in advance of new research and technology developments are under consideration.

As the figure below shows, changes in one leg of the security triangle have 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 societal security system is only as robust as its weakest link, and in meeting societal resilience needs, human and organisational aspects have proven themselves, on frequent occasions to be the weakest link. It is therefore recommended that technological research and development projects awarded under the future security research programme should be evaluated also against the criteria of how well they take into account the triangle of mutual dependency of technology, organisational dynamics and human limitations.



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 almost 500 million people spread across 27 nations each with their own rich tapestry of traditions, historical experiences and approaches to life. The security of European societies can only be assured by attending carefully to this societal diversity and by remaining attentive to the widely ranging security needs and expectations it produces. This challenge in particular has been an underlying assumption running across the areas identified for research.

While it is true that technological research and development in Europe must be strengthened, one key to doing so is appropriate integration into political, social and human dimensions of security. Only by respecting these aspects will European security research be sure to lead to solutions that are adaptable to European diversity. Furthermore, such ability to deliver security solutions that are adaptable to diverse cultural and institutional settings will be a key success factor for European industrial competitiveness.

11.2 Challenges, needs and priorities for research

There is a need for building new knowledge along several fronts. We need to know more about the causes and the consequences of transboundary crises. The management processes and political challenges of such crises must be better understood. One needs to contribute to prescriptions for novel approaches to transboundary, multilateral and multilevel crisis management capacities. In all these areas, innovations in information technology sciences can assist with novel solutions.

There is a great need for research programmes that can develop new knowledge and technology that may result in enhanced practices and new solutions in this field. Research results should also underpin educational and training programs, as well as analytical support for eventual policy reforms.

11.2.1 Good governance

Good governance refers to the well ordered flow of information, authority and public resources. Good governance further enhances trust in democratic institutions and supports their good functioning and provides for good societal security. Good governance can be strengthened on the European level by increased accountability and seeking new ways to instil it as a norm. Research should continue to innovate and support experimentation in models of power sharing, coordination and interaction as the European government changes.

Good governance is reflected through the following themes:

11.2.1.1 Inter-organisational coordination

Inter-organisational coordination refers to the capacity to achieve coherent solutions in crises.

One main area of research is the theme of Prevention and Early Warning. This topic focuses on 'pre-crisis' processes bearing upon organisations' ability to detect, prevent or mitigate the severity of potential crises. Why are some organisations (or inter-organisational systems) relatively passive despite the availability of serious indications of vulnerability or threat, while others react more vigilantly or in some cases even overreact? Why are some organisations able to 'connect the dots' and develop/maintain qualified situational awareness (including the production and dissemination of status reports)? Organisational innovations such as so-called fusion centres need to be examined and their potential suitability for the European context assessed.

It is not easy to recognize emerging trans-boundary threats and crises in time. A network of organisations has to «put the pieces of the puzzle together» without knowing the picture. As we have seen in recent years, it is easy to miss signals that in hindsight seem impossible to ignore. European collaboration can be of great benefit here. Such collaboration is currently reserved for privileged intelligence partners and takes place in arenas far removed from political power (such as academic cooperation). Research is needed to probe the limits and possibilities of early warning and the interorganisational coordination required for it. Research is needed on the dynamics behind the interorganisational coordination and on the obstacles to coherent joint action by members of the distinct professions responsible for aspects of societal security.

The theme of Sense making and Problem Framing focuses on the subjective and socially constructed nature of crisis decision-making. Actors act not on incontestable and objective knowledge of the situation but rather upon their perceptions, interpretations and strategic representations (i.e. sense making) of what is happening. While problem framing often takes place on a semi-conscious, intuitive level - especially by 'naive' decision-makers - problem-framing processes exert a profound influence upon choice. In other words, once a problem has been framed, many possible lines of action have already been discarded and strong propensities for and constraints upon action have been created.

Framing is heavily influenced by cognitive and social structures and processes such as (historical) analogical and metaphoric reasoning, culture, context, organisation and information flow. Why do particular actors perceive and/or represent problems as they do at various junctures of a crisis? Why do these problem representations change (or remain stable) over the course of an unfolding crisis and its aftermath? To what extent do actors develop and share a common (or compatible set) of problem frames? This issue is closely related to the more operational concept of situational awareness.

In recent years, there has been an emphasis on institutional (and technical) innovations designed to improve the capacity to integrate crisis-related information, such as the above mentioned so-called fusion centres that have emerged in various countries. How functional are these solutions and are they viable and appropriate in the political-administrative setting of the EU?

The theme of Politico-Bureaucratic Cooperation and Conflict focuses on the issue of patterns of convergence and divergence, parochialism and solidarity, among the actors and stakeholders engaged in a crisis. There are a number of documented dynamics, which tend to create pressures for cooperation and solidarity in crisis (e.g. the 'rally around the flag' effect, leader attentiveness, and 'groupthink'). However, there are also a number of countervailing tendencies. Crises often present particularistic risk which may induce political or bureaucratic actors to engage in defensive behaviours, which may in turn antagonize other actors and lead to conflict. For example, following failures or setbacks, it is common for actors to play a 'blame game'. Equally importantly, crises present opportunities as well as risk and so actors may compete in seeking credit for their contribution (and denigrating that of others). Finally, situational and contextual factors tend to be moderated by the nature of personal relationships within policy communities and the strength of national cultural norms opposing opportunism in extraordinary situations. Is it possible to design crisis management organisations and practices in a manner which harnesses the benefits of competitive policymaking processes while avoiding the potential downside?

The theme of Accountability, Learning and Change focuses upon the extent to which actors are capable of analyzing their experiences and using the results as basis for change. As noted above in the discussion of problem framing, actors may attempt to use 'lessons' from past experiences (encoded as historical analogies or as experientially-based 'rules of thumb' as a guide for current

action. Similarly, actors may respond to positive or negative feedback regarding performance during a crisis, by drawing lessons and modifying beliefs and practices. Actors commonly attempt to reflect upon crisis experiences after the fact, draw lessons for the future, and formulate reform projects on the basis of interpretations of crisis experiences. Crises present considerable opportunities for learning, but post-crisis learning attempts are often distorted or derailed by a variety of typical social and psychological dynamics. Can researchers identify 'best practices' for organisational learning and change management processes conducive to sustainable gains of not only contingency-specific but also generic crisis management capacity?

11.2.1.2 Societal security and public-private partnerships

We are living in a time when borders between the public and private spheres are re-evaluated, transferred and becoming more porous. The strain on public finances has underpinned an ideological change regarding what the state and the private sphere should do and vice versa. The new public management (NPM) reform introduced a range of private sector management instruments into the public sector. Formerly closed markets are now open for private actors in which various forms of close and durable collaboration between public and private actors are set up. The ambiguous public-private boundary should be scrutinised further.

The overall research question in this theme is the following: What are the democratic implications, especially concerning democratic accountability, when the private actors take part in the public domain of the high takes sphere of safety and security?

Public domain is here defined as the action sphere in which public and private actors are embedded in a broader institutionalised arena concerned with the public goods and services. How can a stronger role for for-profit actors' in the public domain be democratically legitimate considering the fact that the private actors cannot be held democratically accountable for the decisions they make? Indeed, a stronger role for the private actors in the public domain raises questions on the classic dilemma between efficiency and democracy or what is sometimes defined as the distinction between output legitimacy and input legitimacy. It is also related to the accountability dilemma. The main justification for giving the private actors an important role in the field of societal security is that this can make the society less vulnerable and hence more effective. However, measures taken in order to make the society more stable and less vulnerable must also be democratically legitimate which requires political control. Societal security lies at the very heart of the responsibilities of the state.

11.2.1.3 A shared evaluative model

Crisis management is a difficult task that is judged and evaluated with remarkable ease when it is all over. What is lacking is a normative framework that spells out what we can expect from public leaders and crisis management structures in times of high stakes, uncertainty, complexity, and urgency. Differences between various parts of the Union, comprised of 500 million people, surely exist. Joint research can find the common ground of shared expectations and minimum standards. Such a shared model will help design joint capacity to manage trans-boundary crises. Failures of imagination, initiative or coordination will erode the public credibility of the governing capacity of the Union leadership. Consequential events in Europe, affecting the citizens and their common society, must not become crises of governance for the European Union.

11.2.1.4 Supporting actions

The environment of entangled dependencies, where critical functions and nodes on a national, regional and global level rely on the actions of others, creates a necessity for a well functioning EU response and recovery system. Future trans-boundary crisis management in the "inter-mestic" EU-domain should not risk leading to "a failure of coordination". It is imperative to secure in advance an ability to act effectively and legitimately and in concert within this new policy domain for the Union. Establishing regular joint exercises should be a low cost but high yield investment in improved EU practices, when they matter the most. Such training efforts must be founded on research based knowledge, innovative technology and robust methods. Such exercises would also highlight the need for interoperability in a technical, organisational and cultural sense. It could also spark useful discussions on standardisation and harmonisation, which should be of interest to industry and to the science and technology community. Gaps in knowledge, procedures and technology may be identified in such scenario based exercises.

Supporting action is needed on how to enhance inter-organisational coordination through joint training programs. A research-based program for capacity building and training needs to be established. This will improve cross-sector coordination and ensure a sufficient response and recovery capacity to major trans-boundary events in the Union. The goal of the training program should be to link

together - into enduring working level networks - professionals from different spheres of emergency management activity: Security and Safety professionals; National, Regional and Local authorities, Public authorities and the Private Sector; Public domain and Volunteer associations. Actors from all these spheres must be engaged in preparing for response and recovery activities as the consequences of trans-boundary emergencies will spill across several operative domains.

Strategic direction and priority setting in the face of major emergencies is not possible without a trans-boundary approach to response and recovery. This capacity must be developed over time and become institutionalised through continuous training. The focus of the training program will be on interactive exercises and scenario based simulations to strengthen coordination and create synergies within and between different sectors and levels, well ahead of acute events. Yearly exercises based on multiple types of hazards scenarios should be conducted.

11.2.2 Mediatisation and mass communications

Mediatisation refers to the autonomy of public events in media representations. Thus, in moments of crisis media cultivate perceptions that are not in correspondence with the actual situation, this making proportionate political action and trust difficult.

Planning for societal security and effective emergency management concerns identification of risks and threats, but also demands understanding of how people perceive and react to these hazards. Changes in the risk panorama of the future will naturally affect public perceptions and reactions. Social trends and shifts in values can also lead to new concerns and changed reactions to "old" risks. People differ in how they perceive risk and threat situations, and these differences need to be examined in the context of various individual, demographic and social factors. Different experiences and interpretations of these experiences influence both motivation to prepare and capability to act in crisis situations. It is reasonable to expect that the more complex and diffuse the future hazard panorama, the greater the scope for different appraisals of risks within society. This in turn highlights the need for a sound knowledge base for identifying vulnerabilities, developing communication and designing supportive measures.

In the public sector, one potentially serious error concerns emergency planning based on false expectations about human reactions. A number of myths regarding behaviour in crisis which might lead to such false expectations have been identified and reasons why these myths tend to be perpetuated have also been discussed. Analyses of experiences after Hurricane Katrina point to the very real and negative consequences of such disaster myths influencing crisis management. Theoretical underpinnings relevant to this research theme can be found in social science approaches in the fields of risk perception, risk communication, emergency preparedness and crisis management. At the level of personal risk concerns, a challenge for future risk communication would seem to lie in understanding how people deal with an increasing flood of information about different hazards, and in developing measures to help them cope with this.

Key areas for research include:

1. Studies of factors affecting cooperation between on the one hand public authorities, public and private organisations and on the other hand individuals and groups among the public. Important issues here concern new demands on risk and crisis communication in the light of new kinds of threat and the accelerating pace and global scope of events threatening public security.

2. A major challenge for the future lies in finding ways to integrate efficient procedures with public concerns and values. These concerns are likely to be increasingly diverse, and may shift gradually in response to societal changes or more rapidly in response to actual events.

3. In the new emerging communicative landscape traditional roles of journalists and media are being challenged and transformed by the introduction of new information technology. This has happened in parallel to the development of a new global security situation following the end of the Cold War and the September 11 events. Further adding to the complexity is the notion of the global 'risk society' where risks are no longer confined to national borders and can accordingly not be dealt with by single national agencies and governments. Taken together these broad trends call for new research approaches that require an integration of media-, security and crisis studies. One of the core questions

is how the new media in combination with the new conflicts give rise to a new kind of journalism and a new kind of journalist? There is an increasing awareness that the evolving media landscape, through the existence of blogger or/and new digital technologies have a profound impact on journalism and the journalistic profession, but little empirical work has been carried out in this field. Thus there is still limited knowledge on how new technologies impact on journalists' reporting on security and crises events. Are the journalists of today (and of tomorrow) de-ideologies, de-politicised, working faster, being more efficient while at the same time less inclined to analyze and make interpretations for the audiences, collecting information and pictures at home rather than on the field and drawing on different kinds of sources than previous generations of journalists? If so, how will that impact on the reporting from and the framing of today's and tomorrow's security crises?

4. It is fruitful to consider threats and risks in the light of the sociological discourse on modernity. In accordance with the rational thinking that characterises modernity and the demands it poses on the governance of societies, the modernity discourse points to accidents, natural disasters and disease outbreaks as man-made or controlled by man rather than 'acts of God'. Man-made crises call for explanations and cause people to raise questions about responsibility and accountability. The recognition of crises as man-made turns political actors and institutions into problem solvers and problem producers at the very same time. This lends to crisis managers a fundamental credibility deficit at the outset of their missions. Adding to this the mismatch between global problems and national institutional capacities for solving them, further points to how the issues of accountability and responsibility are heightened in today's complex transnational crises. In a mediatised environment where the image of the crisis management tends to be as important as the practice, the media play a pivotal role in assigning legitimacy to some actors while ignoring or delegitimising others. This is to a large extent done by framing the crisis as a 'blame-game', in which journalists tell stories of how sever the crisis is; how it could happen and who is responsible. A framing contest might occur in which various actors attempt to attract attention to their particular frame through the media. We know very little about how and with what success different security actors and crisis managers influence the media output, as well at the real impacts on legitimacy of framing by the media in different situations. With a growing number of transnational media (having no particular government to hold responsible) and with the increasing commercialisation of the media we need to ask how the roles of accountability and responsibility are upheld and by what media actors.

5. Research on the cooperation between public authorities and commercial media outlets is necessary in order to support journalists in adapting to a quickly changing information world and questions of media and democracy require new interpretations.

Losses of control over time and space and imagery may erode the capacity for societal resilience. A fundamental research area emanates from the media, communications and journalism discipline and centres on issues of democracy and legitimacy. This research centres on the power of the media to define and organise our experiences of the world, how it is governed as well as how the media might empower citizens (or not). The discipline has mainly focused on text analysis, while fewer resources have been devoted to reception and production studies. This has resulted in an extensive knowledge about how the media frame different crises and conflicts as well as what the barriers are for media organisations to report in conveying impartial and reliable information. Still, due to the lack of reception and production studies there is limited knowledge on how citizens, interests groups, international organisations and governments react to and act upon media coverage.

We also lack insights on the impact of instant and citizen generated news as driven by new communication technologies for the production of news and other media and its implications for understanding journalism as a profession. Thus, research is needed on the impact of novel and widely dispersed communication technologies for effective prevention, warning, response and recovery from transboundary crises.

Thus WG11 further argues for more research on what and how the media coverage translates to the field of crisis and security studies. How is news media coverage received and acted upon by citizens and by security actors? How do the new media impact on traditional journalism as well as on counter-strategies in asymmetrical conflicts, such as terror attacks?

6. Another research area focuses on communicative strategies-what media actors might accomplish and how they can achieve their desired objectives in the most effective of manners. This focus has to do with communicative flows between the media and other key actors involved in crisis management and conflict resolutions. However, research in this tradition tends to ignore the framing power of the media and the way in which the media enable or disable actors' capacity for communication. For our purposes, it should thus be noted that, especially the political crisis communication literature has made an important contribution in addressing the link between crisis communication and political processes such as accountability and policy processes following in the wake of crises. However, by asking research questions related to the effectiveness of crisis management, this kind of research lose sight of the more long term societal implications of crisis which might have benefitted from an open and critical discussion.

7. There is a tendency in previous research on journalism to understand news organisations as a homogenous set of organisations with identical norms, values and practices. However, the few comparative studies that have been done on news organisational production practices demonstrate that there are in fact important differences between organisational practices which impact on how events are being covered. By focusing research on the organisational level, knowledge will be gained that can help us understand differences between news organisations both on a national as well as international level. This kind of research will also provide knowledge on whether there is empirical evidence for an increasing homogenisation of news as has been proposed by the notion of global risk society.

8. As many journalists argue, reportage and comment must often go beyond the task of simply informing but also entertain audiences amid tight competition between media outlets for market share. Public bodies are obliged, therefore, to devise ways by which emergency information can be effectively transmitted, even in highly stressful settings, via media with differing production and business requirements, content styles and audience profiles.

As these strategies are developed and implemented extensive research is required, in parallel, to identify the impacts which they may have on the effectiveness of security plans and procedures. The core concern rests with how public bodies can facilitate transparency and vigorous media scrutiny of crisis measures while ensuring that emergency measures do not, however unwittingly, become led by media demands and opinions rather than by expert-identified need.

Research on the impacts of intense media coverage or the expectation of such coverage on how emergency agencies plan for or manage a crisis is, therefore, a high priority in the interests of effective emergency management, rigorous journalism and public confidence.

This research should translate into practical pathways for public bodies and media practitioners to assist them through the complexities of communicating and reporting crises without placing the public at unnecessary risk.

Collaborations among practitioners and academics which combine expertise in journalism/media studies and psychology should address how varied audiences respond to emergency information and coverage of crises. This research should bring forward best practices for public bodies and media outlets in the framing and dissemination of information in the interests of public safety.

One should also investigate how the experience/expectation of media coverage impacts on public bodies and, especially, on those charged with devising plans for and managing emergencies. It will identify guidelines to help ensure that public bodies, in engaging with the media, both facilitate transparency and deliver effective public safety measures. Likely expertise will come from practitioners and academics in the fields of security, media, ethics, politics, psychology and law. Research must reflect the changing landscape of media and, in particular, address and provide best practice strategies which reflect the increasing shift to novel media technologies.

Possible innovative routes of enquiry include:

1. Whether media scrutiny prompts public bodies to quality audit their emergency planning and crisis management and whether this assists in striking an appropriate balance between societal security and other basic values?

2. What legal, ethical and security issues arise when public bodies distinguish between information which, by its communication via the media, bolsters public safety and on the other hand information which is withheld so as to preserve security? What procedures, if any, can balance transparency and the avoidance of unnecessary risk while preventing abuses of power?

11.2.3 Violent radicalisation

Understanding and counterstrategies

Today's scientific research into violent radicalisation must be considered fragmentary and embryonic at best. Resources needs to be developed that provides cohesive focus for existing fragmented research efforts across national boundaries. Some baseline research has been conducted that provides useful direction. The European Commission through its network of experts commissioned four studies during 2007-8 that focused on: 1) triggering factors for violent radicalisation; 2) the beliefs, ideologies and narratives of violent radicals; 3) recruitment and mobilisation of support; 4) best practices in preventing and countering radicalisation.

Research is needed as well on the mechanisms of radicalisation as on counter radicalisation efforts.

The following **ten research suggestions** provide a comprehensive approach to the next wave of research into violent radicalisation.

1. **State-of-the-art research inventory into radicalisation**

   Research into violent radicalisation is fragmentary and often fails to integrate the dynamic interrelationship with countermeasures against the terrorist threat. This dynamic relationship changes constantly the nature of the radicalisation challenge. No research exists that captures this evolving complexity.

   More research needs to be conducted that encapsulates the existing growing literature, theories and methods into radicalisation research; models and existing findings which are critiqued and accumulated to prepare the way for the next wave of research. Much research focuses on the pathways into radicalisation and some have emerged on disengagement and exit strategies out of radicalisation networks and milieus. There needs to be a critical evaluation of the strengths and weaknesses of existing research and future research priorities. More research needs to focus on the connectivity between radicalisation as a phenomenon and the way in which countermeasures affect and changes it. More interdisciplinary research agendas are necessary as radicalisation is simultaneously involving individual socio-psychological factors; social and political factors; religious dimensions; cultural identity and group dynamics. Capturing the dynamics and complexity of these interrelationships in specific national contexts and over time is a prioritised research theme.

2. **Violent Radicalisation in Education**

   Research into radicalisation has found that education can be considered both as a key influencer and major intervention point. This means that more research needs to focus on curriculum development that takes into account radicalisation; best practices and models on how to approach and achieve effective delivery across levels and milieus; strategies for responding to radicalisation especially in higher education; capacity building and inter cultural competence development within educational establishments; for teachers; and for local public officials. Development of conflict resolution models needs to be considered within education to better build resilience against the forces of radicalisation and as a mechanism to handle cultural clashes that occurs in identity building among youths. How do youths navigate between different cultural identities; does mentorship work and what are effective mechanisms to engage youths on radicalisation issues? What should the role be for civil society in dealing with radicalisation?

3. **Best Practices in Crisis Management Dealing with Terrorism**

   Terrorism events severely test social cohesion within societies, whether it is small events that unleash vast social forces (murder of Theo van Gogh in 2004), a synchronised major event (London bombings 2005) or a metaphorical war (Muhammad Cartoon controversy in Denmark). Research needs to focus across contexts and incidents to compare the best practices and effectiveness of different approaches how to respond to and communicate most effectively with the public. The end game of these strategies is to assert government control and to manage down the effects of the violence and any associated polarisation between communities. More research needs to be conducted on best practice models how to best respond to crisis events from a communication and crisis management perspective. What are the lessons learned from different types of events? What type of messages needs to be crafted; how is this credibly delivered and how is this best delivered in a fragmented media environment?

4. Best Practices in Community-Based Approaches to Radicalisation

Both research and practice have shown that the most effective level of intervention against radicalisation occurs on the community-based level. Despite the existence of different community-based approaches there has been little effort to benchmark and evaluate the effectiveness of various measures according to national context. What works, why and is it possible to measure each measure and its effects in the community? More research needs to be conducted comparatively as to the merits and effectiveness of various community-based approaches according to context. Where should the balance lie between government interference and support and for more grassroots initiatives, civil society engagement and community-based approaches? In particular, studies on the way in which major cities have approached and managed radicalisation ought to be encouraged.

5. Developing effective counter-narratives

Strategically it is necessary to create mechanisms for a counter-narrative (against extremist elements with an exclusionary ideology and global agenda. The so-called Single Narrative is composed of an expanding collage of intertwined foreign policy and domestic issues that are difficult to separate and deconstruct and one that feeds into the grievance and view that the West is at war with Islam. Some have argued that it is the foreign policies and the regional conflicts that take precedence over domestic causes leading to radicalisation; others argue that foreign issues are only legitimating issues and it is the domestic grievances that are the primary causes for radicalisation. More research needs to focus on this interrelationship between the foreign and domestic parts of the Single Narrative.

Research needs to focus on: what is the media strategy of extremist groups? Who are receptive to the extremist message? How can the attractiveness of the extremist message be undermined? What weaknesses of the extremist messages can be utilised and is it possible to build resilience among the target audience?

Are there hierarchies of contested issues and which ones can be affected strategically and during times of crisis? What are the best strategies to deliver effective counter-narratives and who are best placed to deliver what part of this strategy? Is there a role for public-private partnerships? What are effective and credible delivery mechanisms?

6. The Role of the Media and Internet

Terrorism is invariably the 'propaganda of the deed' and the media has often been charged as being the 'oxygen' of terrorism. Competing narratives in a global, fragmented media environment may feed into the radicalisation discourse and the projection of grievances. Research needs to be conducted on the role media play in fuelling radicalisation and as a countervailing force against it. The role of symbolic discourse and the way it feeds into cultural identity needs to be further understood and studied. Similarly the Internet communities is an important gateway into extremist circles and research needs to focus on understanding the extent to which online discourse and media connects radicalised individuals with each other and how it affects the radicalisation phenomenon. On another level, research should be encouraged to study how existing self-regulation in relation to child pornography and racism could be similarly applied to radicalisation.

7. The Role of Gateway Organisations

Extremist groups that espouse an antidemocratic agenda and advocate separation from mainstream society is increasingly difficult to deal with for governments within democratic societies. On the one hand, these extremist groups may be viewed as a potential conveyer belt into further extremism leading to violence. On the other hand, these groups may be considered to absorb violent tendencies rather than promote them. Research needs to be conducted on what avenues are available for engagement for governments? Should governments engage radical elements? If so, what are the best methods and where are the pitfalls? Should these extremist groups be banned? How do European democracies engage and empower moderate elements as a countervailing force against extremism?

8. Limits of Political Activism

Freedom of speech and freedom of assembly and public protest constitute some essential elements of democratic practice and principles. Activism and public protest are part of a vibrant democracy. However, knowledge about where the limits lie is not always widely known among youths and activists. Where are the so-called red lines of social protest? More research needs to focus on how far political activism can and should proceed. Similarly research should focus on the limits of extremist activist groups; their strategies and behaviour to understand the dilemmas posed for democracies, social cohesion and integration agendas.

9. **Linkages with gangs and youth violence including the study of group dynamics and entry/exit strategies**
   Radicalisation and recruitment occurs through different pathways and in varying speeds. Research has uniformly shown that there is not a single trajectory into radicalisation. It is the cumulative combination of complex push-pull factors. Trends show a growing connection between gangs and radicalisation networks. Studies on gangs constitute a mature scientific literature and there is merit to consider the insights and lessons from gangs to radicalisation phenomenon. Similarly group dynamics constitute the engine of radicalisation. More studies need to consider the role of leadership and the specifics of group dynamics in understanding different entry/exit strategies.

10. **Connectivity between Extremism**
    Research shows that there is in some contexts a connection with right-wing extremism as a cause for radicalisation within some communities. Recent EU-commissioned studies on radicalisation have concluded that the sense of living in a hostile society that views Islam with suspicion creates pressure for religious communities. Some feel under pressure to assess, as Muslims, their relationship to violent radical narratives and the politics of the Muslim world without knowing these or their interrelationship. Similarly governments need to be cognizant of the effects of policies in order to avoid playing into supporting one or the other poles of extremism. How is this best done?

    Research needs to focus on the dynamics of interrelationship between different forms of extremism and across historical contexts. How do extremist ideologies and behaviour feed other forms of extremism?

11.2.4 Economics of security

Understanding the rationale and behaviour of actors is a challenge of the economics of security. This includes the economics of terrorism. Interests of European citizens and of those who might do them harm is often directly correlated with economic issues. Understanding the one can often serve to understanding the other. Even though this area has been researched in relative detail, the analysis should be extended.

11.2.4.1 Recent Developments in Security Economics

Security economics is the analysis of aggregate risk facing society and the economy using rigorous analytical and empirical economics tools. In line with ESRAB's recommendations of 2006, this area of research has made some steps forward. First, the European Commission's DG JLS commissioned "A Survey on the Economics of Security" (Brück et al., 2008). This work provides an overview of the existing research capacities and gaps in knowledge. Following up on this report, DG JLS has supported the initial development of the Network for the Economic Analysis of Terrorism (NEAT), which is a first step toward the sustainable development of capacities and the coordination of research topics among Europe's experts in security economics. The output of NEAT's first meeting illustrates that significant deficits in knowledge exist regarding the economic impact of terrorism and counter-terrorist policies. Also relevant is the FP7 project EUSECON (European Security Economics), which will analyze the causes, dynamics, and long-term effects of both human-induced insecurity threats and European security policies.

11.2.4.2 Current knowledge, capacity and research gaps

The critical review of the literature commissioned by the European Commission "A Survey on the Economics of Security"] uncovered **six critical research gaps** on the economics of security, which are not being sufficiently filled:

1. Much knowledge is based on theoretical reasoning with only limited and highly fragmented empirical evidence to substantiate the theory. The major cause of this gap is the restricted availability of data not only of terrorist behaviour but also of the behaviour of targets and their governments.

2. The literature is heavily biased to impacts of terrorism in industrialised countries, even though it is shown that a) most terrorism is occurring in relatively less developed countries, b) economic development in less developed economies can be negatively affected by both terrorism and security measures and c) there may be a relation between economic grievances and terrorist activities in terror host countries. Thus understanding the dynamics of terror in developing economies may prove critical for the understanding of insecurity in the EU.

3. Terrorism and counter-terrorist measures are often analysed in isolation in the literature, although this form of insecurity represents only one element in a larger "portfolio of risks" that includes other factors of insecurity, such as organised crime and mass violent conflicts. Further, there are several indications of substantial conceptual and practical overlaps between diverse threats to security that should be analysed within an integrated framework of the "human drivers of insecurity".

4. The available empirical literature in economics focuses largely on the macro-economic outcomes rather than understanding the underlying processes that lead to these impacts. Particularly little is known about the structure and behaviour of terror organisations, with the consequence that only limited conclusions can be drawn about the impacts and effectiveness of security measures to reduce terrorism.

5. The security economics literature focuses on the negative impacts caused by perpetrators but rather neglects impacts resulting from responses to terrorism. As the literature survey shows, economic impacts of terrorist events are transient in large economies but can be extended due to security reactions of targeted agents. Yet, no detailed research is available that studies the actual responses of economic agents to terrorism. Related to this, no aggregate analysis exists that studies the macro-economic consequences of security measures on economies.

6. Last but not least, little economic research concerns the explicit analysis of policy processes and institutions concerned with terrorism and counter-terrorism.

11.2.4.3 Recommended actions: research needs and priorities

Understanding the rationale and behaviour of actors is the main challenge of the economics of security. This includes:

1. The creation of a critical mass of research and policy advice capacity in Europe requires the establishment of a European Centre of Security Economics. This centre would allow security economists to communicate and cooperate and to enhance the visibility of economics and economists in security policy-making. Such a step could contribute towards establishing and maintaining a minimum critical mass of European research capacity in the field of security economics. This centre could also complement the national support for research on economic aspects of security.

2. The economics of terrorism and development: Even though this area has been researched in relative more detail, the analysis should be extended to cover three further fields. First, a wider range of developing countries, particularly in countries where terrorist activities have been more frequent, should be included. Second, while knowledge exists on the impacts of terror attacks on the economy under attack, no information is available on the economic repercussions of underlying terror activities in host countries. Third, this should also include analysis of the symbiosis of terror organisations and fragile states.

3. The micro-economics of the fear of terrorism: This area should demonstrate, through the applied economic analysis of individual and household data, as well as experimental economic approaches, how the perceptions and the fear of terrorism shape human behaviour and well-being in areas such as consumption, saving, investment, and labour market decisions. Furthermore, data on the attributes of radicalising individuals should be collected from security organisations and combined with official statistical sources. Still other possibilities include comparing the fear of terrorism to other mood-related variables like happiness or life satisfaction.

4. The economic impacts of security measures: This area of research should focus on the quantification of costs and benefits across-time derived from security measures. Cost calculations should address the societal effort related with the implementation of security measures in terms of investment required. Nevertheless potential large detrimental effects on the economy are sometimes easily overlooked such as increased frictional costs, decreased efficiency, transboundary impacts (e g externalities) and citizen dissatisfaction. Benefits shall consider the increase of welfare and wealth associated with the achievement of a safer society. Further research is also needed to cover the considerable knowledge gaps existing about the degree of success of the organising mechanism to satisfy society's wants in security i.e. the European industrial security market structure and its economic performance – in other words, additional progress is needed in the analysis of the interactions between security behaviour and societal economic growth across time.

5. Conceptual ground work is required in the field of economics to overcome the isolated analysis of terrorism in economics and place it into a larger framework of security and insecurity.

6. Data collection and methodologies: More representative and nuanced data of terror activity and security measures in Europe and worldwide and the development of methodologies able to account for the various non-monetary impacts of terrorism are critical to provide a more accurate quantification of impacts and repercussions of terrorism and security measures.

7. Structure and behaviour of terror organisations: This research area should provide a more nuanced insight into terrorists' preferences and motivations, the emergence, evolution and cessation of terror organisations and their inter-relation with actors of security and insecurity not least to be able to understand the effectiveness of security measures to thwart terrorism.

8. Knowledge about policy processes and issues: Apart from general accounts of security measures, a critical analysis of current EU policy should identify their coherence across member states, their effectiveness and their potential negative repercussions.

9. Understanding of counter-terrorist organisations: The effectiveness of counter-terrorism organisations and their alternative counter-terrorism measures should be pursued.

10. Knowledge about the relationship between media, terrorism, and counter-terrorism: While there is some research into this field, substantial gaps remain.

11.2.5 Legal framework and data protection issues

An open society is a necessity for a secure society. New security technologies risk putting aside the dignity of humans in the name of the security of society. Data protection links society's need for information about individual citizens and the needs and rights to privacy and dignity.

11.2.5.1 Taking privacy seriously

Rapid progress in the development of communication technologies, biometrics, sensor technologies and data storage and analysis capabilities is causing constant pressure on the fundamental right to privacy for both economic and security reasons. We have seen the development and implementation of new security technologies and measures throughout Europe. These are expected to raise security for European citizens, but they are at the same time increasing the surveillance of citizens and causing infringements of privacy.

A primary task of ESRIF is to develop criteria and guidelines for security technologies and measures in line with human rights in general and with the protection of privacy. Security technologies that are consistent with and enhance privacy should allow the security industry to develop widely acceptable security products. Integrating privacy in the design of new security technologies and systems will be a competitive advantage for the European security industry. It should be possible to implement them in such a way that in the future more security does not imply a loss of privacy.

The dynamics of an open society is a prerequisite for social development, innovation and economic growth. To act proactively not only with respect to security, but also in taking privacy seriously will be an investment for the future. When developing and implementing security technologies for the future, privacy will be enhanced by respecting the following principles:

- There is a baseline of privacy that is inviolable
- Privacy and security is not a zero sum game
- General access for law enforcement authorities to existing databases is not acceptable
- Preservation of privacy is a shared responsibility for all stakeholders
- Privacy protection requires continuous reassessment of criteria

11.2.5.2 Themes for future research

1. Exploration of the concept of a **baseline of privacy**. The concept is based on the democratic demand that there is a sphere of individual privacy which is beyond intrusion, irrespective of the competing concern of state security and the ever greater technical capabilities of security technologies. This concept builds upon the recognition of privacy as an indispensable element of individual security. It is divorced from a traditional proportionality analysis, whereby privacy rights may be trumped or limited by legitimate competing security needs. For illustrative purposes, a broad analogy with the principle of an absolute prohibition on torture may be drawn, whereby there are spheres of privacy which are absolute, and which are not subject to a proportionality analysis.

Research should focus on refining this concept and exploring its utility within the EU legal framework.

A related topic is the exploration of the **functional roles of privacy.** This would involve a root-and-branch analysis of the meaning and importance of privacy protection within the European legal and societal order. A clear and agreed understanding of why privacy is desirous of legal protection (whether from the point of view of individual autonomy and security, democratic development, legitimacy of security measures or even economic competitiveness) is crucial to develop a greater understanding of how privacy should be protected.

2. Exploration of the concept of **European Security Law** as a coherent, stand-alone body of law. The competence of the European Union in the sphere of security is a relatively recent development, and one which is still evolving. The legal foundation for this competence and its interaction with Member States' regimes is complex and its application is fragmented across various security areas – anti-terrorism measures, border management, police and judicial co-operation, asylum, immigration etc.

The lack of a coherent understanding of how the various legal strands tie together leads to a lack of transparency and consequently to a potential democratic deficit. A second consequence of this lack of coherence is the difficulty of ensuring that privacy and data protection requirements are met.

It is proposed that it would be of value to carry out a thorough review and analysis of the current fragmented European security law landscape in order to get a comprehensive picture of what kind of legal security regime currently exists within the EU. Such an analysis would also serve as a basis to carry out a further critical analysis of how the legal security landscape might develop. This would be of value to various stakeholders, including students and academics, policy makers, suppliers, enforcement agencies etc.

3. Exploration of the potential to develop an agenda for **revising privacy and data protection law and principles.** The current data protection regime in Europe has been in existence without significant amendment since the core principles were set out in the 1995 Directive (95/46/EC). These principles are in turn largely based on the 1981 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. Subsequent rapid developments in the technical capacity to generate and to process personal data, through advances such as the internet, mobile technology, RFID, biometrics and surveillance technologies, have led to a recognition that there is a need to revise the current data protection regime.

There is already a broad recognition within the EU of a need to modernise data protection legislation. As data protection is of fundamental concern to the security sector and the sector has considerable insight into the challenges of data protection, privacy challenges from the security sector should be considered in any revision of data protection legislation. For example, a mandatory requirement to deploy **Privacy Enhancing Technologies** is regarded as an important means to support data and privacy protection in view of technical and societal developments. The PRISE project has developed specific criteria for privacy enhancing security technologies. An agenda for revision of privacy protection needs to discuss the role of organisational and technical safeguards and explore the possibilities to include them as mandatory non-functional requirements in future regulations (by analogy to the "state-of-the-art" requirement for data security). Further research is required to explore the various potential inputs from the security sector.

In the interim, a related research topic for exploration is the possibility to develop best **practice models** and **codes of conduct** within the existing legal framework, which could learn lessons from the experience in other jurisdictions, such as the US Protecting Individual Privacy in the Struggle against Terrorists framework from the National Research Council or the Australian Biometrics Institute Privacy Code.

11.2.6 Ethics and trust

The security of citizens is increasingly dependent upon their own trust in the people and technologies supposed to assure it. As the complexity of technologically based security systems grows and the ability of citizens to understand and control the technologies that surround them weakens, trust in their ordered functioning and the dependability of their operators becomes crucial. Trust refers to the willingness of European citizens to put their lives and well-being into the hands of others. It concerns their confidence in different security systems and in their operators. Trust is, finally, the very source of the legitimacy of those democratic institutions entrusted with our security.

The nature of perceived and real security threats to Europe has changed immensely in the years since 2001. This rapid transformation has seen the emergence of the concepts of risk and uncertainty as tools for organising and mobilising response to perceived security threats. In particular, the Precautionary Principle - a standard for organising and legitimating action under conditions of uncertainty - has become prominent in discussions and official legislation on European security. Ethical knowledge underpinning assessments of how to take decisions under conditions of uncertainty is widely needed.

11.2.6.1 Themes for future research

1. Uncertainty as a challenge to European security

The emergence of risk and uncertainty as tools for analysis is driven by the acceleration of events and by the need for rapid political interpretation of events. The point of departure for our analysis must thus be an attempt to sort out the politics of security in Europe and the particularity of the European approach. This approach should include a consideration of the ethical challenges following from the need for rapid decision making in conditions of uncertainty.

2. Overview and analysis of current regulations

The problem of risk and uncertainty is evoked or directly addressed in a wide variety of European initiatives. The most prominent of these is the Commission Communication on the Precautionary Principle (2000), but there are a variety of other Commission and European Parliament documents that evoke the notion of taking political action in the name of European security based on an assessment of risk. These official positions need to be catalogued, documented, analyzed and compared.

3. Overview of technological responses to uncertainty and current needs

Concerns for security in Europe have been channelled into a significant investment in technological response to insecurity. The technological reaction has created a large-scale mobilisation of the European security industry. This mobilisation has focused on technology solutions to the challenges at hand. A typology of technological approaches to uncertainty is needed as to form a pillar of the analysis.

4. Revising the Precautionary Principle for EUROSUR

An official expression of the Precautionary Principle was already made in 2000 in the Commission document with the same title. Since then the scope of security concerns in Europe have both changed and expanded. Immediately on the horizon is the recently adopted aim to implement the European Border Control System (EUROSUR). This will open a new chapter in pre-emptive security in Europe. The analysis of its ethical assumptions and consequences is overdue.

5. Trust – combining technical feasibility and ethical coherence

The role of trust in assuring security, through cross-cultural technical collaboration and democratic legitimacy will play an ever more central role in the way Europeans meet the dangers of the unknown. The role of trust becomes particularly acute to the extent security challenges are seen as people-oriented. Health and human services are core examples of this. Trust in complex systems, such as those central to information technology cannot be made viable by technological

excellence alone. Such systems are socially dependable and thus capable of evoking an experience of security. Similarly, trust issues form the scope of a number of border security issues. Documents and data, practices must be reliable across cultures and national borders. Programmes such as the 'registered traveller' must hold the confidence of users that they are fair and just. Information transparency in security matters is not only about the trueness of available documents, but also about the reliability of claims to transparency. The civil security challenges presented by crisis management depend highly on the trust of the public.

Education, training and other forms of long term trust-building will be important for this effort. Likewise one should explore new forms of communication between public authorities and the population, assuring e.g. coherence in public communications, and appropriate measures for an improved cross-cultural understanding among crisis management stakeholders.

11.3 CONCLUSIONS

A holistic approach to security research and innovation must include efforts to ensure that the social, cultural, legal and political aspects of security are taken into account. Research programmes should reflect relevant ESRIF key messages, and thus promote overall "societal coherence".

This could be achieved by working for

- **Societal Security**
  Human beings are at the core of security processes
- **Societal Resilience**
  Certain risks cannot be catered for, nor avoided. Societies must prepare to face shocks and have the ability to recover
- **Trust**
  Assuring security implies nurturing trust among people, institutions and technologies
- **Awareness raising through education and training**
  Security is a common responsibility of all stakeholders; the citizen is at the forefront
- **Interoperability**
  Interoperability in multiple dimensions is essential to allow security providers to work together

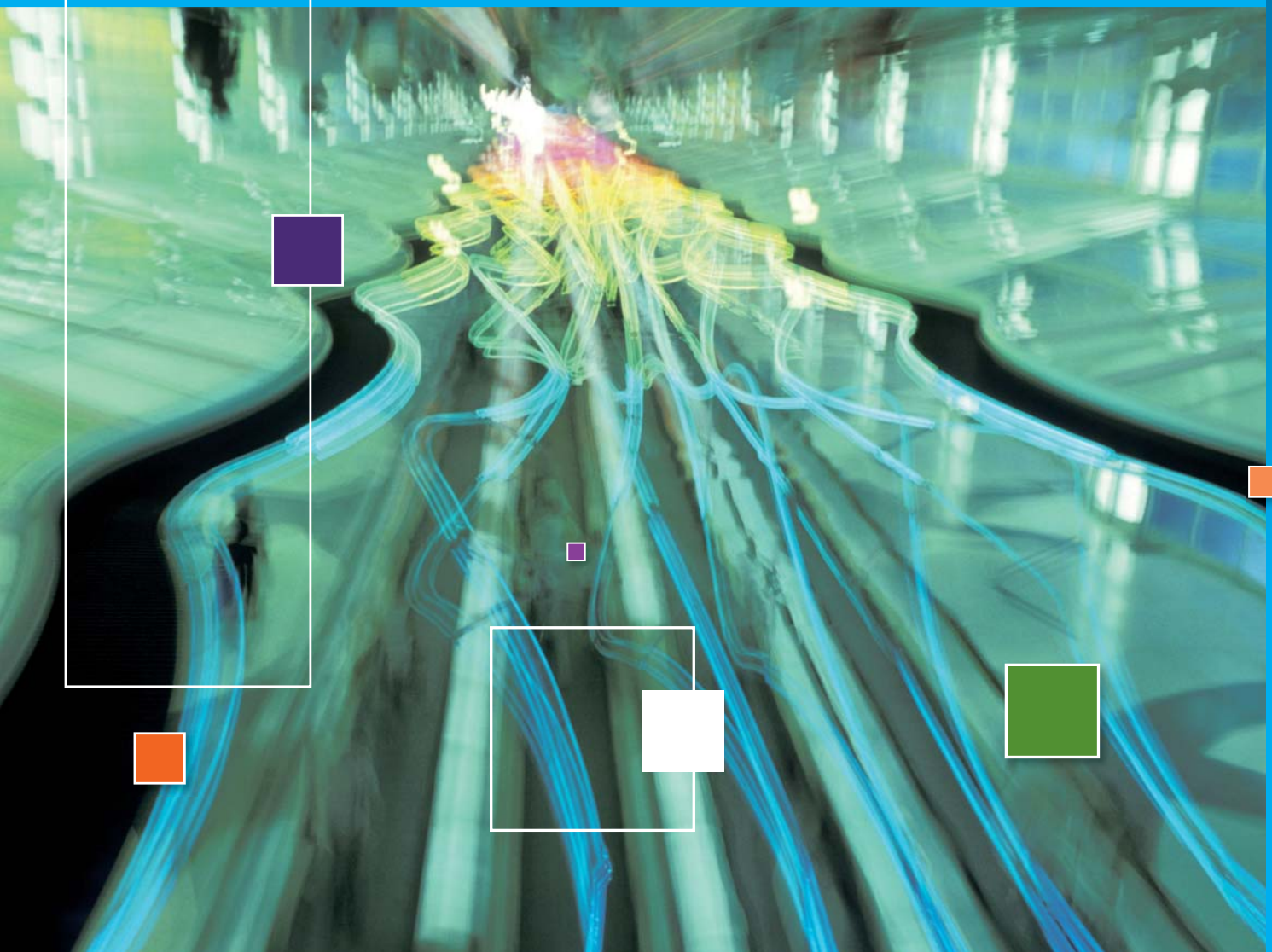
The overall societal security system is only as robust as its weakest link, and in meeting societal resilience needs, human and organisational aspects have proven themselves, on frequent occasions to be the weakest link. It is therefore recommended that technological research and development projects awarded under the future security research programme should be evaluated also against the criteria of how well they take into account the triangle of mutual dependency of technology, organisational dynamics and human limitations.

EUROPEAN SECURITY RESEARCH & INNOVATION FORUM

ESRIF

ESRIF FINAL REPORT

ANNEXES



ANNEX I

Terms of Reference (ToR) for the establishment and operation of the European Security Research and Innovation Forum (ESRIF)

1. Mission and objectives

- ESRIF contributes to supporting civil security policy making with the appropriate technology and knowledge base by establishing and carrying forward a mid and long term **Joint Security Research and Innovation Agenda** that involves all European stakeholders (both the supply and the demand sides). This creates a common basis in the planning of research activities and their timely exploitation, particularly through national and EU programmes. The role of ESRIF is solely consultative.
- ESRIF assists the **European security research sector in the mid and long term** through:
  - strengthening and highlighting the importance of a public-private dialogue in the field of the European security research and innovation by bringing together the demand and supply side of security technologies, systems and services, showing new perspectives for the utilisation of technology, accelerating the efforts of social and political sciences in relation to security research, and creating an atmosphere of mutual trust and cooperation;
  - continuous analysis of the future capability needs of the security demand side in the light of existing and future threats based on analysis of relevant impact factors of crime (i.e. terrorism) and of the supply side capabilities to deliver the relevant technologies, systems and services, which in appropriate cases should also lead to the definition of common user needs (both public and private), as challenges for enhancing the EU technology and knowledge base;
  - and promoting the integration of the full technology, systems and services supply chains throughout Europe (security research community; industry including SME; security demand side).
  - all the above will be addressed with due consideration of ethical issues, impacts on citizens' rights, and social perceptions of technological and broader knowledge developments in this field.

2. Scope and approach

- In designing and implementing its work, ESRIF will take into account the Commission Communication COM(2007) 511 of September 11, "on Public-Private Dialogue in Security Research and Innovation".
- ESRIF will not cover the activities of FP7security research[1]; its aim is to go towards meeting mid and long term security RTD needs throughout the EU to be covered by national, EU and private investments.
- ESRIF should contribute to increased transparency and joint planning of Security Research and Innovation programmes / activities in Europe, with a view to enhanced co-operation while reducing the gap between end user needs and available capabilities for responding to security threats in the most essential areas of vulnerabilities for an increased protection of our societies, economies and of European citizens in general.
- Through its operation ESRIF will contribute to promoting a Europe-wide single market for security equipment, systems and services, while supporting interoperability, integration, and smooth cross-border cooperation.

[1] which was the scope of ESRAB

3. Structure

ESRIF comprises:

- A single **plenary** with balanced representation of all stakeholders that are relevant for security research and innovation, both from the public and private sectors;
- a number of **working groups** that are defined by ESRIF;
- and an **integration team/steering group** which will support the operations of ESRIF. It will consist of: the chair, two vice chairs and the leaders of the working groups.

4. Membership

4.1 The notion "ESRIF Membership"

"ESRIF membership" refers to the members of the ESRIF plenary (only), who are supposed to contribute to the work of ESRIF in the plenary as well as in working groups. Other contributors at working group level are not "members".

Membership is ad personam.

4.2 Stakeholder representation / Composition of ESRIF

To ensure both satisfactory representation of all stakeholder groups and operability, the target size of ESRIF is 50-70 members. It brings together representatives of the relevant stakeholder groups from:

- *The security technology / solution demand side*
  - Authorities and end users in charge of civil security from the 27 EU Member States as well as from the FP7 Associated Countries;
- *The security technology / solution supply side*
  - Representatives of industry, research establishments and academia with a particular security profile;
- *Civil society representatives*
  - Think-tanks, civil liberty organisations and other relevant experts;
- *The European representatives*
  - Observers from the European Parliament (EP) from relevant EP committees;
  - European agencies and comparable organisations in the security and / or security research domain, such as EDA, EUROPOL, FRONTEX;
  - the European Commission, in particular its Directorates General concerned with security and/or security research issues.

5. Chairperson(s)

5.1 Election

A Chairperson and two Vice Chairpersons of ESRIF (i.e. ESRIF plenary) are elected in the constitution phase of ESRIF.
Leaders of the working groups are determined by ESRIF plenary as required.
Priority will be given to representatives of the demand side.

5.2 Roles

Tasks of the chairperson (can be shared with deputies): Overall guidance and coordination of ESRIF and its working groups; invitation, draft agenda, chairing and draft minutes of the ESRIF plenary meetings; representing ESRIF to the outside world.

Tasks of the working group leaders (can be shared with *rapporteurs*): Overall guidance and coordination of the working group; invitation, draft agenda, chairing and draft minutes of the working group meetings; representing the working group in the ESRIF plenary.

6. Confidentiality

ESRIF members, rapporteurs, sherpas, or any kind of ESRIF contributors, called hereafter *ESRIF contributors* should respect the following confidentiality rules:

ESRIF contributors agree not to disclose any information that is presented, discussed or made accessible during their participation in ESRIF to any person or legal entity other than another ESRIF contributor.

ESRIF contributors also agree that any information of which they may become aware of, or obtain, as a result of this access, will be considered as private and sensitive[2]. Accordingly, ESRIF contributors undertake not to appropriate any such information for their own use or to release or disclose it unless specifically authorised to do so by the owners of such information.

This provision shall remain in force for two years either from cessation of ESRIF membership/ESRIF contribution period or from the date upon which the ESRIF contributors shall last have access to such information. ESRIF contributors shall have a continuing obligation after the ESRIF contribution period has terminated not to disclose any sensitive or proprietary information[3] to any unauthorised person or legal entity.

7. ESRIF Working Groups

Structure, number, duration and mandate of ESRIF working groups and their leaders and *rapporteurs* are determined by ESRIF plenary as required. Contributors are nominated and invited by ESRIF members. The working group leaders have to be ESRIF members *Rapporteurs* can be members or additional contributors.

The following structure was chosen for the working groups.

1. **'Security of the Citizen'** primarily aims primarily to protect the citizen against terrorism and organised crime.
2. '**Security of critical infrastructures'** aims to protect critical infrastructures and utilities.
3. '**Border security'** addresses the control of air land and sea borders in the context of integrated border management.
4. '**Crisis management'** will look at the preparedness to react to catastrophic incidents.
5. **'Foresight and scenarios'** is relevant for and will give input to all the political mission areas. In addition, this group will address also the need for research in support of foresight.
6. '**CBRNE'** will address technologies and methods to detect chemical, biological, radiological, nuclear substances and explosives.

Working groups 7, 8 and 9 will coordinate with other mission area groups, in particular groups 1,2,3 and 4

7. Group 7 will deal with '**Situation awareness & the role of space'**
8. Group 8 will look at '**Identification (incl. tracking) of people and assets'.**
9. '**Innovation issues'** will address the Security Industrial and Technological Base, the European Security Equipment Market and interoperability and regulatory measures.
10. **'Governance and coordination'** will look at security policy making and implementation of security research at EU and national levels.
11. **'Socio-economic and ethical issues'** will address human and societal aspects of Security

[2] **Sensitive information -** is information or knowledge that might result in loss of an advantage or level of security if revealed (disclosed) to others who might have low or unknown trustability and/or indeterminable or hostile intentions.

[3] **Proprietary information -** Material and information relating to or associated with a entity's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as "proprietary information," trade secrets, or company confidential information.

8. Logistics

The operations of ESRIF are supported by a small team. In particular, the team supports the ESRIF chairperson(s) and is the contact point for all procedural and logistical ESRIF issues.

9. Operation

9.1 Plenary meetings

Plenary meetings are convened by the chairperson.

Taking into account that ESRIF may deal with sensitive issues, plenary meetings are open only to pre-registered participants, in particular members, observers and the sherpas of the chairperson, the vice chairpersons and the working group leaders. Further participants can be invited on ad hoc basis.

9.2 ESRIF Intranet

A dedicated forum on CIRCA (http://circa.europa.eu/, a collaborative workspace with partners of the European Institutions) is made available for the share of documents among ESRIF members and working group contributors.

ESRIF members and observers receive a password to access CIRCA and are responsible for the secure use of it.

10. Reimbursement of expenses

No reimbursement of the work input into ESRIF is foreseen.

11. Disclosure of information

If required, appropriate arrangements will be made for the work in all levels of ESRIF. In such a case, all persons and organisations involved will have to meet these requirements to continue.

12. Roadmap

Feb - March 2007	Agreement on approach amongst stakeholders
26 March 2007	Announcement at SRC'07 in Berlin
April – July 2007	Nomination and selection of ESRIF members
Sept 2007	Constituting meeting
Oct 2007	Setting up the Working Groups
Oct 2007 – Dec 2009	ESRIF operational
Late 2009	ESRIF Report
End 2009	ESRIF will automatically expire by the end of 2009

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
1	1	**Preparation of citizens for enhancement of societal security with respect to incidents**	Citizens have to be prepared for security issues and incidents, in order to behave optimally to prevent personal harm.	Behavioural analysis of people (collective and individual) for risk perception and emergency situation. education of population to security issues. human behaviour in stress situation Information / warning methodologies (incl. minorities) Organisation Governance / Decision making	3.1; 3.2;	1	mid term	
2	1	**Protection of soft targets**	The primary goal of any initiative devoted to protecting soft targets is the protection of people. The scope of this action is to introduce proactive and coordinated measures to strengthen the protection of soft targets, the ultimate aim of which is to guarantee normal life. Targets that require special attention are VIP's and major events.	Models for field cooperation around specific targets concerning systematic risk assessment and review of security measures. Methods and infrastructure for Information sharing: - providing public with updates/ alerts/ warnings, - private reporting about noticed unusual /suspicious activities.	3.1; 3.2;	1	mid term	
3	1	**Warning systems and new interventions concerning terroristic acts by organised groups and networks**	Being capable of detecting as early as possible the development of dissatisfaction in organised groups could help to prevent future evolution towards violence. Special attention for the direct and indirect signals of growing criminal intentions could create the basis for new early warning options and proper interventions.	Models for social dynamics of groups with high levels of dissatisfaction. Models for the social processes driving to the originating of personal criminal intentions and alignment with other persons with criminal intentions. Tracing of stabilizing and destabilizing triggers.	3.1; 3.2;	1	short term	
4	1	**Creation of cross-cultural, cross-generational, cross-societal links**	In order to increase the resilience of society and its resistance towards violence, human links of solidarity should be created across the city between communities, between rich and poor, between the educated and the uneducated.	Analysis of mechanisms that impact solidarities between citizens from various parts of town and of society. Methodology for the development of practical measures, eg information to new comers, dedicated activities.	3.1; 3.2;	1	mid term	
5	1	**A common European structure for cooperation between actors involved in urban security**	Defining the goals and implementing security at an urban level requires the involvement of all actors of security and prevention – local and regional authorities, police, judiciary, administration, health, social workers, including the youth and popular and immigrant classes. A common European structure is needed for cooperation in new developments comprising the various aspects of Urban Security	- exercise, training, cost / benefit assessment of prevention actions;	3.1; 3.2;	1	mid term	

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small25€; med 10-25€; large 30-40€)
6	1	**Common operation procedures for civil protection**	Providing an efficient civil protection requires a solid cooperation between the various organisations in charge. Such cooperation implies strong common procedures to protect and react.	- knowledge capitalisation tools (such as event / intervention data bases, "business" intelligence / process optimisation tools). - scenario simulation tools (incl. Virtual reality) for rapid assessment during crisis Connectivity / interoperability with the systems of the various responding or investigating organisations. Information systems for shortening of the reaction time. Protection of first responders against hostile treatment. Tools for Common Operational Picture: Use of data from external on-line data information sources (including from public peers).	3.1; 3.2; 3.3;	1	mid term	
7	1	**Enhanced resilience and protection of the financial and payment systems**	The fraud targeting the financial and payment systems is growing dramatically. New kinds of approaches are needed to address this major problem.	Elaboration of a common policy on the development and implementation of methods for financial investigations. Methods for training of relevant personnel in the private and the public sector for fighting against organised financial crimes. Monitoring systems for detecting counterfeit banknotes and coins. Rules and integrity standards for a higher transparency of financial systems. Tools and methods for investigations of financial systems. Tools for detection of fraud and counterfeiting of non-cash means of payment by the private sector (e.g. the retail sector).	3.1; 3.8; 3.13;	3	short term	
8	1	**Resilience and protection against cyber criminality**	Protecting the cyberspace from serious abuses is a vital challenge for the years ahead. New protective technological measures and cooperation between law enforcement agencies cannot lag behind modern forms of crime. Our citizens expect an adequate response from authorities.	Enhanced detection methodologies and blocking/filtering technologies. Improved systems for automatic translation. International applicable unique interfaces, protocols, connectors etc. for trusted exchange of sensitive information. Methods and procedures to detect dangerous sites. New anti virus programs identifying senders of messages, detecting potentially hostile intent and warning for malicious sites. New approaches for investigating the use of Internet. Search engines for detecting suspicious behaviour patterns.	3.1; 3.10; 3.11; 3.13;	5	short term	

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
				Tools to trace illegal activity in cyberspace, back to its origin.				
9	1	**Tracking of counterfeit money**	A special category of counterfeiting relates to counterfeit money, bank cards or documents and acts. Dedicated tools are needed to better detect and track such activity.	Mobile technologies for the inquiry of counterfeit money, bankcards, documents and act.	3.1; 3.13;	3	mid term	
				This would include artificial intelligence methods and agent technologies to support operational and investigative activities and evidence procedures.				
10	1	**Evacuation of population after a catastrophic event**	In case of major disasters or security calamities, evacuating (and sheltering) people from dangerous zones can be a huge challenge. Tools are needed to evaluate the optimum solutions.	Modelling and simulation tools of residential areas and built infrastructure, for virtual scenario's of evacuation and sheltering.	3.2; 3.3;	1	long term	
11	1	**Efficient communication during civil protection operations**	Efficient communication capabilities is crucial during crisis management. Existing solutions must be significantly improved.	Highly interoperable communication systems for crisis management operations with *integrated portable equipment* (radio, sat, ad hoc networks, …)	3.3; 3.11; 3.12;	1	short term	
				means to provide alert / warning / information to general public (media, dedicated equipment, …).				
12	1	**Explosives detection**	Existing detection equipments must be improved on all aspects (spectrum, performances, speed, ease of use, cost). The management of the information related to the use of explosives, vis à vis the public, is a major challenge to address.	Educative methods for preparing citizens to a better response with respect to the threat of explosives .	3.4; 3.5; 3.7; 3.9;	2	short term	
				Fast and reliable detection and control systems concerning all spectrum of explosives at vulnerable locations, buildings and events.				
				Quickly deployable protective solutions and tools for supporting balanced decision making on countermeasures to take .				
				Tracking and tracing and automatic warning (linked to detailed information on persons and goods, in respect of privacy rules).				
13	1	**Enhanced resilience of supply chains against pollution with counterfeited products**	Counterfeited products are spreading worldwide; impacting European business and economy. Specific action should be taken to address this problem.	Architecture for interoperable national and European databases.	3.7.3;	3	short term	
				Coherent international approaches for improved branding of products with better tracking and tracing of goods along supply chain.				
				Standard and harmonized procedures to support investigations in multiple Member States.				
				Systematic studies of the potential risks concerning counterfeiting of products.				

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
14	1	**Intelligence and data analysis**	A very large volume of data is available in public and open sources. Extracting intelligence from this data is a major challenge. New solutions are needed.	Retrieval capabilities for analysing the data and information available in a variety of proprietary or open sources but contained in unstructured, multilingual texts.	3.11; 3.14;	5	mid term	
				Special challenges are: - dealing with out-of-date and erroneous data; - structured data mining - video mining - social network analysis - machine translation technologies.				
15	1	**Surveillance for civil protection**	To monitor situations, security forces must dispose of efficient equipment to carry the surveillance activity, from small to very large areas, including in hostile environment.	Autonomous wireless / disposable / miniaturised sensors.	3.12; 3.14; 3,1	1	short term	
				Bio- and environmental sensors.				
				Improvement of electronic devices for surveillance tasks on board satellites and planes.				
				Intelligent collaboration of heterogeneous sensors is a major challenge.				
				Next generation video protection / threat identification systems.				
				Robotic devices for S&R.				
				Tools for localisation in closed / hostile environment.				
16	1	**Forensics methodology**	Forensic activity requires a large cross-border exchange of information. Common methods and tools are needed to improve the efficiency of these exchanges.	Common structures for databases.	3.13;	5	mid term	
				Common models for effective application and evaluation of forensic science in a complex multi-jurisdictional environment.				
				Statistical methods, and tools, for objective interpretation. Standardized European protocols.				
17	1	**Analysis of forensic traces**	Analysing evidence on a crime scene is the basis of the forensic approach. This evidence is, most of the time, composed of various kinds of traces which require sophisticated tools for analysis.	Appropriate training and education methods.	3.13;	5	mid term	
				Decision making and risk handling models to manage real time application of outputs from analysis.				
				Improved trace recovery.				
				International standards for trace recovery				
				Recording and reconstruction of the crime scene.				
				Screening methods for detection and on site analysis (portable, robust, high speed, sensitive and simple to use).				
				Software for scenarios visualization.				
18	2	**Resilient system architectures**	The growing complexity of security-relevant systems makes prevention and protection increasingly difficult. Emphasis should therefore be placed upon increasing a system's	Studies on specific system interdepencies and resilience requirements	3.7; 3.7.2; 3.11; 3.12;	3	short term	
				Methodologies for vulnerability and effects assessment incl. spill-over effects				

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
			capability to absorb shocks and recover.	Models of fallback procedures in case of incidents (e.g. transportation)				
				Models of best-practice infrastructure development (e.g. levels of decentralization)				
				Autonomous damage assessment and mitigation protocols				
				Development of smart materials (in nodes, structures and vehicles)				
				Adaptive simulation and modelling tools development for crisis situations				
19	2	**Transportation of people and goods**	Transportation of people and goods will remain a critical area for security research in the next 20 years. New means of transportation will be developed, having their own security specificities. All the while, "classic" security assets must be continuously improved	Studies on future transportation system specificities (air/sea/land/space)	3.7; 3.7.3	3	mid-term	
				Operational, inter-system (air/sea/…) contingency plan development				
				Development of tracking/tracing/localization and remote status querry technologies and systems				
				Development of systems for transportation network monitoring and surveillance				
				Prohibited substance/articles detection development for remote/stand-off and high-throughput environments				
				Adaptive simulation and modelling tools development for crisis situations				
20	2	**Power generation & dissemination**	Europe is heavily reliant on ist power generation and transmission grids to ensure that standards of living and essential functions can meet their requirements	Studies on best practices of secure generation&transmission system characteristics	3.7.2;	3	short to mid term	
				Development of secure automation and control methods for stations and grids				
				Studies on generation environment security specificities (e.g. marine/off-shore, "green" power generation, decentralized etc.)				
				Development of effective autonomous shut-off procedures to mitigate cascade and chain effects				
				Development of common procedures and interfaces enabling rapid re-onlining of affected grid elements				
				Studies on and development of subsitutes for insecure power generation means and resources				
				Adaptive simulation and modelling tools development for crisis situations				

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
21	2	**Secure and fast computation and communication technologies**	ICT, including the realm of Cyberspace, is of critical importance for modern European societies in many facets. This priority topic not only refers to security thereof, but also to capabilities in non-threatened state, i.e. computation or data transfer power.	fast and secure broadband communication technologies,	3.11; 3.12; 3.14;	5	short term and ongoing	
				Research on: increasing computation power and cognitive correlation capabilities,				
				resilient architectures design				
				securing computers,				
22	2	**Sensibly Interoperable Systems**	Crises do not respect national or systemic borders, but tend to spill over and cascade through systems of like nature. At the same time, low barriers to interoperability are of benefit in operations. Therefore, sesnible and secure interoperability and understanding of interdependencies is of essence	Studies on vulnerabilities and effects spill-over between linked systems	3.7; 3.7.2; 3.11; 3.14;	3	short to mid term	
				Studies on inter-system re-routing and fallback solutions				
				Development of static&flexible system barriers enabling operations without reducing security;				
				Development of standardized protocols for rapid re-onlining of linked systems				
				Development of node and hub surveillance and security protocols				
				Development of secure, standardized interfaces and middlewares				
				Adaptive simulation and modelling tools development for crisis situations				
23	2	**Reliable, linked and affordable detection**	Security of dispersed structures and systems is heavily dependent upon detection, verification and identification means. Sensor data needs not only to be made available, but also to be logically connected, made sense of, verified and visually displayed.	affordability where mass availability necessary	3.7.3; 3.4; 3.5; 3.6; 3.10; 3.13;	2	short to mid term	
				identification capability,				
				Research on: networks of improved sensors with broader sensitivity (CBRNE, non-metallics),				
				sensor fusion,				
				stand-off and high-throughput capability,				
24	2	**Situational awareness and decision making**	Security operatives will increasingly be faced with enormous amounts of information. These need to be filtered, made sense of, displayed and visualized in interfaces that are capable of handling massive amounts of data input, in order to create a comprehensive and detailled, yet not cluttered common operational picture.	Research on: methodologies of optimum operations conduct;	3.1; 3.2; 3.3; 3.7.1; 3.9; 3.12; 3.14;	4	mid term	
				flexible technical and operational interoperability of security actors				

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small25€; med 10-25€; large 30-40€)
25	2	**ID of people and goods, tracking and tracing of goods**	Referring not only to biometric ID documents, but also to goods integrity monitoring and localization tools, and lastly to safe cyberspace identities, this area is of increasing importance in the future.	research on: Technologies for ID'ing, tracking and tracing of goods, as well as their integration into a larger, internationally interoperable monitoring system	3.7.3; 3.9; 3.10;	4	mid term	
26	2	**Secured critical goods& capabilities access**	Euopean economies and societies are in need of access to both basic resources critical for consumption, but also of the capability to produce critical goods and services without outside influence. What these are and how such dependencies can be bypassed needs research.	alternative solutions	3.7; 3.7.1; 3.8;	3	short term	
				critical necessary manufacturing capabilities and capacities;				
				research on: critical resource dependencies;				
27	2	**Social embeddedness and empowerment of the public**	Security is a reciprocal process: generating understanding and empowering the public to be a full security actor will increase security across the board in systems that directly interface with the public.	new modes of communication;	3.2; 3.3; 3.7.1-3; 3.11;	1	short term	
				research on: new models of system/content governance;				
				role of the public in directly interfacing systems;				
				trust generation techniques				
26	3	**Integrated Surveillance Management - seamless, unimpeded access to surveillance and intelligence data of different tiers, requiring interoperability/interfaces and procedural as well as legal frameworks**	Border security, not defined as a static line but as a layered, area-wide security approach, will require the flowing use of numerous surveillance methods - intelligence feed (COMINT, ELINT, etc), fixed and mobile terrestrial sensors, maritime vessels, patrol aircraft and space surveillance assets. Only such a concerto of assets, adding layers of area surveillance, detail and linked with intelligence assets, can provide a comprehensive, scaleable and flexible surveillance system. Such a capability would enable European security agencies to not only monitor glacis and border area movements, but also movements within Europe that are subject to customs.	capability to integrate new assets into the surveillance cover (i.e. UAVs)	3.7.3; 3.9; 3.10; 3.12; 3.14;	4	short term	
				comprehensive complex system integration guidelines (architectural, technical, operational etc.),				
				development of new and integrateable sensors,				
				high-seas surveillance capability,				
				intelligence input integration,				
				legal frameworks,				
				research on: sharing and pooling of legacy and future surveillance assets (upgradeability),				
				systemic interoperability prerogative,				
				tracking&tracing capability,				
27	3	**Sensors, Detection and Identification - development of new concepts of, and**	In line with prior item (integrated Surveillance Management), sensors will need to be continually improved to enable better, more	active and passive underwater sensors,	3.4; 3.5; 3.6; 3.9; 3.10; 3.11; 3.12;	2	mid term	
				advanced identification of people and goods,				

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
		improvements of existing, sensors; platform integration, systems interfacing (i.e. with future tracing/integrity monitoring solutions), ID checks and management	reliable, higher distance capabilities regarding the surveillance sequence. This will give security actors access to more detailled data required for execution of their tasks.	airborne radars (A/C, LTA, UAV), clutter-clearance protocols, ESM capabilities (including GSM), hazmat detection capability in high-throughput environments optical cameras, remote sensing satellites with high resolution scanning cameras (imagery) and new technology radars, research on: Coastal based high performance radars (HFSW, FMCW),				
28	3	**Communications - adaptive width broadband data transfer to/from sensors/control centers, secure communications,**	Border security forces and assets need to be able to enjoy secure communication over long distances, with rapid transfer of larger amounts of data upon situational demand. Only this will enable them to evaluate and react within reasonable amounts of time.	definition of information exchange interfaces and property guidelines, encryption and authentication tools internet-like access to data, research on: adaptive secure broadband communication over long distances,	3.2; 3.3; 3.11; 3.12;	5	short term and ongoing	
29	3	**Common Operational Picture Generation and Dissemination - generation of intelligent situational picture from multiple sensors and sources, intelligence-feed and intelligent processing, dissemination of relevant data to related services**	In the multinational arena of European border security, COP generation from various multinational sources is an issue, as is reciprocal exchange of such data, or up/down-filtering of relevant data to and from engaged agencies. This is the core capability for rapid reaction and intervention for border security forces.	data mining software dissemination protocols, information validation through cross-referencing and data correlation, research on: generation of enhanced intelligent COP from to be defined sources, technical and operational interoperability,	3.11; 3.14;	5	short term	
30	3	**Standardization, Norms, Interoperability - standardized equipment/elements, similar procedures/protocols, joint operations, education and training**	In order to achieve maximum efficiency in operations and reduce costs of technology procurement and operations conduct, standardization where feasible and interoperability are key	development of affordable technological solutions, development of generic interfaces/middlewares, norms of implementation research on: development of common operational and procedural guidelines and requirements,	3.11; 3.7; 3.7.2; 3.7.3;	4	short to mid term (meaning such an endeavour should be started asap, but would be	
31	3	**Role of Intelligence - source access and validation of**	Broadly defined, this is the capability to make sense out of numerous data feeds from a	access protocols to sensitive data as per access rights,	3.9; 3.10; 3.14;	5	short term	

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
		sources, system input, cross-referencing and context-based connections, sensor integration	multitude of sources, both technical as well as human, in order to understand and extrapolate developments. In border security, this is crucial as a preventive means, and helpful in reaction.	data correlation and context-based connections, intel validity checks, research on: improvement of intel source feeds, tracing and tracking /abnormal patterns of goods				
32	3	**Threat Modelling via Social Sciences - understanding push- and pull-factors for illegal immigration, smuggling of people, goods and hazardous materials, early-on warning of potential perpetrators**	in order to effectively protect our borders and societies, the root causes of illegal border crossings within and without Europe, of people and goods, need to be understood. This enables preventive action on the political side (i.e. development aid) as well as areas of distinct focus of interest. It is an early warning system for border security forces within and at the fringes of Europe, who logically should be at the end of the protective chain.	research on: understanding social, economical and political causes of illegal immigration and ways to counter them, flagging of potentially adverse future developments,	3.1; 3.2;	1	mid term and ongoing	
33	4	**Enabling the public**	The European citizen is a decisive and integral active part in any future crisis management solution. Each single individual has its own resilience capabilities which need to be enforced and deployed in a crisis situation.	> public could be best enabled to actively contribute to such solutions, > what the key enablers are, > how public should be educated, trained and prepared to be ready to act accordingly when the moment is there.	> sociological, psycho-social and socio-scientific studies on human behaviour etc. > education and training of public for crisis situations 3.2; 3.3;	1	short to long term *(step-by-step approach)*	small to med
34	4	**Communication with the public and the media**	Public and media have an immense influence on the perception of the performance of the Crisis Management and intervention forces. They may both help and obstruct crisis management activities.	Research should relate to the > understanding and exploiting of new forms of > addressing the media for the benefit of crises containment and overcoming.	> sociological and socio-scientific studies > communications technology > human factors > media sciences 3.3;	1	short term	small

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
35	4	**Operations support (medical and psycho-social)**	Medical and psycho-social support of crisis management operations is vital. Stress and traumata of victims, eye witnesses and the response forces itself have a strong impact on the dimension and magnitude of a crisis, and effective intervention strategies and related support should be developed respectively existing approaches consequently enhanced and best practices shared on European level.	Research should identify > optimum deployment scenarios of medical and psycho-social intervention forces. > Tools and methods of intervention should be improved.	> scenario development and technologies > medical and psycho-social intervention tools and methods > human factors 3.3;	1	short term	med
36	4	**Co-operation**	The growing complexity of crises situations and their response needs counts also for the number of persons, agencies, authorities and organisations involved in dealing with crises.	Research should > investigate and improve the ability of all actors to flexibly cooperate with multiple organisations in order to cope with fast developing and changing crisis situations (multi-dimensional, multi-national, multi-agency, spacious or remote, etc.), > identify and develop cross-cultural needs capabilities (e.g. overcoming language barriers) for crisis managers. Core area is communications technology.	> communications technology > modelling & simulation tools (M&S) > interoperability > sociological and socio-scientific studies > standardisation > system-of-	1	short to mid term	large
37	4	**Strengthening response forces**	Response forces need state-of-the-art technical equipment in the field of sensors, communications and utilities. However, the most promising way to strengthen and enforcing crisis response forces is to bundle and deepen all efforts on European level, in the Member States and by the private sector in the broad area of education, training and exercises.	Research should > focus on appropriate on-site diagnostic and victim identification technology to support first line response teams in dealing with specific crisis, which will assist in rescuing and identifying people as well as providing information to those organisations supporting the first line of response (e.g. information on the status of patients provided to hospitals in advance to help them being prepared). > deliver credentials to victims for identity management. The credentials must have a limited live-time redundant with live-time of the information stored in a victim's database to be used during the crisis it-self.	> diagnostics > ID technology for victims > credentials > standardisation of ID > M&S tools for training and exercises (simulators) > training & exercises for	1	short to mid term	med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
				> provide standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation for a more efficient international cooperation. > address the use of virtual live exercises and other simulation-supported training methods, in particular multi-hazards training simulators, the development of appropriate and sufficient methods and tools for structured ways of lessons learned analysis, exchange and integration into planning and training, and on the education side the development of international degree courses and standards for crisis management leaders aimed at excellence would be recommended.	response forces > lessons learned analysis and exchange 3.2; 3.3;			
38	4	**Situational awareness and decision making**	With the increasing amount of available information coming from more and more sophisticated sensor systems on the one hand and by means of information sharing with other organisations on the other research on crisis management processes and workflows together with human factor issues shall improve the effectiveness and efficiency of the crisis managers.	Research should > focus on new ways of offering information to the user. > The rapidly increasing amount of data available needs accurate compilation depending on processes, workflows and most important the individual needs of the user. Each person develops a very personal model to cope with information overflow. "One size fits all" will not be appropriate for future amounts of data.	> human factors > process and workflow analysis > data integration, fusion, compilation > information interpretation > display technologies	4	short term	small to med
39	4	**Innovative management/ organisational concepts**	The idea of innovative concepts is that the changing security environment with its inherent uncertainties and emerging new challenges for security forces require not only improved strategic planning capabilities, but also continuous reviewing of current crisis management concepts.	Research should support the process of adaptation of these concepts to the new challenges two-fold: > on the one hand, modern management concepts and tools and their possible use for innovating crisis management concepts should be assessed, understood and exploited (e.g. adaptive complexity management), and ultimately a comprehensive, integrative, general conceptual, theoretical framework for adaptive crisis management should be developed. > On the other hand, novel system of systems approaches like the NEC (network enabling capabilities) concept should be analysed for civil security applications and related capabilities should be developed.	> management theory and concepts > systemic analyses > NEC 3.14;	5	short to mid term	small to med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
40	4	**Strategy and tactical simulation**	The need for "intelligent" planning and decision support on strategic and tactical level is noticeable, comprising e.g. behavioural simulations and on flows of goods and persons, simulations during operations to support decision making etc.	Research activities in the security sector dedicated to > M&S-based supporting tools need to be continued having a close look at the emerging technologies in particular on the interoperability issues for M&S tools.	> M&S-based decision support tools > interoperability of M&S tools 3.14;	5	short to mid term	med
41	4	**Strategic planning**	Traditionally, crisis management forces are strongly operations and incident oriented, with little need for long-term, strategy oriented planning. With the growing complexity of crisis management operations the need for a more systematic and long-term oriented planning becomes evident.	Research should support this kind of strategic planning by > developing strategic foresight and risk assessment capabilities, > supporting scenario development and analysis, > providing appropriate monitoring and mapping tools for crisis management capabilities, > contributing to a systematic and coherent capability analysis and development process which could be referred to on European and Member State level. > The development and evaluation of emergency and contingency plans should be improved by exploiting the "Concept Development & Experimentation" approach.	> strategic foresight > strategic risk assessment > scenario development and analysis, > capability mapping and monitoring tools > capability analysis and development tools and methods > CD&E tools and methods 3.6; 3.14;	5	short to mid term	small to med
42	5	**Understanding and modelling complex inter-dependencies**	Security problems typically have complex interdependencies, inducing big risks for unintended consequences. This needs to be considered in decision-making.	Many approaches exist but a lack of consolidation and knowledge accumulation leads to a tendency of reinventing the wheel. There is need for systematic evaluation of approaches leading to consolidation of	> systematic evaluation of alternative approaches to	5	short term	med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small25€; med 10-25€; large 30-40€)
				A key aspect is the methods' ability to support effective interfacing with decisionmakers and experts.	modelling complexity and interdependencies > interfacing with decision makers and experts >ability to support novel insights (e.g. on unforseen consequences) 3.14;			
43	5	**Systematic risk monitoring and assessment method**	Limited ability to recognise "weak signals", either with respect to emerging risks or with respect to possible solutions/technologies. Limited ability to identify early on potential areas of conflict and problems, as well as for dealing with them on the public agenda	By improving monitoring and early warning of potential security problems and solutions ("technology watch"). Development of multilingual semantic analysis systems. Improving the robustness of methods and tools for risk monitoring and assessment. Improving the understanding of the use of intelligence in the operation of security solutions.	> monitoring and early warning > comprehensive, inter-dependent and multi-dimensional risk assessment > using intelligence in security operations > multilingual semantic analysis systems 3.6;	2	short term	large
44	5	**Prioritising security investments**	Security analysis require the simultaneous application of all the 'current capabilities' (i.e. tools for projecting both i) potential uncertainty related to alternative futures and ii)	case oriented empirical research on decision-making in the face of insecurity Development of architecture (methods and approaches) for prioritising security investments;	> methods and capabilities for prioritising security	5	short term	med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
			current insecurities likely to prevail in the future, to the present day investment decisions).	new key capabilities bridging extant ones; human factors/user interface issues;	investments > decision-making in the face of insecurity > human factors/user interface issues 3.14;			
45	5	**Handling high-quality societal foresight debate on security**	Lack of ability to deal with future deep uncertainty; need for translating strategic insights/concepts into R&D or investment priorities. No mature security specific communities available; short term focus of policymakers. Lack of common vision of future threats to security interests; lack of understanding.	1) Foster shared understanding of long-term security issues in European policy communities (content), 2) A shared conceptual framework for security policy writ large among European decision-making and decision-supporting communities. Embed sound foresight and risk assessment practices in decisionmaking. 3)Develop strategies for sound foresight and risk assessment practices to affect public perceptions of insecurity: processes (process), 4) Improve understanding the interdependencies between the internal and the external dimensions of security and defence issues	> embedding foresight in decision-making on security policies > comparative studies on national and sectoral foresight communities; NoE:s, > holistic approach to security 3.6;	2	short term	small
46	5	**Enhancing creative capabilities in foresight**	Potential of ICT not yet exploited, e.g. virtual reality tools, etc. More sophisticated methodologies are needed to explore future worlds in a systematic manner.	Advancement of scenario methodology as an essential tool for enabling and organising creativity. Development of cooperative ICT tools to facilitate deliberation and creative collaboration within distributed teams. Development of creativity-enhancing tools	> scenario methods > ict tools for creative collaboration > creativity enhancing toolsfor foresight 3.6;	2	short term	med
47	5	**Understanding human behaviour (individual and group) in the context of security**	The impacts of interventions in interdependent sets of root causes can be captured at a very abstract and general level only. Major threats associated with emerging	Development of an operational concept of social resilience. Improve understanding on ways of affecting 'root causes' of insecurity (e.g. violent radicalisation).	> human and societal resilience (citizens' ability	1	short term	large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
			technologies reside in the – often unexpected - use that can be made of them.	Investigate malevolent uses of emerging technologies from an inter-disciplinary perspective Understand Human-System Integration aspects of the operation of security solutions.	to cope with insecurities and crises) > malevolent use of emerging technology > human- system integration > root causes of insecurity 3.1;			
48	6	**CBRN integral threat assessment: Surveillance tools for detection of offensive capacity with emphasis on emerging technologies with dual-use potential; analyzing actor intention; Intelligent agent data-base and sharing capabilities with high level of standardization using validated accepted data; Systematic identification of vulnerable targets**	Before prevention or preparation strategies can be applied, a complete and accurate assessment of the CBRN threat is required. Continuous assessments and foresight then helps to ascertain the efficacy of prevention strategies and future investments. An accurate CBRN threat assessment is also important to first responders and other crisis management personnel for setting planning and training agenda and can help prioritize research in this critical security area as well.	Map, through multidiscipline approaches, relevant potential pathways to CBRN terrorism (including radicalisation mechanisms in a CBRN context) and their unique and specific signatures, sensitive to group dynamics and technological abilities Through cautious awareness raising-dialogue gain support from civil society, law enforcement, academia etc to detect anomalies Meta-analysis of the complex threat dilemma and development of new, non-frequentist and non-deterministic analysis methods Methodology to derive the probability of successful incidents. Input is from actor profiles, actor capabilities, consequence prediction, probabilitics Intelligent database development and analysis; Objective/quantitative algorithms Modelling capabilities for attack simulation and intervention planning (in/out-door; urban, sub-urban, rural, industrial, infrastructure	3.1; 3.5; 3.11; 3.14	2	short term	med
49	6	**Prevention of CBRN incidents by effective multinational counterproliferative organisational measures: Increased CBRN-security of infrastructure (including knowledge, material, and equipment) involving industry, academia, research institutes, and governmental**	The best defense against CBRN terrorist threats, next to eliminating the cause, is to prevent extremists from having the availability of CBRN sources and knowledge. International legally-binding treaties and agreements on control of export of sensitive technologies, materials and knowledge, along with nationally implemented non-proliferation measures can reduce the threat of CBRN by various ways.	Ability to prioritize and perform technical assessment within (inter)national networks Better and more flexible coverage of emerging threats in CBRN-related treaties; better defining general purpose criteria, systems, and having more possibilities and mandates for monitoring Creating dual-use awareness Design of toolbox for monitoring and verification of implementation of (new) CBRN treaties Develop alternatives to replace radioactive sources by non-radioactive means	3.2; 3.5; 3.6; 3.7;	2	short to long term	med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small25€; med 10-25€; large 30-40€)
		agencies; Global awareness of dual-use potential; Tools for facilitating implementation and global adherence to CBRN regulations and international conventions		Develop solutions for safe disposal of radioactive sources Development of deterring and norm-enforcing tools and methodologies against use of agents as violent means Down-blending surplus HEU to LEU safely and economically Safe, quick, and secure process to dismantle obsolete nuclear facilities				
50	6	**Prevention of CBRN incidents by effective counter-measures and limitation of terrorist capabilities: Scanning of cargo; Border control of goods; Interdiction capabilities; Strengthening international cooperation to combat illicit trafficking and terrorist use of CBRN material; Dissemination of information between national authorities, regional and international organizations to assure measures in combating criminals and an efficient use of the resources**	Terrorist threats can be reduced by preventing extremists from either entering Europe or illicitly transporting materials, components, and devices across our borders. A crucial mission is to control the borders by interdicting threats before they arrive in EU nations. Unlawful export of technologies and expertise that may be used by our adversaries to expedite the development of CBRN and related capabilities must be prevented. Within EU borders unlawful access to materials and attempts to acquire, transport and use these materials must also be prevented.	Bulk detection of chemical, biological and radiological materials Development of (dynamic and secure) information sharing systems regarding trade and transport of CBRN-materials Fast and reliable detectors to monitor large volume containers for CBRN materials and precursors with negligible false alarms Tracking and tracing of goods including hazardous materials, CBRN precursors, and production equipment Research of totally new methods for the signature of covert production facilities by emission, shape and defining new measurable properties	3.1; 3.2; 3.3; 3.5; 3.9; 3.10;	2	short to mid term	large
51	6	**Early warning, monitoring, and surveillance in preparation for or as an immediate response to CBRN incidents: On-site or remote automated and reliable surveillance and detection for the security of the public Completely networked warning and situational awareness system that can be**	Protection against attacks of high-consequence buildings, events and critical infrastructure by enhancing domestic preparedness and information sharing. Timely sharing of threat information within the intelligence and crisis management communities is essential to protect people and critical assets against CBRN attacks or related high-consequence events. Tailored intelligence and coordinated outreach at multiple levels is required to enable threat-informed and risk-based decision making. Enhanced situational awareness of CBRN and	Detection of toxicity and virulence requiring innovative databases for the prediction of toxicity and virulence by molecular and submolecular properties Detection technology for novel type agents (e.g. bioregulators, peptides, non-lethal weapons, non-traditional agents); Harmonization of testing and validation procedures for new detection instruments International harmonisation of threshold values for application of measures; Passive or active detection/imaging technology for the detection of chemical hazards; R&D towards real-time detection of suspicious aerosols.	3.2; 3.3; 3.5; 3.6;	2	short to long term	large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
		used seamlessly by first responders, decision makers, and everyone working in possible CBRN scenarios from all nations Improved global disease surveillance systems including awareness of rare diseases	[illegible] related threats is vital for prioritizing resources, developing response plans, reducing vulnerabilities, and mitigating consequences.	Stand-off / early warning detection technology including orbit based surveillance means Technology for equipment with dose-rate meters for early detection of radioactivity Technology to mark radioactive sources with a fingerprint Develop non-invasive methods for pre-symptomatic detection of disease (alert state dependent)				
52	6	**Response to CBRN crisis; identification and investigation: Standardized tests and equipment for testing CBRN threats with the goal of quickly ruling out at least 90% of hoaxes**	It is crucial for the crisis management system to identify the real nature of the incident as reliably and as quickly as possible.	Development of methods and procedures for forensic sampling, analysis for unknowns. Extended strain collections; representing world-wide geographic origin. Genome sequencing with immediate comparison with extensive sequence databases. Micro-systems technology for miniaturisation CBRN laboratory capability, transportable;	3.3; 3.5; 3.13;	2	short to mid term	med
53	6	**Physical protection against CBRN hazards: Protection of response teams against CBRN exposure with minimal physiological burden and minimal interference with operational tasking; Physical and mental verification of protective capability under realistic conditions**	Responders need personal protective gear that protect against CBRN agents but do not cause extreme hindrance to mission. Collective Protection (COLPRO) in areas where CBRN events occur are necessary to keep clean areas available for medical units, mission control, logistics, etc.	Development of multi-purpose, standardized body protections that are operational over longer times with increased mobility, communication, and tactile capability Personal protective gear with integrated communications systems and other protective measure, e.g. ballistic protection Personal dosimetry systems that could be quickly and easily integrated with personal protective gear Improved COLPRO systems Escape hoods for short-term airways protection of citizens	3.1; 3.3; 3.5; 3.11;	2	short term	med
54	6	**Response to CBRN and related events by enhancing initial incident management: All hazards approach; standard protocols and training programs; presymptomatic clinical diagnostics operable under field conditions; failsafe [illegible]**	The response system involves improved situational awareness, search & rescue of victims, all integrated with scenario-based decision-support tools. Channels of communication among intelligence analysts, CBRN protection experts, and first responders must be established in advance to provide timely and accurate assessments of events.	Design of a system for search and rescue, triage and transport of contaminated victims and tracing and tracking of evacuees and patients (mass casualties and large scale evacuations) Fieldable R/N biodosimetry (or fast post-accident dosimetry) and chemical/biological point of care diagnosis Crisis management tools including robust communication systems that can withstand any CBRN incident	3.3; 3.5; 3.11; 3.13; 3.14	2	short to mid term	med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
		procedures for identification and rescue of victims and containment of contamination		Development of standard protocol for triage, decontamination and training programs for mass CBRN incidents Development of operating procedures focusing on the particulars of CBRN threat agents in addition to ordinary chemical, biological, radiological poisoning (all hazards approach) taking adequate measures to keep a forensic approach and not destroy evidence during actions				
55	6	**Mitigation: broad-spectrum treatment of CBRN hazards: Antidotes against broad spectrum of threat agents; specific treatment where necessary;**	The CBRN area has to deal with agents and diseases that are not always covered by regular drug development, this gives rise to a need for additional efforts.	Development and stockpiling of more effective vaccines, antitoxins and chemotherapeutics with longer shelf lives and safer profiles Antidote activities on: stabilization, appropriate coating material and fillers, microencapsulation and improved logistic systems Basic research designed to measure sensitive markers of nerve agent exposure to assure that low-level exposures are not associated with long-term or delayed health effects Specific know-how and capacity for rare situations, such as treatment of patients with severe radiation injuries	3.1; 3.2; 3.5;	2	short to long term	large
56	6	**Capability to decontaminate targeted items and areas attacked: Standard decontamination procedures need to be established along with measurable criteria that ensure health and safety of potential inhabitants.**	To completely neutralize the effects of all CBRN agents without causing serious damage to items being decontaminated and to allow rehabitation of contaminated buildings and land as quickly as possible	Automated/robotic decontamination equipment Creation of and training for dedicated decontamination teams Determinination of safe contamination levels Development of decontamination products to increase potency against all CBRN threats and reduce hazards; that are environmentally safe, reduce resource requirements, and are nonhazardous to sensitive equipment and electronics Self-decontaminating materials and coatings Standardized procedures	3.3; 3.5;	2	short to mid term	med
57	6	**Psychological and social resilience to CBRN incidents: Management of the psychological impact of CBRN incidents; Understanding of underlying mechanisms Identification of stakeholders**	To enhance recovery from CBRN incidents and hoaxes. Large numbers of persons who feel like they have or might have been contaminated will ask for medical help. Well-informed, educated people who have confidence in decision makers during times of crisis are more likely to react proportionally to	Develop realistic training procedures and facilities for responders Development of CBRN incident serious gaming products onto real-world scenarios to establish awareness; to identify critical elements; to verify research needs Generate understanding of public communication and education	3.1; 3.2; 3.5;	2	short term	med

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
		Identification of stakeholders **Emergency psychological support** **Media is a key player; the public a responder**	crisis are more likely to react proportionally to CBRN incidents and hoaxes. While emergency responders are trained for and accustomed to facing stressful situations, the public and other services involved in the response are not	Investigate psychological mechanisms to understand (mass) response to extreme incidents, also related to other kinds of incidents and accidents Investigation of effective means to communicate with the public, e.g. in a crisis situation				
55	7	**Automatic analysis capabilities adaptive to dynamic situations.** **Global Tracking of naval and cross-border traffic**	In multi-agency environment often non-interoperable systems are used to gather and archive data and meta-data. Information retrieval including forensic search is currently cumbersome, time consuming and often not coherently feasible. Adequate mechanisms for controlled data access need to be devised	Research should focus on Data Fusion - Automatic network reconfiguration	3.3; 3.9; 3.12; 3.14	4	short term	small
56	7	**Sharing of sensors and sensor data (meta data)**	Interworking between public and private security installations is commonly performed on an alarm basis in a preconfigured manner, e.g. permanent connection of alarms to a security operation centre (SOC).	Research should focus on Vulnerability modeling and analysis	3.3; 3.9; 3.12; 3.14	4	mid term	small to med
57	7	**Establishment of a Critical Infrastructure Warning Information Network**	Robust and secured sensor network within an infrastructure and for remote control and monitoring. Automatic authentication of people accessing terminals and networks and monitoring of network traffic. Permanent communications infrastructures in crisis phases need > Intelligent and proactive intrusion detection systems (IDS) on critical network infrastructure in place. > Use of multimodal biometric identification in critical infrastructure. > Overall strategy at European level for tackling cyber-warfare	Research should focus on: > Standardised adaptive systems for different radio > NEC concepts. > Broadband satellite communications infrastructure. > Satellite based observation systems and telecommunication infrastructure. > Space Situational Awarennes and Signal Intelligence	3.3; 3.7; 3.9; 3.11; 3.12; 3.14	3	short to mid term	large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
58	7	**Detection, localization and identification of difficult targets in complex environment**	Improvements needed must be focussed on the increased sensitivity, improved clutter rejection and enhanced jamming suppression, including the comprehensive development of generic technologies (system concepts and architectures, signal and data processing, platforms and integration, control and operation, design and production) and main hardware components (transmitters, receivers, antennas, amplifiers, filters, converters etc.) as well.	Research should focus on Technologies for both radars and EW (electronic warfare) systems.	3.10; 3.12;	2	mid term	small to med
59	7	**Adaptive, self-learning and anticipative technologies for dynamically changing operational situations and various environmental conditions**	The operating environment for RF sensors is becoming more and more difficult due to dense ElectroMagnetic (EM) spectrum, efficient Electronic Counter Measures (ECM), sophisticated repeater jammers e.g. with Digital Radio Frequency Memory (DRFM), complex operational environment (inhomogeneous natural terrain, urban terrain, operation in brown water etc.);	Research should focus on: > software reconfigurable sensors, > dynamic frequency management, > co-existence and effective interference suppression of RF systems, > adaptive beam forming, > wideband antennas, > waveform generators, > power amplifiers, > wideband high dynamic range receivers, > adaptive sensor management, > prediction of target behaviour and intent.	3.7; 3.10; 3.11; 3.12;	5	short to mid term	med
60	7-comms	**mobile ad-hoc networks in urban and metropolitan areas to be deployed in emergency phase. Optimized communication capabilities to available resources (bandwidth, frequencies) in emergency mode**	1. quick recovery of communication capability with reasonable data rate and networking capabilities 2. improve communications in congested emergency environment	1. Mobile Broadband Wireless Access (MBWA) to route and/or relay packets (e.g., IP packets) between the external networks and the mobile terminals or between the mobile terminals 2. Advanced software radio reconfigurable functionalities including "cognitive capabilities radio"	3.1; 3.2; 3.3; 3.11; 3.12;	5	short to mid term	small
61	7-space	**Satellite Communications System fully integrated with the Global Communications Network, next generation terrestrial network and Networ Centric communication capability**	global worldwide coverage broadband communications supportig IP-network centric services and full interoperability with IPvX standard and terrestrial IP based network with high data throughput satellite channels	IP based, high-capacity microwave and optical network in space, made of advanced next generation satellites with very high data rate telecommunication connections, including inter-satellite links.and including new generation LEO Satellite constellations. Bandwidth/power efficient IPv4/IPv6 satellite on board/ground modems with open standard interfaces.	3.11; 3.12;	5	short term	med to large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
62	7-space	**Satellite comms in System-of-system capability**	**Improve disaster management relief actions through the deployment of global, robust communication systems** Collaborative satellite, including data relay systems, operation has the potential to increase the performances of the overall Communication networks	Satellite Constellations and Formation Flying (FF) in the Networked Environment	3.11; 3.12;	5	mid to long term	large
63	7-space	**Space Surveillance in System-of-system capability**	Collaborative satellite and satellite constellations/formations (micro/nano sat) operation has the potential to increase the effective performance of individual sensors and to improve the system response time.	Synthetic aperture radar (SAR) systems to the features of image acquisition in all time, all weather conditions and a size of the spatial resolution cell is independent of the distance between target-sensor and of the wavelength for ideal processing. These requests are on one hand the sufficient for detection, recognition and identification, and on the other hand for a broad spectrum of applications, e.g. worldwide reconnaissance, surveillance, catastrophe monitoring, border control, etc.	3.10; 3.11; 3.12;	5	mid to long term	med
64	7-space	**Reconnaissance and identification for surveillance, using satellite asset**	exploitation of natural data and reconnaissance of non natural assets based on natural signatures.	Space Based Multi- and Hyperspectral Sensors Technology and Applications	3.10; 3.11; 3.12;	5	mid term	small to med
65	7-space	**early warning space systems**	Advanced space surveillance capabilities (MTI, …)	early warning and ELINT satellite solution (GEO satelllites with very large deployable reflectors, mini/micro sat constellations, nanosat disposable constellations)	3.11; 3.12;	5	long term	med to large
66	7-space	**3D Urban mapping by satellite**	disaster relief operations are often conducted in urban areas where effective operations require rather accurate updated 3D maps in reasonable short time	digital elevation models SAR and optical observation systems	3.2; 3.11; 3.12	5	short to mid term	small
67	7-space	**Decision support system by Geospatial Information Systems**	Provide data, technology and procedures allowing the exploitation of geospatial information to produce proper information needed in supporting its decisions	integrate data produced by a number of high performing (resolution, number of observations,…) space sensors, Exploiting of added value services based on Galileo high speed satcom infrastructure to make available the information quick as needed by the dynamic scenario and in an full interoperable way; Space based Positioning, Navigation and Timing and high accuracy spatial date GIS.	3.11; 3.12; 3.14	5	short to mid term	medium
68	7-space	**Space Situational Awareness**	Comprehensive understanding and	Ground radar and telescope infrastructure,	3.11; 3.12; 3.14	5	long term	large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
			knowledge of the population of space objects and debries, the space environment and existing threats/risks.	space weather, survey/tracking and space-imaging solutions through in-orbit demonstration via dedicated missions		5		
69	7-space	**Space environment and Space Weather**	The exposure of space components to the harsh conditions of space environment is a major concern for their performances and reliability	The study and prediction of space weather by integration of data resulting from multiple satellites, detectors and forecasting systems is a key element in this respect.	3.11; 3.12;	5	long term	med
70	8	**Improved performances of biometric technologies applied to identity management**	Biometric technology can provide a very solid basis to manage people's identity. To get the full benefit of this technology, several topics must be improved: - accuracy (very low false acceptance and false reject rates); - robustness to spoofing attacks; - speed (fast processing of EAC data on travel documents); - quality and ease of use of biometric acquisition mechanisms, in particular for enrolment processing	• Development of secure biometric acquisition systems. • Improved accuracy (FAR, FRR) of basic modalities. • Efficient methods/tools for fusion of modalities. • Robustness to spoofing attacks (liveless/ motion detection,..). • Fast equipment to process ID control from documents (including EAC data processing). • Improved biometric acquisition device and procedures. • Development of new and innovative biometric sensors able to operate in the critical conditions that are typically found in a disaster scenes. • Evaluation of performance and robustness of counter-measures related to internal and external attacks and, if required, to profiling. • User behaviour and postural recognition, promoting "person identification" beyond biometric traits and avoiding identity theft. • Acquisition devices and systems certification. • Create biometric model specific for a usage. • Investigate multi-biometric traits application benefits and increased performances.	§ 3.1, 3.3, 3.9, 3.10 & 4.2.4 part 1 ; § 4.1.2. part 2 (WG8) final report	4	short to mid term	med
71	8	**Mobile Identity Devices**	A growing number of situations require the capability to control identity on the field, such as border control, police controls, or for the management of victims after a catastrophic event. New generations of mobile devices are needed for this purpose.	• Define common procedures for ID check with mobile devices, including interoperability requirements. • Develop new generation of mobile equipment: privacy by design, multi-modalities, accurate, fast, highly secured, easy of use.	§ 3.9 part 1 ; § 4.2.2 part 2 (WG8) final report	4	short term	med
72	8	**Protection against Identity Theft and frauds in both physical and virtual worlds**	Identity theft is a major current problem in the world, impacting millions of people and undermining global and financial security. No coherent approach to address this threat is currently in place. It requires a concerted effort	• Harmonize national legislation between all European Member States for all applications where eID is mandatory (travel, e-Services, Driving license, eHealth, ...). • Development of agreed processes and standards.	§ 3.10, 4.2.4 part 1 ; § 4.2.1 part 2 (WG8) final report	4	short term	large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
			involving significant advances in processes and technology.	• Use of strong authentication processes and technologies. • Development of secure enrolment processes and technologies. • Solid solutions to secure on line transactions (secure payment on Internet based on eID and banking smart cards). • Education and training for all stakeholders on threats and preventive measures. • Harmonize security level of all identity documents (security evaluation common criteria and security target).				
73	8	**Identification of victims during Disasters and Emergency Management**	In case of disaster, it is critical to identify, as soon as possible the identity of the victims (including survivors). In case of major disasters, experience (2004 tsunami, Katrina..) has shown that more solid and efficient solutions are needed for the management and tracking of the survivors. Solid identifications solutions, adapted to the specific context must be developed.	• Software mechanisms to build up an identity service based on heterogeneous information (biographic and biometrics). • Develop identity management production that can deliver credentials to victims. • Standardisation of rescuer identity, skills and credential to allow interoperable command and control cooperation. • Electronic wall-mechanism to supervise disasters border zone to manage access rights and to protect victims from unauthorised reportage. • Build robust, portable and autonomous tools to digitally collect on site victims' information.	§ 3.3 & 4.2.4 part 1 ; § 4.2.4 part 2 (WG8) final report	1	short to mid term	small
74	8	**Improved Asset Tracking**	A huge volume of merchandises/assets is transported all over the world, mainly through cargos. Controlling the content and guaranteeing the security of these assets is a critical challenge. New solutions and technologies are needed to address it.	• Innovative tracking devices (e.g. RFID based systems) for assets, containers and related seals. • Intelligent sensing solutions using state of the art technologies (including GNSS) allowing continuous monitoring and tracking of the load unit and its content. • Automatic identification of containers and vehicles. • Integration of OCR systems for the localization and recognition of the standard ISO-codes of containers and for the identification of trucks licence plates and railways wagons codes. • Detection and tracking of hazardous materials. • Portals for logistics monitoring and management, fully interoperable and interconnected supporting standardised software and hardware communication interfaces and information flow.	§ 3.7.1, 3.7.3 & 4.1.4 part 1 ; § 4.2.6 part 2 (WG8) final report	4	short term	med to large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
				• Need of a single system governing all the international movements of assets.				
75	8	**Harmonised privacy protection for identity management**	Security solutions that are put in place must provide an efficient protection of the privacy of the individuals. The Data Protection Directive provides a common framework for the EU-27. MS have to take proper actions correspondingly. Specific technological solutions, such as PET, have to be developed.	• Development of Privacy Enhancing Technologies (PET) solutions. • Biometric solutions to effectively improve the privacy of individuals. • Mechanisms allowing revocation of biometric information.	§ 3.1, 3.10, 4.1.1, 4.2.4 & reco. 5 part 1 ; § 3.3.3 & 4.2.1.part 2 (WG8) final report	4	short to mid term	small
76	8	**Harmonised global border control**	Lack of Change Management and planning. Failure to plan and build efficiency into systems such that individuals can be fast tracked will result in major user satisfaction and management issues. Lack of business models to manage costs of new security systems. Lack of system interoperability. Hence new systems are limited and will ultimately not be fit for the sophisticated purposes for which they are required. Standards – failure to agree and put in place all required standards continues to hold up our ability to exploit and maximise our use of available and new technologies. Also it hinders innovation and R&D as developers still do not have roadmaps for all requirements as yet.	• Automated border control to leverage the increasing number of electronic travel documents and to manage the associated technical and legal complexity. • Move the border controls from reactive to proactive through a connection to a secure information system (through companies operating flights or through a special secure connection); passengers checked by authorities during the flight; only those who need a more detailed control at the border will be actually and physically checked • Need to manage the threat posed by the regulated workers and populations such as the police, the x-ray screeners in airports. • Develop standards required to ensure true interoperability of secure documents and systems. • Architecture - Require architectural support and clear interface specification including data formatting and security for the new systems and use central infrastructures for multiple applications –removing redundant and/or isolated "stovepipe" systems • Support best of breed technologies, • Efficiency versus accuracy trade-off	§ 2.3, 2.4, 3.9, 4.1.3 & 4.2.3 part 1 ; § 4.2.5. part2 (WG8) final report	4	short to mid term	med to large

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
77	8	**Intelligent-led border management**	The growing need for high security controls at border crossing has a negative impact on the management of the flow of travellers (lengthy waiting time). Solutions are needed for easier and faster processing. A fast and automatic border control process should be put in place for the majority of travellers, and better tools should be developed for support non automatic procedures.	•Develop a new global scheme which integrates 3 levels of controls: - At origin/in transit: collect details of traveller's data and send them to destination country - At border of destination country: light and fast control, focused on limited number of people at entry; fast recording of travellers at their exit (Entry/Exit scheme) - Within the destination country: capability to perform checks anywhere in the country (mobile devices) • Develop standards for interoperability of secured ID documents and equipments. • Harmonize procedures/rules for determination of applicability of automatic control to travellers (fully exploit PNR/API/ESTA data).	§ 2.4, 3.9, 3.13, 4.1.3 & 4.2.3 part 1 ; § 4.2.3.part 2 (WG8) final report	4	short term	med
78	8	**A common Certificate Policy for EAC checks and controls**	There is a lack of trust and sufficient interoperability between the Country Verifying Certification Authorities (CVCAs) and Document Verifiers (DVs) of different Member States for the EAC-PKI to operate	• Build a common structure on the example of the Schengen Information System, which should be operated and run by one or two voluntary Member States (one principal site, and one rescue site). • Define precisely a common rule of creation, distribution, update, exchange and revocation of certificates between the EU Member States of Schengen. • Define rules of governance of the system.	§ 2.6, 3.9, 4.1.3, 4.1.5 & 4.2.4 part 1 ; § 4.2.7. part2 (WG8) final report	4	short term	small to med
79	9	**Standards development**	The European security market is highly fragmented, favouring the development of multiple and incompatible solutions. A solid standardisation effort at European level would help promote the development of innovative solutions addressing the overall market, and would strengthen the European industry.	Analysis of the standardisation needs in the various segments of the security market. Analysis of the conditions allowing the definition and implementation of a European Security Label. Analysis of the economical impact. Promotion of dynamic standardisation.	3.8; 3.10; 3.11; 3.12;	3	short term	small
80	9	**European Security Technological and Industrial Base (STIB)**	Developing security solutions requires a good knowledge of the capabilities of the European stakeholders in the security domain (industry, research laboratories). It is necessary to identify and understand the competencies of all these stakeholders.	Develop or refine the mapping of security stakeholders in all EU-27 Members States. Identify their capabilities, strengths and weaknesses.	3.8;	N/A	short, mid and long term	small

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2-5€; med 10-25€; large 30-40€)
81	9	**European technology platform**	To allow for the development of coherent and large scale security solution in Europe, a powerful tool, such as the JTI, put in place in the FP7, should be used for the security domain.	Put in place a JTI program for a large scale security programme.	3.7; 3.8; 3.11;	N/A	mid term	the JTI must be more focused, means related to sub-themes within security; the necessary budget may be in the order of 300 Mio EURO per sub-theme
82	9	**Education and training**	An efficient implementation and use of security solutions requires a large education and training effort for end users, but also for other stakeholders directly concerned: the public, decision makers, regulators and the media	Develop specific programmes to educate the public on security issues and available solutions. Associate the decision makers , regulators and media to these programmes. Use scenarios to develop training exercises	3.1; 3.2; 3.4; 3.5; 3.7; 3.8;	1	short, mid and long term	small
83	9	**Pre-commercial procurements**	Mature security solutions are not yet widely available. Some specific actions are neeeded to help defining or refining the requirements of new solutions, and to validate their technical, operational, and societal aspects.	Launch pre-commercial procurements for some specific security domains.	3.8; 3.11;	N/A	mid term	as a genarl rule of thumb one should keep in mind that R&D are about 10% of the whole innovation chain; therefore pre-commercial procurement must identify the ownership for the missing 90%, in oyher words, the estimation should assume a factor of 9 to the R&D investment

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small25€; med 10-25€; large 30-40€)
84	10	**Compatibility of security capabilities among MS**	Members States employ different approaches for the management of the Security Research Plans ranging from the establishment of dedicated National Authorities to the extension of the role of existing structures. The variety of implementation approaches represents an issue for ESRIF,	Before implementing an R&T plan it is necessary to develop an R&T strategy based on:1) needs defined by the public and private end users in that case of "policy driven" research 2) a shared global vision 3) capabilities priorities.This can be done by a work to define and prioritize "capabilities" in a capability development plan. The aims of such a work are :A) to make the global vision more specific and thus more useful;B) to identify priorities for capability development; C) to bring out opportunities to pool and cooperate.The CDP can (and should) be used as an important tool to guide R&T investments, but the CDP is not a work addressing only R&T: I) the CDP focuses on needs for capability improvement in security task terms, and not in technologies or R&T tasks II)the CDP does not focus exclusively on equipments or R&T: the outputs can be global technological needs for a better efficiency but also a better organization, a better use of existing resources etc.Not everything that is proposed by the CDP necessarily has an R&T component.	3.2; 3.3; 3.7.2; 3.7.3; 3.11; 3.12;	N/A	short term and ongoing	
				At the end the capability development plan must be get a political approval at the right level. For us the designated lisbon treaty High Rep / EC Vice Pdt is the good person for an approval. The capability development plan must be a continuous task to implement each year, due to the evolution of threats, of technologies etc. After a starting work, for one or 2 years, creating an initial CDP, an annual upgrading has to be done. We have to define a permanent network / structure with 2 geometries: one for the initial work, another to annually upgrade the CDP…Due to its importance (in particular the definition of R&T priorities), this capability development plan can be prepared by an "Independent adequate Structure" populated by experts from MS, Agencies/Institutions dealing with operational issues, through a constructive dialog between that structure and the "research world" (public laboratories and industry)				

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small2 5€; med 10-25€; large 30-40€)
,	10	**Multilateral cooperation in international organisations and through partnerships with key actors**	The existing relationship between NATO and the EU needs to be improved, making them ever more integrated, reducing duplication .	The challenge for both the EU and NATO is to make use of the same national pool of resources (both personnel and capabilities).creating permanent joint structures of co-operation, while respecting the independent nature of both organisation	3.2; 3.3; 3.7.2; 3.7.3; 3.11; 3.12;	N/A	short term and ongoing	
86	10	**Standardisation and Certification within a European reference system, co-ordinated by the EU and implemented through national bodies**	The existence of a multitude of protection levels and standards across EU Member States increases costs for businesses, which have to incur redundant security investments depending on the jurisdictions under which they operate.The EU must define a security standard notably for strategic infrastructures.	The "Stable Structure" should be in charge of the development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability and/or commonality that are necessary to attain the required level of interoperability	3.7; 3.10; 3.11; 3.12;	N/A	short to mid term	
87	10	**Extensive use of interoperability between security and defence (achieved through the "securitisation of the military markets" rather than the "militarisation of the security**	Technologies are increasingly of a dual-use nature for military and civilian operators	The European Framework Cooperation for Security and Defence has the purpose to systematically ensure complementarity and synergy of Defence R&T investment by the Agency with research investment of the European Commission under the Seventh Framework Programme for civilian security	3.4; 3.5; 3.6; 3.9; 3.11; 3.12; 3.14;	N/A	short to mid term	
88	11	**Good governance, referring to the well-ordered flow of information, authority and public resources.**	Good governance enhances trust in democratic institutions and supports their good functioning, and provides for good societal security.	Good governance can be strengthened on the European level by increasing accountability, and seeking new ways to instill it as a norm. As the nature of European governance changes, research should continue to innovate and support experimentatio in models of power-sharing, coordination and interaction.	3.1; 3.2; 3.3; 3.7;	1	long term	
89	11	**Mediatization, referring to the autonomy of public events in media representations.**	It moments of crisis media cultivate perceptions that are not in correspondence with the actual situation, thus making proportionate poltiical action and trust difficult.	Research on the cooperation between public authorities an commercial media outlets is necessary, in order to integrate public concerns. Information and training are necessary in order to support journalists in adapting to a quickly changing information world. Questions of media and demcracy require new interpretations.	3.1; 3.2; 3.3;	1		
90	11	**Violent radicalisation understanding and counterstrategies**	Violent movements of all kinds are determental to the well-being of society and citizens.	Research is needed on the mechanisms of radicalisation. Counter-radicalisations efforts can be made through education, community-based approaches and the development of counter-narratives.	3.1; 3.2; 3.3; 3.7; 3.13;	1	short to mid term	

running No.	From WG	What?	Why?	How?	Key link elements	Cluster	Timeline (short-mid-long-term)	Weight / Cost Estimate (small25€; med 10-25€; large 30-40€)
91	11	**Economics of security aiming to understand the rationale and behaviour of actors involved in both purveying and countering threats to Europe.**	Interests of European citizens and of those who might do them harm is often directly correlated with economic issues. Understanding the one can often serve to understanding the other	A critical mass of reaserch and policy advice cpacity in Europen should be created. Research on the economics of terrorism, micro-economics of fear of terrorism and economics of the impact of catastrophes should be organized.	3.2; 3.3; 3.7; 3.7.1;	1	mid term	
92	11	**Data protection, linking society's need for information about individual citizens and the needs and rights to privacy and dignity.**	An open society is a necessity for a secure society. New security technologies risk putting aside the dignity of humans in the name of the security of society.	A baseline for privacy should be establish and monitored. This should be enhanced by an updating and revision of privacy and data protection law. In addition, privacy issues need to be built into innovatin processes.	3.1; 3.10; 3.11; 3.13;	1	short to mid term	
93	11	**Ethics and trust, referring to the willingness of European citizens to put their lives and well-being into the hands of others.**	The well-functioning of technologically based solutions depends on trusts of systems, trust of systems operators and trust in authorities who deploy them.	Trust in authorities, systems, and other citizens must be built through education, training and other forms of long-term trust-building interactions. New forms of communication between public authorities and citizens should be developed and promoted.	3.1; 3.7; 3.7.2; 3.10; 3.11; 3.13;	1	long term	
94	11	**Inter-organizational coordination refers to the capacity to achieve coherent solutions in crisis**	Failure of coordination is a prevalent cause of loss of life, property and legitimacy in crises.	Research is needed on the dynamics behind inter-organizational coordination and on the obstacles to coherent joint action by members of the distinct professions responsible for aspects of societal security	3.1; 3.2; 3.3;	1	mid term	
95	11	**Instant and citizen generated news as driven by new communications technology**	The loss of control over time, space and imagery may erode the capacity for societal resilience	Research is needed on the impact of novel and widely dispersed communication technologies for effective prevention, warning, response and recovery from trans-boundary crises.	3.1; 3.2; 3.11; 3.12;	1	short to mid term	

ANNEX III

List of ESRIF Members (November 2009)

ACCARDO Lucio (Italy)	Ministero della Difesa/Segretariato Generale della Difesa e DANN. Capo V Rep. Ricerca Tecnologica SGD/DANN
AMINOT Jean-Luc (France)	ANTS
BERG Frank Robert (Norway)	The Financial Supervisory Authority of Norway (Kredittilsynet)
BERGLUND Erik (EU)	FRONTEX – Capacity Building Division
CAMELI Antonio (Italy)	Ministero Degli Interni - Polizia di Stato
CENAS Narimantas (Lithuania)	Institute for Biochemistry, Dept. Of Biochemistry of Xenobiotics
DE MESMAEKER Yvan (Belgium)	ECSA European Corporate Security Association
DELVILLE Thierry (France)	Direction de l'administration de la police nationale
DESIMPELAERE Luc (Belgium)	Barco Corporate Research
DOBROWOLSKI Grzegorz (Poland)	AGH University of Science and Technology, Faculty of Electrical Engineering, Automatics, Computer Science and Electronics
DOBSON Tibor (Hungary)	National Directorate General for Disaster Management
DURBAJLO Piotr (Poland)	Ministry of Interior and Administration, Dept. Of Teleinformational Infrastructure
DURRANT Paul (United Kingdom)	Department for Transport
EGGENBERGER René (Switzerland)	Eidgenössisches Department für Verteidigung, Bevölkerungsschutz und Sport, Bereich Forschungsmanagement & Kooperation
GALVÃO DA SILVA Frederico (Portugal)	GNR - Guarda Nacional Republicana
GRAMMATICA Alvise (EU)	EUROPOL - Information, Management & Technology Coordination Unit
GRASSO Giancarlo (Italy) (Deputy Chairman)	**Finmeccanica**
GREVERIE Franck (France)	Thales Security Solutions & Services Division
GULTEKIN Recep (Turkey)	Turkish National Police
GUSTENAU Gustav (Austria)	BMLV Bundesministerium für Landesverteidigung, Direktion Sicherheitspolitik

HADJITODOROV Stefan (Bulgaria)	Bulgarian Academy of Sciences, Centre of Biomedical Engineering
HENDEN Peter (United Kingdom)	Petards Group plc
HERTEMAN Jean-Paul (France)	Sagem Défense et Sécurité
HOLL Milan (Czech Republic)	Aeronautics Research and Test Institute
JERNBÄCKER Lars (Sweden)	Saab AB
KALNINS Kaspars (Latvia)	Riga Technical University
KLISARIC Milan (Serbia)	Ministry of Interior, Office for professional education, qualification, specialisation and science
KOTZANIKOLAOU Panayotis (Greece)	Hellenic Authority for the Assurance of Communications Privacy and Security (ADAE)
KÜRTI Tamás (Hungary)	KÜRT Corp. Information Managment (Information Security Technology), Research & Development Department
LEVENTAKIS George (Greece)	Centre for Security Studies (KE.ME.A)
LINDBERG Helena (Sweden)	MSB
MADALENO Utimia (EU)	EDA - European Defence Agency, R & T Directorate
MATE Dragutin (Slovenia) (Chairman as of 18 November 2008)	
MEDINA Manel (Spain)	Universidad Politécnica de Cataluna, Spanish computer emergency response team
MEY Holger (Germany)	EADS
MICHEL Bernd (Germany)	Fraunhofer Gesellschaft, Micro Materials Center
MURESAN Liviu (Romania)	EURISC Institute
NEKVASIL Vladimir (Czech Republic)	Academy of Sciences, Prague
NURIEL Nitzan (Israel)	National Security Council, Counter Terrorism Bureau
OGILVIE - SMITH Adam (United Kingdom)	Home Office
PAPADOPOULOU Vicky (Cyprus)	University of Cyprus, Department of Computer Science
PARIAT Monique (EU)	EUROPEAN COMMISSION - DG JLS - General Affairs Directorate
PHIPSON Stephen (United Kingdom)	Smiths Group plc, Security & Resilience Industry & Suppliers Council (RISC)
PISO Marius-Ioan (Romania)	Romanian Space Agency (ROSA)

PRANJÍC Stipan (Croatia)	Ministry of Interior, Inspectorate for the production & traffic of the dangerous substances
PRINZ Johannes (Austria)	FREQUENTIS, Corporate Research
RINTAKOSKI Kristiina (Finland)	Crisis Management Initiative
RODRIGUEZ AUGUSTIN Carmen (Spain)	INTA, Relaciones Institucionales y Politica Comercial
ROUJANSKY Jacques (France)	Ministère de la défense, DG de l'armement, Division Développement et technologies de sécurité et souveraineté
SERWIAK Sebastian (Poland)	Ministry of Interior & Administration of the Republic of Poland, Department of Public Security
SHALAMANOV Velizar (Bulgaria)	George C. Marshal Association
SIMON Carlo (Luxembourg)	Centre de Communication du Gouvernement
STIG HANSEN John-Erik (Denmark)	National Centre for Biological Defence
STOCK Jürgen (Germany) **Deputy Chairman**	**Bundeskriminalamt**
TEPERIK Dmitri (Estonia)	Ministry of Defence, Bureau of Security of Industry and Innovation
TOMASSON Bodvar (Iceland)	Linuhonnun Consulting Engineers
TRAVERS Eleanor (Ireland)	Transport Security Solutions Ltd.
UNGER Christoph (Germany)	BBK Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
VAN DUYVENDIJK Cees (The Netherlands)	TNO - Netherlands Organisation for Applied Scietific Research, TNO Board of Management
Van Rijn Afke (The Netherlands)	Clingendael - Netherlands Institute of International Relations
VILLANUEVA DIEZ Francisco (Spain)	Ministerio del Interior, General Directorate of Infrastructure and Security Means
WAGNER Juraj (Slovakia)	Ministry of Education
WEISSENBERG Paul (EU)	EUROPEAN COMMISSION - DG ENTR - Aerospace, GMES, Security & Defence Directorate
WIEDEMANN Sabine (Germany)	Deutsche Post AG, Abt. Konzernsicherheit
ZANASI Alessandro (Italy)	ZANASI Alessandro Srl. and University of Bologna

List of former ESRIF Members

DE BRABANDER – YPES Heleen (The Netherlands)	Ministry of Economic Affairs
DE VRIES Gijs (The Netherlands) Chairman until 18 November 2008	**Clingendael - Netherlands Institute of International Relations**
DUBRIE Brian (United Kingdom)	Home Office
ENSTEDT Dan-Åke (Sweden)	Saab AB, Saab Mgmt Team, Civil Security
KUETT Kristiina (Estonia)	Ministry of Defence
MARGUE Tung-Laï (EU)	EUROPEAN COMMISSION - DG JLS – General Affairs Directorate
THORELL Dan (Sweden)	Swedish Coast Guard Headquarters

List of ESRIF Working Groups (coordination and main contributors)

Coordination: BRATZ Christian, LEONE Cristina, TORKAR Matej

Working Group 1: Security of the citizens

Leader: VAN DUYVENDIK Cees

Rapporteur: SUCHIER Jean Marc

Sherpa: VAN VEEN Hendrik-Jan, DON Bert

Working Group 2: Security of critical infrastructures

Leader: TRAVERS Eleonor

Rapporteur: MEY Holger

Sherpa: HOFER Florian

Subgroups: COUDON François (Transport), WILLIE Donnelly (ICT), LANGER Michael (Site Security), BENES Ivan (Distributed Network Security)

Working Group 3: Border Security

Leader: BERGLUND Erik

Rapporteur: BARONTINI Giovanni

Subgroups: CLARKE Dave (Land Border Surveillance), GULIENETTI Giorgio (Air Border Surveillance), LHUISSIER Jean-Marie (Maritime Border Surveillance), SMIT Leon (Border Checks)

Working Group 4: Crisis Management

Leader: UNGER Christoph

Rapporteur: PRINZ Johannes

Sherpa: PASTUSZKA Hans-Martin, MISSOWEIT Merle (Co-Sherpa)

Subgroups: VAN BERLO Marcel (Terrorism and Crime attacks), CARLING Christian (Humanitarian Crises), KOPPE Rüdiger (Natural Disasters), FLUIJT Hans-Willem (Major Industrial Accidents), KIRK Manfred (Modern Concepts for Innovative Crisis Management)

Working Group 5: Foresight and Scenarios

Leader: RINTAKOSKI Kristiina

Rapporteur: ERICSSON E Anders

Working Group 6: CBRNE

Leader: BUSKER Ruud

Sherpa: BUCHWALDT-NISSEN Jacob
GREEN Tom

Working Group 7: Situation awareness and role of space

Leader: MADALENO Utimia

Rapporteur: COMPARINI Massimo Claudio

Working Group 8: Identification of people and assets

Leader: AMINOT Jean Luc

Rapporteur: WALSH Martin

Sherpa: DELARUE Henri

Working Group 9: Innovation issues

Leader: SIEBER Alois

Rapporteur: DESIMPELAERE Luc

Sherpa: JANSSENS Myriam

Subgroups: JANSSENS Myriam (Specificity of the Security Market), GROTH Sabine (Legal Framework), WARWICK Roger (Standardisation), SERRAULT Brigitte (Business Model), DON Bert and PASETTO Davide (Innovation Policy), SCHWIER Irene (Education and Training)

Working Group 10: Governance and coordination

Leader: ACCARDO Lucio

Rapporteur: OGILVIE-SMITH Adam

Sherpa: TONINI Pietro

Working Group 11: Human and societal dynamics of security

Leader: MURESAN Liviu

Rapporteur: SUNDELIUS Bengt

Transversal Coordinator:	McCARTHY Sadhbh
Sherpa:	CASTENFORS Kerstin, BURGESS J. Peter (Transverse Committee)
Subgroups:	SUNDELIUS Bengt (Governance), RANSTORP Magnus (Violent Radicalization Dynamics), OLSSON Eva-Karin (Mediatisation and Communication), HOLMES John (Economics of Security), CAS Johann (Ethical Aspects of Security Technologies), BURGESS J. Peter (Trust and Sherpa Transverse Committee)

List of ESRIF main contributors

ACCARDI Alberto
ADAMS Andrew
AL KHUDHAIRY Delilah
ALESSANDRINI Alessandro
ANNUNZIATO Alessandro
AUDREN Jean-Thierry
BASON Mark
BAUDINAUD Vincent
BEHRENS Jörg
BERGER Charles
BEYERER Jürgen
BIANCHI Alberto
BONERT Michael
BOULAT Jean-Charles
BOUTRY Philippe
BRAND Hermann
BRESCH David
BROSZKA Michael
BRÜCK Tilman
BRUMMER Wille
BYMAN Jan
CADISCH Marc
CARDIEL José
CARLSEN Henrik
CARTER David J.
CASERTA Laura
CECCHI Daniele
CENAS Narimantas
CHARALAMBOUS Yiannis
CHAWDHRY Pravir
CLARKE Michaela
CLARKE John
CLAVERIE Alain
COLE Andy
CONTARETTI Alberto Pietro
COOPER Timothy
CUSSET Xavier
DALY Ger
DAVIES Hilary
DAVIES Huw
DE GROEVE Tom
DE MISCAULT Jean-Claude
DE SMET Pieter
DE VITO Stefania
DELACHE Xavier
DELVAUX Nicolas
DESJEUX Isabelle
DESPAGNE Bruno
DETTER Helmut
DIETZ Patrick
DOGLIANI Mario
DOS SANTOS Josefine
ELOMAA Kimmo
EMARDSON Ragne
ERIKSSON E.Anders
ETTERER Thomas
FALLY Gerhard
FELGENHAUER Harald

FERNANDEZ VASQUEZ Diego
FERRARI Mariana Zuleta
FOURNIER Gilles
FOURNIER Raymond
FRANCHINA Luisa
FRENNBERG Hans
FRINKING Erik
FROTA Octavia
FUERSTENHOFFER Norbert
GABRIEL Vladislav
GALATOLO Giovanni
GARCIA-JOURDAN Sophie
GARNIER Bernard
GHERARDI Giuseppe
GIANNICCHI Luca
GIDE Laila
GOLDSWORTHY John
GOMEZ Celestino
GORETTA Olivier
GRAFF Xavier
GRAMMATICA Alvise
GRANTURCO Thierry
GRASEMANN Gerd
GROMMES Patrick
GRONWALL Christina
GUILPIN Jean-Claude
GURLEYIK Ender
GUSTAVSSON Per
GUTIERREZ Maria Cruz
HAMPSON Brian
HANEL Peter
HAP Benoit
HARNETT Kevin
HEDEKVIST Per Olof
HEIMANS Dick
HEISKANEN Markus
HELLMAN Maria
HERMANNS Andre
HIERNAUX Olivier
HIMBERG Kimmo
HLAVATÝ Richard
HOFFKNECHT Andreas
HONKONEN Risto
HOSKEN Norm
HÜBEL Wolfgang
JADOT André
KAEMPER Frank
KALAR Amo
KANGASPUNTA Seppo
KARBAUSKAITE Rasa
KEIZERS H.L.J. (Huub)
KEUS Klaus
KIOMETZIS Michael
KOCK Dagmar
KÖGEL Rudolf
KRAFT Holger
KRAFT Kristin
KRASTEV Krassimir
KUDRLOVA Monika
KUNERT Thomas
KUNZ Juergen
KÜNZEL Matthias
LACOSTE Francis
LANÇON Brice
LANGSELIUS Ann-Christine
LEGRAND Walter
LEONE Cristina
LEWIS Adam
LIBERATORE Ângela
LINDENCRONA Eva
LINDSAAR Mjr Inge
LÓPEZ Javier
LOUSBERG Maikke
LOZANO Raquel
LÜTZELER Michael
MAJID Fabienne

MARHIC Ronan
MARIN Nelson
MARINI Fabio
MARTÍNEZ Celia
MARTÍNEZ Daniel
MARTINI Gloria
MASON Stephen
MAUER Victor
MAYRHOFER Christoph
MAZZETTI Bruno
MCMAHON Stephen
McNULTY Sean
MEDINA Manel
MEHLHORN Jens
MEUWLY Didier
MILLER Mark
MOISIO Mikko
MOLL Bob
MOREL Michel
MULERO Manuel
MULLIGAN Ultan
MULQUEEN Michael
MURGADELLA François
MURPHY Michael
MURRAY Gerald
NIETO Octavio
NIEUWENHUIZEN Maarten
NORQVIST Anders
NORRHEM Bo
NÚÑEZ ALONSO Javier
ÖDMAN Svante
OLMEDO Laurent
OLSSON Hans-Ake
OOSTERWIJK Michiel
ÖSTMARK Henric
PACI Michel
PAPALIA Bruno
PASCAL Sylviane
PASIC Aljosa
PEJCOCH Jaroslav
PERANI Paolo
PFÄFFLE Peter
PRASTITES Loizos
PRIETO JUAN José
PRIETO SAIZ Carlos
PRIGGOURIS Nikolaos
PROTTI Marco
RAFALOWSKI Chaim
RAMIS José Manuel
RANTZER Martin
REBUFFI Luigi
RENARD Nicolas
RIOS MORENTIN David
RIZZO Carmine
ROSENSTOCK Wolfgang
ROSSI Federico
ROUCHOUZE Bruno
ROUHIAINEN Veikko
RÜHRIG Herbert
RUSSOTTO Remy
RYAN Johnny
RYDELL Robert
SAGNES Olivier
SAN JUAN Jesús
SCHREIER Gunter
SCHULZ Sandra
SCHULZE Joachim
SCOTTI DI UCCIO Gustavo
SERRANO CHECA Julio
SIEDSCHLAG Alexander
SIMONET Françoise
SNIJDER Max
SODERLIND Gustav
SÖKMEN Nermin
SOUDANI Karim
SOUFFLET Damien

STAICU Marcel
STELTE Norbert
STENERUS Anne-Sofie
STONE Howard
STOUSSAVLJEWITSCH Martin
SVENSON Pontus
SVÍTEK Miroslav
TÉBAR Clara
TINZ Marek
TOURET Olivier
TRENČANSKÝ Andrej
TROY Richard
ULMER Cedric
VAN DER STEEN Marcel
VAN HOOGHTEN Marc
VARCO Alan
VERGARI Fabrizio
WALLENIUS Klas
WARD Andreas
WARLETA Javier
WEBER Matthias
WENZEL Wolfgang
WERRETT David
WIKMAN-SVAHN Per
WINTERS Tom
ZILGALVIS Peteris
ZIMMERMANN Frank
ZUMAR Francisco Dequinto
ZUNKER Hugo
ZWAENEPOEL Sabine

ANNEX IV

Working Group References and Annexes

Working Group 3: Border Security

Australian Customs Service. *Customs Strategic Outlook 2015*. Australian Government, December 2007.

COLE Andy, HM Inspector, Border and Immigration Agency, Home Office, UK. *Presentation to ESRIF WG 3 - Clandestine Illegal Immigration: Costs and consequences*. March 2008

European Commission. *COM (2008) 68. Communication examining the creation of a European Border Surveillance System (EUROSUR).*

European Commission. *COM (2008) 69. Communication on an entry/exit system at the external borders of the European Union, facilitation of border crossings for bona fide travellers, and an electronic travel authorisation system.*

FRONTEX, *Identification of Capability Needs in the Field of Green Border Surveillance: Case Studies of Austria and Finland.* July 2007

Joint Research Centre Ispra, Italy. *INTEGRATED MARITIME POLICY FOR THE EU - Working Document III on Maritime Surveillance Systems*. European Commission, 14 June 2008

SEIFFARTH Oliver. *Presentation to ESRIF WG 3 - EU Border Security - Latest Developments*. European Commission for Justice, Freedom and Security, 2008.

Working Group 4: Crisis Managment

Documents on European level, in chronological appearance:

Commission of the EC, COM(2009) 263, Justice, Freedom and Security in Europe since 2005: An Evaluation of the Hague Programme and Action Plan, Brussels, June 2009

Commission of the EC, COM(2009) 262, An area of freedom, security and justice serving the citizen, Brussels, June 2009 (the Stockholm programme)

Council of the EU, A Secure Europe in a Better World - European Security Strategy, Brussels, December 2008

SOLANA Javier, S407/08, Report on the Implementation of the European Security Strategy – Providing Security in a Changing World –, Brussels, December 2008

Commission of the EC, COM(2008) 748, Global Monitoring for Environment and Security: we care for a safer planet, Brussels, November 2008

Council of the EU, 10128/08, Council Conclusions on Reinforcing the Union's Disaster Response Capacity – towards an integrated approach to managing disasters, Brussels, June 2008

Council of the EU, 7249/08, Climate change and international security, Brussels, March 2008

Commission of the EC, COM(2008) 130, Communication from the Commission to the European Parliament and the Council on Reinforcing the Union's Disaster Response Capacity, Brussels, March 2008

European Commission DG ENV (client), Assessing the Potential for a Comprehensive Community Strategy for the prevention of Natural and Manmade Disasters, Final Report, COWI A/S (Editor), Brussels/Kongens Lyngby, Denmark, March 2008

European Parliament, Directorate-General for External Policies of the Union (Publisher), Improving the Coherence of Crisis Management: New Technologies for Command and Control Systems, Study, CMI Finland (Editor), Brussels, February 2008

Council of the EU, 2008/C 25/01, The European Consensus on Humanitarian Aid, Joint Statement by the Council and the Representatives of the Governments of the Member States meeting within the Council, the European Parliament and the European Commission, in: Official Journal of the European Union, January 2008

European Commission, DGs RELEX, ECHO, Preliminary User Requirements for GMES-like services, Brussels, July 2007

EDA (client), The impact of commercial S&T development upon European Union Crisis Management Operations in 2030, SCS Ltd (Editor), Brussels/Henley-on-Thames, United Kingdom, April 2007

European Parliament and the Council of the EU, Regulation (EC) No 1717/2006 establishing an Instrument for Stability, in: Official Journal of the European Union, L 327/1, November 2006

ESRAB, Meeting the challenge: the European Security Research Agenda, Brussels, September 2006

EU Institute for Security Studies (Publisher), Civilian crisis management: the EU way, Paris, June 2006

Barnier Michel, Report to the Council of the EU, For a European civil protection force: Europe aid, May 2006

Commission of the EC, COM(2005) 565, Global Monitoring for Environment and Security: From Concept to Reality, Brussels, November 2005

Commission of the EC, COM(2005) 153, Reinforcing EU Disaster and Crisis Response in third countries, Brussels, April 2005

Council of the EU, 16054/04, The Hague Programme: strengthening freedom, security and justice in the European Union, Brussels, December 2004

The Group of Personalities in the field of Security Research, Research for a secure Europe, Brussels, 2004

Council of the EU, A Secure Europe in a Better World - European Security Strategy, Brussels, December 2003 (updated in 2008)

Documents on national level, countries in alphabetical appearance:

Finland, Prime Minister's Office, Finnish Security and Defence Policy 2004, Helsinki, 2004

France, The President, The French White Paper on defence and national security, Paris 2008,

Germany, Forum on the Future of Public Safety and Security, Risks and Challenges for Germany – Scenarios and Key Questions, Green Paper, Berlin/Bonn September 2008

Germany, Federal Ministry of Defence, White Paper 2006 on German Security Policy and the Future of the Bundeswehr, Berlin, October 2006

Germany, The Advisory Board for Civil Protection to the German Interior Minister, Third Risk Report, Bonn, March 2006

Germany, Ministry of the Interior, Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ), New Strategy for the Protection of the Citizens in Germany, 2003

The Netherlands, Ministry of the Interior, National Security: Strategy and Workprogramme, Den Haag, 2007

The Netherlands, Ministry of the Interior, Policy plan Crisis Management 2004-2007, Den Haag, 2004

United Kingdom, HM Government, The United Kingdom's Strategy for Countering International Terrorism, London, March 2009

United Kingdom, Cabinet Office, The National Security Strategy of the United Kingdom - Security in an interdependent world, London, March 2008

United States, National Intelligence Council, Global Trends 2025: A Transformed World, Washington D.C., November 2008

United States, Department of Homeland Security, National Response Framework Overview, Washington D.C., January 2008

United States, Homeland Security Council, National Strategy for Homeland Security, Washington D.C., October 2007

United States, Department of Homeland Security, National Preparedness Guidelines, Washington D.C., September 2007

United States, Department of Homeland Security, Target Capabilities List – A companion to the National Preparedness Guidelines, Washington D.C., September 2007

United States, Homeland Security Council, Planning Scenarios - Executive Summaries, Washington D.C., July 2004

United States, Department of Homeland Security, Universal Task List (UTL), Washington D.C., Draft July 2004

Working Group 5: Foresight and Scenarios

ERIKSSON E. A. and WEBER M. (2008): Adaptive Foresight: Navigating the complex landscape of policy strategies, *Technological Forecasting & Social Change*, 75(4): 462-482

European Commission (2001): European Governance: A White Paper, Brussels: European Commission

European Commission (2002): *Thinking, Debating and Shaping the Future: Foresight for Europe,* Final Report of the High Level Expert Group for the European Commission, September 2002

European Commission (2009): *What is Foresight :_Definition* (http://cordis.europa.eu/foresight//definition.htm, last accessed on 2 October 2009)

ForLearn (2009): *ForLearn Online Foresight Guide* (http://forlearn.jrc.ec.europa.eu/guide/0_home/index.htm, last accessed 2 October 2009)

HAVAS A., SCHARTINGER D., WEBER M. (forthcoming): The impact of foresight on (innovation) policy-making: Recent experiences and future perspectives, *Futures*

KUHLMANN S. (2001): *Management of innovation systems: The role of distributed intelligence*, Maklu Uitgevers N.V., Antwerpen

OECD (2005): *Governance of Innovation Systems*, *Volume 1: Synthesis Report*, OECD, Paris

TRUFFER B., VOSS J.-P., KONRAD K. (2008): Mapping Expectations for System Transformations. Lessons for Sustainability Foresight in German Utility Sectors, *Technological Forecasting and Social Change 75,* 1360-1372

UNIDO (2003): *Technology Foresight Manual,* United Nations Industrial Development Organisation, Vienna

WIKMAN-SVAHN P. (2009): State of the Art Scan; Meta-analysis of recent security-related foresight studies, ESRIF

Working Group 6: CBRN

Commission of the European Communities. *Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan*. Brussels: COM(2009) 273 final.

Commission of the European Communities. *Green Paper on Bio-Preparedness*. Brussels: COM(2007) 399 final.

Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats; Development, Security, and Cooperation Policy and Global Affairs Division; Board on Global Health Institute of Medicine; Institute of Medicine and National Research Council of the National Academies. *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington: The National Academies Press, 2006.

EU Permanent Representatives Committee. *First annual Presidency report (2003) to the Council on the implementation of the joint Programme of the Council and the Commission, of 20 December 2002, to improve cooperation in the European Union for preventing and limiting the consequences of chemical, biological, radiological or nuclear terrorist threats*. 16285/03. Brussels: Council of the European Union, 2003.

EU Working Party on Civil Protection. *Second annual Presidency report (2004) to the Council on the implementation of the joint Programme of the Council and the Commission, of 20 December 2002, to improve cooperation in the European Union for preventing and limiting the consequences of chemical, biological, radiological or nuclear terrorist threats (2002 CBRN Programme)*. Rep. no. 8988/05. Brussels: Council of the European Union, 2005.

Faull Jonathan et al. *Report of the CBRN Task Force*. European Commission for Justice, Freedom and Security, 2009.

LANGENBERG Jan, GÖRAN Olofsson, Ruud BUSKER, Veikko KOMPPA, MELLADO Rafael, STREBL Friederike, VAN HOOFT Peter, BULLEN Bert, WINKLER Thomas and NIEUWENHUIZEN Maarten.

Preparatory Action on the enhancement of the European industrial potential in the field of Security research PASR (2004-2006). Grant Agreement no. SEC4-PR-008000. IMPACT (Innovative Measures for the Protection against CBRN Terrorism) WP900, 2007. Deliverable D900.2.

LEEUW M. W., Project coordinator. *Assessment of the vulnerabilities of modern societies to terrorist acts employing radiological, biological or chemical agents with the view to assist in developing preventive and suppressive crisis management strategies*. EU Project 502476, 2008. Deliverable #9 Final Report.

LINDSTROM Gustav. *Protecting the European Homeland; the CBR Dimension*. European Union Institute for Security Studies Chaillot Paper No. 69. Condé-sur-Noireau: Corlet Imprimeur, 2004.

MACKBY Jennifer. *Strategic Study on Bioterrorism*, Center for Strategic and International Studies, 2006.

NATO Headquarters, Supreme Allied Command Transformation (HQ SACT), Intelligence Sub-Division. *Future Security Environment*. First ed. Norfolk: NATO HQ SACT, 2007.

The Netherlands Ministry of Foreign Affairs, Department for Security Policy, Division of Nuclear Disarmament and Non-Proliferation. *The non-proliferation policy of the Netherlands*. Text by F. Van Beuningen. Den Haag: OBT bv, 2006.

The Royal Society working group on detecting and decontaminating chemical and biological agents. *Making the UK safer: detecting and decontaminating chemical and biological agents*. Chair: Herbert Huppert. London: The Royal Society, 2004.

TUCKER Jonathan B. *Biosecurity: Limiting Terrorist Access to Deadly Pathogens*. Peaceworks No. 52. Washington: United States Institute of Peace, 2003.

United Kingdom Ministry of Defence. *Defence Technology Strategy for the demands of the 21st century*. London: Ministry of Defence DGMC PR Graphics, 2006.

United States Federal Research Division. *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?* By Rex A. Hudson. Ed. Marilyn Majeska. Washington: Library of Congress, 1999.

Weapons of Mass Destruction Commission. *Weapons of Terror: Freeing the World of Nuclear, Biological, and Chemical Arms*. Final report. Stockholm: EO Grafiska, 2006.

Working Group 8: Identification of People and Assets

I. Biometrics Improvement

ANDRONIKOU Vassiliki et alii, Biometric Implementations and the Implications for Security and Privacy, National Technical University of Athens Department of Electrical and Computer Engineering, 20 pages, 2007.

BATALLER Cyrille et alii, Accenture Technology Labs, Biometrics Liveness Detection, Accenture white paper, 12 pages, Sophia Antipolis, France, 2009.

BIO TESTING EUROPE, Towards European Testing and Certification of Biometric Components and Systems, PASR 2006, 11 pages, June 2008.

BLOMEKE Christine R., ELLIOTT Stephen J., WALTER Thomas M., Bacterial Survivability And Transferability On Biometric Devices, 5 pages, Purdue University, West Lafayette, Illinois, USA, 2008.

BONANSEA Laurent., Biometrics and Migration, EU Perspectives, Presentation for IOM – BITE project meeting, Geneva, Switzerland, 30 pages, July 2005.

CEYHAN Ayse, Identité et identification au prisme de la biométrie, Institut des Hautes Etudes de la Justice, Séminaire de Philosophie du Droit 2005-2006, Paris, France, 15 pages, mars 2006.

CAVOUKIAN Ann, STOIANOV Alex, Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, Information and Privacy Commissioner, Ontario, Toronto, 52 pages, March 2007.

DESSIMOZ Damien et alii, Multimodal Biometrics for Identity Documents, State-of-the-Art, Research Report, University of Lausanne, 161 pages, June 2006.

DORIZZI Bernadette, GARCIA-MATEO Carmen, Multimodal Biometrics, Editorial, ANN. TÉLÉCOMMUN., 62, n° 1-2, pp. 1506-1514, 2007.

MODI Shimon K., ELLIOTT Dr Stephen J., Impact of Image Quality on Performance: Comparison of Young and Elderly Fingerprints, Proceedings of the 6th International Conference on Recent Advances in Soft Computing RASC 2006), K. Sirlantzis (Ed.), pp. 449-454, 2006

MTIT (Minutiae template interoperability testing), Research report on minutiae interoperability tests, version 1.0, 10 pages, March 2007.

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, Subcommittee on Biometrics, The National Biometrics Challenge, 22 pages, Washington, August 2006.

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, Biometrics "Foundation Documents", Washington, 166 pages, 2007.

PRISE, Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies, Overview of Security Technologies v 1.2, 2007.

SMITH Joshua, SCHUCKERS Dr S., Improving Usability and Testing Resilience to Spoofing of Liveness Testing Software for Fingerprint Authentication, Honors Program Thesis Proposal, 10 pages, March 2005.

SNELICK Robert) et alii, Large Scale Evaluation of Multimodal Biometric Authentication, Using State-of-Art Systems, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, pp 450-455, March 2005.

SNIJDER Marc, Security & Privacy in Large Scale Biometric System, Report, European Biometrics Forum, 28 pages, September 2006.

TILTON Catherine J., Biometrics Standards : Overview, A Daon White Paper, Dublin, Eire, 12 pages, March 2009.

VAN DES PLOEG Irma, The Politics of Biometric Identification, BITE Policy Paper Nr 2, 16 pages, November 2005.

WHADWHA Kush, Biometrics and Privacy, Presentation for 2nd scientific BITE project meeting, Roma, Italia, 45 pages, April 2005, on line at www.biometricgroup.com.

II. Struggling ID Theft and Fraud

BUCCI Steven) and POULAIN Guy, L'alliance du terrorisme et de la cybercriminalité ?, in Défense Nationale et Sécurité Collective, pp. 117-128, March 2009.

CEN Workshop Agreement (CWA 15263), Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization, Brussels, Belgium, 33 pages, April 2005.

CLARKE Roger, Introducing PITs and PETS Technologies: technologies affecting privacy, http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html.

DAVOUX Alexis) et alii, Federation of Circles of Trust and Secure Usage of Digital Identity, Journal of computer security, Vol. 14, Issue 3, Paris, France, pp.269—300, 2008.

DETRAIGNE Yves, ESCOFFIER Anne-Marie, La vie privée à l'heure des memoires numériques, Rapport d'information, Sénat, n° 08-441, Paris, France, 153 pages, mai 2009.

ELLIOTT Stephen J., HUNT Adam R., The Challenge of Forgeries and Perception of Dynamic Signature Verification, Proceedings of the 6th International Conference on Recent Advances in Soft Computing (RASC 2006), K. Sirlantzis (Ed.), pp. 455-459, 2006.

EUROPEAN COMMISSION, Europe Information Society, Privacy Enhancing Technologies, Communication, COM 2007 (228) final, May 2007, on line at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0228:EN:NOT .

IFRAH Laurence, Les nouvelles menaces criminelles numériques, in Cahiers de la Sécurité n°6, INHES, Saint Denis la Plaine, pp. 59-65, October 2008.

IFRAH Laurence, Fraude identitaire, phishing et spam : les menaces majeures en 2009, in Défense Nationale et Sécurité Collective, pp. 43-51, March 2009.

KIM Rachel) et alii, Javelin Strategy & Research, 2007 Identity Fraud Survey Report, Consumer Version, How Consumers Can Protect Themselves, Pleasanton, California, USA, 22 pages, February 2007.

KIM Rachel) et alii, Javelin Strategy & Research, 2008 Identity Fraud Survey Report, Consumer Version, How Consumers Can Protect Themselves, Pleasanton, California, USA, 23 pages, February 2008.

KOON Ronald) et alii, KPMG Information Risk Management, Privacy-Enhancement Technologies, White Paper for Decision-Makers, La Haye, Nederlands, 76 pages, December 2004.

MATTATIA Fabrice, De l'utilité d'une carte d'identité électronique pour sécuriser le monde numérique, ANN. TÉLÉCOMMUN., 62, n° 11-12, 2007, pp. 1221-1238.

Mc KENNA Rob, Combattre le cybercrime – Un point de vue du Ministre de la Justice de l'Etat de Washington, in Cahiers de la Sécurité n°6, INHES, Saint Denis la Plaine, pp. 164-172, October 2008.

NAUDIN Christophe, Cybercriminalité identitaire, in Cahiers de la Sécurité n°6, INHES, Saint Denis la Plaine, pp. 42-48, October 2008.

NEWMAN Graeme R., Mc NALLY Megan M., Identity theft – A Research Review, full report to the National Institute of Justice, Washington DC, USA, 114 pages, July 2005, on line: http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=210459.

NIST National Institute of Standards and Technology), Recommended Security Controls for Federal information Systems and Organisations, Special Publication 800-53, Revision 3, Gaithersburg, MD, USA, 237 pages, August 2009, on line at : http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf.

PAGET François, Identity Theft, White Paper, Mac Afee, 15 pages, January 2007, on line : www.mcafee.com

PESCH Gérard, Cybersécurité : protection des systèmes d'information et résilience des organisations, in Cahiers de la Sécurité n°6, INHES, Saint Denis la Plaine, pp. 83-90, October 2008.

PLATZER Christian) and FORWARD Consortium, Threats on the Internet, Seminar Report, Seventh Framework Programme, ICT and Secure, dependable and trusted Infrastructures, 28 pages, Vienna, Austria, October 2008.

RAND EUROPE, Technological Solutions to Protect Privacy in e-Government, Review 2(3), 2003, on line at: http://www.rand.org/ randeurope/review/2.3-horlings.html.

RASMUSSEN Rod, AARON Greg, Global Phishing Survey : Domain Name Use and Trends in 1H 2008, APWG, Lexington, Maryland, USA, 23 pages, November 2008.

RASMUSSEN Rod, AARON Greg, Global Phishing Survey : Domain Name Use and Trends in 2007, APWG, Lexington, Maryland, USA, 29 pages, May 2008.

RUBINA Johannes) et alii, Javelin Strategy & Research, 2006 Identity Fraud Survey Report, Consumer Version, How Consumers Can Protect Themselves, Pleasanton, California, USA, 20 pages, February 2006.

US FEDERAL TRADE COMMISSION, Consumer Fraud and Identity Theft Complaint Data, January-December 2007, Washington DC, USA, 92 pages, February 2008.

WEBER Tim, Cybercrime threat rising sharply, BBC news article, Davos, 2009. on line at http://news.bbc.co.uk/2/hi/business/davos/7862549.stm.

III. DISASTERS ID VICTIMS MANAGEMENT

BROMBERG Katherine, EBT Disaster Aid Integration, Lessons from Katrina, Possible Solutions, and Foreseeable Complications, 30 pages, May 2007.

CHENEY Julia S., The Role of Electronic Payments in Disaster Recovery: Providing More Than Convenience 194, Federal Reserve Bank of Philadelphia, May 3-4, 2006.

KIDDER F. Key, After Katrina: Identifying the Dead with Biometric ID, 2007, article on line at http://www.forensicmag.com/articles.asp?pid=70.

MORDINI Emilio, OTTOLINI Corinna, Body identifcation, biometrics and medicine: ethical and social considerations, Ann Ist super sAnItà, Vol. 43, no. 1: pp. 51-60, Rome, Italy, 2007.

SCHULLER-GOTZBURG P., SUCHANEK J., Forensic odontologists successfully identifytsunami victims in Phuket, Thailand, rapid communication, Forensic Sci. Int., 2006, on line at www.sciencedirect.com.

STANTON Thomas H., Delivery of Benefits in an Emergency: Lessons from Hurricane Katrina 14, IBM Center for the Business of Government, 2007.

IV. PASSENGER TRAVEL SECURITY AND FACILITATION

AME Info.com, How to fast track through airports, Middle East: Tuesday, October 23 – 2007, on line at http://www.ameinfo.com/135604.html

BATALLER Cyrille, Accenture Technology Labs, Simplifying Passenger Travel Interest Group: miSense Biometrics Trial, 4 pages, Sophia Antipolis, France, 2007.

BATALLER Cyrille, Accenture Technology Labs, Automatic Border Clearance, Presentation at Londoon Biometrics 2008, 12 pages, Sophia Antipolis, France, October 2008.

DOUGLAS Tony, miSense, Biometrically enabled access control trial at Heathrow Airport 2006/07, Summary report, 18 pages, BAA 2007.

EUROPEAN COMMISSION, New tools for an integrated European Border Management Strategy, Memo/08/85, Brussels, Belgium, 5 pages, February 2008.

EUROPEAN COMMISSION, Consultation Paper on the technical options associated with setting up an entry/exit system at the external borders of the European Union and facilitating border crossings for bona fide travellers, Brussels, 24 pages, October 2008.

SAUNIER Michel, s-Travel: using biometrics to improve Passenger Handling at Airports, European Commission, Final report, Brussels, 2005, on line at http://s-travel.aero.

UKBA (United Kingdom Border Agency), A strong new force at the border, London, United Kingdom, 24 pages, August 2008.

UNISYS, Entry-exit Feasibility study, Final Report for European Commission DG JLS, 360 pages, February 2008.

V. MOBILE READERS

BOERTIEN Nicky, MODDELKOOP Eric, Authentication in mobile applications, Project's Final Report, Virtuale Haven, Telematica Instituut & CMG, 54 pages, 2002.

EARLAND Richard, Mobile Technology Creates New Ways of Working for Police, NPIA Report, April 2009, on line at : http://www.npia.police.uk/en/13058.htm.

EUROPEAN COMMISSION, Joint Research Centre, Biometrics at the Frontiers: Assessing the Impact on Society, Technical Report to the European Parliament, Brussels, European Communities, 67 pages, 2005.

MOTOROLA, Mobile Biometric Identification, White Paper, 8 pages, Anaheim, California, USA, 2008, available on line at : http://www.motorola.com/staticfiles/Business/Products/Biometrics/Mobile%20AFIS/Mobile%20AFIS/_Documents/Static%20Files/Mobile%20Identification%20White%20Paper.pdf?localeId=33.

NESS Werner, Performance Considerations on Reading ePassports, presentation for Brussels Interoperability Group's Meeting of Paris, 13 pages, October 2007.

NPIA (National Policing Improvement Agency), MIDAS & Lantern Mobile Fingerprints projects, Equality Assessment Consultation Paper, 21 pages, London, UK, 2009,

ORANDI Shahram, McCABE R. Michael, National Insititute of Standards and Technology, Mobile ID Device Best practice Recommandation, Version 1.0, Gaithersburg, MD, USA, 55 pages, August 2009, on line at : http://fingerprint.nist.gov/mobileid/MobileID-BPRS-20090825-V100.pdf.

PICKERING Sharon, WEBER Leanne, Borders, mobility and technologies of control, Springler, Berlin, Germany, ISBN: 978-1-4020-4898-2, 222 pages, 2006.

VI. TRACKING GOODS AND ASSETS

BABUL LTC Michael J., "No Silver Bullet": Managing the Ways and Means of Container Security, Strategy Research Project, US Army War College, Carlisle Barracks, Pennsylvania, USA, 29 pages, January 2004.

ROBINSON H. William et alii, Border and Transportation Security: Possible New Directions and Policy Options, Congressional Research Services, The Library of Congress, Washington DC, USA, 24 pages, March 2005.

SIEBER Aloïs J. et alii, Emerging Technologies in the Context of "Security", Research Security Paper, Institute for the Protection and Security of the Citizen, Sensors Radar Technologies and Cybersecurity Unit, 46 pages, September 2005.

THEYS Jacques, Quelles technologies-clefs pour l'Europe ? : Les enjeux liés aux transports, Dossier de prospective et de recherche, Commission Européenne, DG Research, Brussels, 145 pages, April 2005, on line at : ftp://ftp.cordis.europa.eu/pub/technology-platforms/docs/kte_transports.pdf.

VAN DE WOORT Maarten, LIGTVOET Andreas, Towards an RFID Policy for Europe, Workshop report prepared for the EUROPEAN COMMISSION, Directorate General Information Society and Media, 61 pages, August 2006.

WILLIS Henry H., ORTIZ David S., Evaluating the Security of the Global Containerized Supply Chain, Technical Research Report, Rand Corporation, Santa Monica, California, USA, 49 pages, 2004. On line at www.rand.org

Working Group 9: Innovation Issues

Presentations to ESRIF WG 9 from experts in various fields

Bresch, David N., Disaster Risk Management and Financing - Dr. David N. Swiss Re – ESRIF WG9 meeting of 13-10-2008

Insurance of Government Assets - Anna Kingsmill-Vellacott AKV Associates Ltd – ESRIF WG9 meeting of 13-10-2008

Certification of Critical Infrastructures – Antonius Sommer TÜV Informationstechnik GmbH – ESRIF WG9 meeting of 13-10-2008

Perspectives on Innovation - Prof. Dr. Ir. Ruud Smits, Innovation Studies Group University of Utrecht – ESRIF WG9 meeting of 13-10-2008

Privacy and Security: "What about Security Research?" – Peter Hustinx, European Data Protection Supervisor – ESRIF WG 9 meeting of 09-12-2008

Education and Training in Forensics: The European Network of Forensic Science Institutes – Dr. Jan De Kinder, Nationaal Instituut voor Criminalistiek en Criminologie, Chairman designate ENFSI – ESRIF WG 9 meeting of 09-12-2008

Conceptual Approach to the Chemical Weapons Convention (CWC) Education and Outreach – Jiří MATOUŠEK, Masaryk University, Faculty of Science – ESRIF WG 9 meeting of 09-12-2008

Innovation in Human Factors – Patrick Grommes, Aerospace Psychology Research Group, Trinity College Dublin – ESRIF WG 9 meeting of 09-12-2008

Education and training of forensic experts – Pavel Kolář, Institute of Criminalistics Prague – ESRIF WG 9 meeting of 09-12-2008

T&E of forensic experts - Ulrich Simmross, BKA – ESRIF WG 9 meeting of 09-12-2008

Szenario-Studie "Forschung im Bereich Sicherheit und Verteidigung im Jahr 2030" – Dagmar Kock, Fraunhofer INT – ESRIF WG 9 meeting of 09-06-2009

Towards harmonised national procurement for Fire services, challenges and opportunities – Brian Hansford, Firebuy (UK national procurement office) – ESRIF WG 9 meeting of 09-06-2009

Working Group 10: Governance and coordination

Annex 1: Four Models of Analysis

	Culture as a factor in the perception/definition of threat	**Culture as a factor in the response to threat**
Cultural factors influencing the thematic thrust of national security research programmes (e.g. prevention/ preparedness v. reaction/response; technology v. society)	*Model II / Knowledge and interpretation* Development of shared understanding of the concept of security; cognitive construction of a common European security space; overcoming traditional national interpretations and courses of action through the development of common concepts and knowledge Example: *Explanation for the variety of research themes present in EU Member States security research programmes and the interpretation of cultural factors as part of the security problem vs. part of the solution. For example, immigrant cultures may be interpreted as the cause of social radicalization processes that mount up to threats to internal security (such as in France or the Netherlands); differently, a user security culture may be interpreted as a social firewall against IT security offences (as it is the case in Sweden).*	*Model IV / Action repertories* Reduction of complexity to available individual/proprietary, experience-based strategies; attempt to make national strategies international standards; divergent national responses to same structural pressures; problem of harmonization of national implementation actions Example: *Explains why EU Member States adapt differently to similar security threats and also may implement commonly defined security capabilities plans and research coordination strategies in divergent ways. Standardisation for example might be implemented by Europeanization (development of or adherence to common standards on the EU level) or by a national joined-up approach of interagency coordination*

	Culture as a factor in the perception/definition of threat	Culture as a factor in the response to threat
Cultural factors influencing the national approach to security (research) governance (e.g. national inter-agency coordination vs. international standardisation)	<u>*Model III / Common symbols*</u> Ideas and habits defining national characteristics of security and governing threat perception; explanation of formation of action repertories as assumed as independent variable in model IV Example: *A country that has a security culture centred on prevention and foresight as the symbol for security will have normative difficulty to engage in security research coordination centred on response/reaction and to accept topics such as civil protection as elements of a European security (research) agenda.*	<u>*Model I / Normative values*</u> Focus on institutional foundations that provide values on which decision-making is based: Deriving common values from coordinated threat assessments and common security capability plans; development of a common European security identity along with standardisation and certification of security solutions Problem: May lead to the development of separate national values and themes for national security research (coordination) and for European security research (coordination) Example: *A certain normative concept of civil society present in a EU member state may prevent that state from participation in international security (research) coordination, especially in the field of technical solutions to security problems, because this runs counter to that state's conception of liberty and self-determination of its people.*

Annex 2: Evidence of the Four Cultural Factors

Matrix 1: Assignment of evidence for each of the four big cultural factors (models I-IV) per country to the four identified gaps/challenges

AT Austria, DE Germany, ES Spain, FR France, IT Italy, NO Norway, NL Netherlands, SE Sweden, UK United Kingdom

A country may be have "+" and "-" -entries in the same field, reflecting an ambiguous effect of the respective cultural factor

Status/gap	**Culture as a factor in the response to threat**	**Culture as a factor in the perception/definition of threat**		**Culture as a factor in the response to threat**
	Cultural factors influencing the national approach to security (research) governance	**Cultural factors influencing the thematic thrust of national security research programmes**	**Cultural factors influencing the national approach to security (research) governance**	**Cultural factors influencing the thematic thrust of national security research programmes**
	Model I **Normative values**	**Model II** **Knowledge/interpretation**	**Model III** **Common symbols**	**Model IV** **Action repertories**
Potential for a comprehensive approach at the national level	**AT** + Tradition of and legal provisions for "comprehensive national defence" **FR** + Internal security as a general concept in the context of sûreté which is meant to be a guarantee for exercising liberties and rights **DE** - Technical understanding of security and culture of security centred on the norm of preserving state functioning and protecting market economy	**AT** + Common practice of consocialism and consensus democracy increases potential for pluralistic analysis **FR** + Joint issuing of the current edition of the national security research programme by the National Research Agency, the General Delegation for Armament and the General Direction of the National Police **DE** - Academic approach to security research, centred on the technological science dimension,	**AT** - Tradition of "comprehensive national defence" tends to limit threat perception to threats that affect the public on a nationwide scale **FR** + Security as a symbol for crisis management in a broad sense, independent from the source of origin (such as natural, man-made and others) **DE** + Security as defence (Cold-war front state threat from outside and extremist threat from within)	**AT** + Common practice of consocialism and consensus democracy increases potential for national coordination + Management of transversal issues happens on a regular basis in the framework of a steering committee with representatives from all relevant ministries that is regularly convened by the Ministry of Transport, Innovation and Technology as the owner of the national security research programme **FR**

	infrastructure/mechanisms **NL** + Normative conviction that security is an all-societal affair and must rest on contributions from the national government, local governments, the business community, social organizations and citizens **NO** + Internal security as national security, security of the "riket"; multidimensional, multifunctional approach – not only confronting threats to citizens and infrastructure but threats to values of the nation, from democracy, health and territorial integrity up to economic security and cultural values **ES** + Normative idea of national innovation by dedicating research to cross-cutting themes **SE** - The leading normative value for security policy and research is emergency management and information security/protection	limits thematic scope **NL** + Security interpreted as a task on the level of the state organization as a whole, including societal stakeholders **ES** - Security mainly framed in terms of critical information and communication infrastructure **SE** + National security research is understood as an instrument for improving conditions for participating in the EU's security research programme **UK** + Combating terrorism is interpreted as a comprehensive task, including politics, public, technology, applied sciences and academia **NO** - Interpretation of security as information security	- security culture as such has been characterised by a relative separation of external and internal security **NL** **ES** - Very different concepts of security with different connotations; National security challenges are seen as symbolizing European challenges (e.g. illegal immigration and terrorism);streamlining/harmonization therefore is seen taking place at the interface between the national and the European level; Policy of alignment with European and international institutions; enhancement of national programmes and initiatives through European programmes and initiatives **SE** **UK** + Homeland security symbolism favours science and technology cooperation and critical infrastructure protection **NO**	**DE** - Cold war front state legacy leads to an over-emphasis of civil protection practices **NL** **ES** **SE** **UK** + Commonwealth tradition facilitates sharing of experience and solutions with international partners **NO** - Nurturing a culture of security, but only in the sector of critical information and communication technology **IT** + Concern with organized crime promotes electronic surveillance and information management on the level of the national government

	UK + Inter-agency joined-up approach is a normative value, based on experience with administration in commonwealth and multiculturalism affairs **IT** + Political norm of comprehensive risk assessment and management; coordinates local, regional and central/national authorities, technical and scientific experts and operational entities	**IT** + Cognitive approach directed at comprehensive risk information and assessment, involving international import and export of scientific (technological) knowledge	**IT** + Internal security and public safety as national tasks, at the same time political culture is open towards an Europeanization of the security sector due to long experience with internationally acting organized crime	

Potential for a comprehensive approach at the European level	**AT** + Tradition and legal provisions for "comprehensive national defence" **FR** **DE** - Idea of national security and protection of own values against challenges from within (normative response to totalitarian experience) **NL** **ES** **SE** - Establishing international linkages, but mainly in order to support industry participation in foreign (mainly U.S.) security research programmes **UK** - Norm of reference is rather the U.S. than the EU context	**AT** - Common practice of consocialism and consensus democracy limit the potential for developing shared European understandings - Security interpreted as a task on the level of the state organization as a whole **FR** - Management of transversal issues confined to the idea of national security; comprehensive risk assessment and strategic foresight increasingly vested in the policing sector **DE** - Security interpreted as a task on the level of the state organization as a whole/as a government matter **NL** - Security interpreted as a task on the level of the state organization as a whole, including societal stakeholders **ES** + Tendency to use EU institutions to promote own agenda and to seek support for own positions is limited by mistrust against other security cultures	**AT** - Tradition of "comprehensive national defence" tends to limit threat perception and preparedness to confront threats to the national level; European activities are expected to have immediate returns on national security **FR** **DE** - Idea of a protective state responsive to the specific security requirements of its citizens **NL** **ES** **SE** **UK** **NO**	**AT** + Domestic security (research) culture of coordination and pluralistic analysis and associated practices can help implement coordination on a European scale **FR** + Practice of involvement in international mechanisms in fight against organized crime, seen as an opportunity to develop knowledge of global trends in crime and advocate own policies **DE** - Bundesländer-based competencies in the civil protection sector **NL** + Practice of networking, establishment of international security networks and deems the national approach to be aligned of that of other nations and organizations **ES** - Typically uses EU institutions to promote own agenda and to seek support for own positions. But limited by mistrust against other security

	NO - Internal security as national security, security of the "riket" **IT**	**SE** + National security research is understood as an instrument for improving conditions for participating in the EU's security research programme **UK** - Security interpreted as a task on the level of the state organization as a whole/as a government matter **NO** + Security seen as based on international standards/standardisation **IT** + Cognitive approach directed at comprehensive risk information and assessment, involving international import and export of scientific (techno-logical) knowledge	- Information and infrastructure protection as a symbol of national security **IT** + Internal security and public safety as national tasks, at the same time political culture is open towards an Europeanization of the security sector due to long experience with internationally acting organized crime	cultures **SE** **UK** + Commonwealth tradition facilitates sharing of experience and solutions with international partners + Tradition of permanent cooperation with partners in the fields of conventional crime/violence prevention and protection against terrorist attacks **NO** + Nurturing a European culture of information security **IT** + Concern with organized crime promotes culture of information sharing - problem of implementing European practices into the action repertories of national agencies with overlapping powers which are often difficult to coordinate

Overcoming the lack of a comparable set	**AT** - Coordination approach based	**AT** - Pluralistic approach, but focus on the	**AT**	**AT**

of security strategies and approaches to security governance (coordination vs. standardisation), including the improvement of coordination of national security research and foresight activities with European-level research programmes	on a certain idea of national security **FR** + Sûreté tradition/culture supports a balanced approach between internal and international dimension and governance mechanisms **DE** - National basis of threat assessment: European programme is not a substitute for Member States' national programmes with their own focus and concentration on specific security requirements **NL** **ES** **SE** **UK** - Norm of reference is rather the U.S. than the EU context	national security space and on standardisation on the national level (e.g. common situation picture/assessment) **FR** **DE** - Security interpreted as a task on the level of the state organization as a whole/as a government matter **NL** - Security interpreted as a task on the level of the state organization as a whole, including societal stakeholders **ES** **SE** + National security research is understood as an instrument for improving conditions for participating in the EU's security research programme **UK** + Combating terrorism is interpreted as a comprehensive task, including politics, public, technology, applied sciences and academia	- Security is seen as a national symbol **FR** - Security is seen as a national symbol **DE** - Security culture as such has been characterised by a relative separation of external and internal security; European efforts are concentrated on the ESDP dimensions of security **NL** **ES** - Very different concepts of security with different connotations; National security challenges are seen as symbolizing European challenges (e.g. illegal immigration and terrorism);streamlining/harmonization therefore is seen taking place at the interface between the national and the European level **SE** **UK** **NO**	**FR** **DE** - Cold war front state legacy leads to an over-emphasis of civil protection practices **NL** **ES** **SE** + Establishing international linkages in order to support industry participation in foreign security research programmes **UK** + Tradition of permanent cooperation with partners in the fields of conventional crime/violence prevention and protection against terrorist attacks **NO** **IT** + Importing and exporting

	NO - Internal security as national security, security of the "riket" **IT**	**NO** - Security overly seen as based on international standards/standardisation + Security research aimed to contribute to Europeanization/internationalization of information security **IT** + Cognitive approach directed at comprehensive risk information and assessment, involving international import and export of scientific (technological) knowledge	**IT**	technical-scientific knowledge for comprehensive risk assessment

Overcoming the split in thematic thrust (society vs. technology), with a tendency to favour technological solutions to security problems)	**AT** - Traditional value of "comprehensive national defence" favours technological solutions and prevention, risking gaps in the field of (governance and coordination of) crisis reaction/response **FR** - Internal security as a general concept in the context of sûreté which is meant to be a guarantee for exercising liberties and rights **DE** **NL** **ES** + Normative idea of national innovation by dedicating research to cross-cutting themes **SE** + Culture of security awareness links technological with societal (e.g. education) factors/instruments	**AT** - Ministry of Transport, Innovation and Technology as the owner of the national security research programme favours technology themes; security research politically seen as opening up a security market for domestic enterprises and industries **FR** - Sûreté tradition/culture causes on overemphasis on the societal (as opposed to the technical) dimension **DE** - Security interpreted as a task on the level of the state organization as a whole/as a government matter in the sense of civil protection **NL** + Security interpreted as a task on the level of the state organization as a whole, including societal stakeholders **ES** - Security (research) mainly interpreted in terms of science and technology **SE** - Security often interpreted as crisis management in the sense of civil protection and emergency management	**AT** **FR** + Security as a symbol for crisis management in a broad sense, independent from the source of origin (such as natural, man-made and others) **DE** **NL** **ES** **SE** **UK** - Homeland security symbolism favours science and technology cooperation and critical infrastructure protection **NO** - Critical information and communication infrastructure as a	**AT** **FR** **DE** - Cold war front state legacy leads to an over-emphasis of civil protection practices **NL** **ES** **SE** **UK** **NO** - Nurturing a culture of security in the sector of critical information and communication technology **IT** - Importing and exporting technical-

	UK **NO** - Culture of security (prevention) in the sector of critical information and communication technology is a leading value for security (research) policy making **IT**	+ Association of low a rate of poverty and social exclusion with a high crime rate makes security awareness a significant issue **UK** + Combating terrorism is interpreted as a comprehensive task, including politics, public, technology, applied sciences and academia **NO** - Security commonly interpreted as information security **IT** - Cognitive approach directed at comprehensive risk information and assessment, but centred on the scientific (technological) dimension	cultural symbol of national security **IT**	scientific knowledge for comprehensive risk assessment - Practical concern with organized crime promotes electronic surveillance/concentration on technological solutions

Matrix 2: Overall assessment of evidence for the four big cultural factors (integration of country-related ratings from matrix 1)

	Cultural factors (can) reduce gap / are part of the solution				Cultural factors produce gap / are part of the problem			
	Model I	**Model II**	**Model III**	**Model IV**	**Model I**	**Model II**	**Model III**	**Model IV**
Potential for a comprehensive approach at the national level	AT, FR, NL, NO, ES, IT, UK	AT, FR, NL, SE, UK, IT	FR, DE, UK, IT	AT, IT, UK	DE, SE	DE, ES, NO	AT, ES	DE, NO
	7	6	4	3	2	3	2	2
Potential for a comprehensive approach at the European level	AT	IT, NO, SE, ES	IT	AT, FR, IT, NL, NO, UK	DE, NO, SE, UK	AT, FR, DE, NL, UK	AT, DE, NO	DE, IT, ES
	1	4	1	6	4	5	3	3
Overcoming the lack of a comparable set of security strategies and approaches to security governance (coordination vs. standardisation), including the improvement of coordination of national security research and foresight activities with European-level research programmes	FR	IT, NO, SE, UK		SE, UK, IT	AT, DE, UK, NO	AT, DE, NL, NO	AT, FR, DE, ES	DE
	1	4	1	3	4	4	4	1
Overcoming the split in thematic thrust (society vs. technology), with a tendency to favour technological solutions to security problems	SE, ES	NL, SE, UK	FR		AT, FR, NO	AT, FR, DE, ES, SE, NO, IT	UK, NO	DE, NO, IT
	2	3	1	-	3	7	2	3
Sum	11	**17**	7	12	13	**19**	11	9

Matrix 3: Cultural factor/model for which most evidence was found per country

Country	Main factor(s) reducing gaps	Main factor(s) producing gaps
AT	I / Normative values	II / Knowledge/Interpretation

	IV / Action repertories	III / Common symbols
FR	I / Normative values III / Common symbols	II / Knowledge/Interpretation
DE	III / Common symbols	II / Knowledge/Interpretation IV / Action repertories
ES	I / Normative values	II / Knowledge/Interpretation III / Common symbols
IT	II / Knowledge/Interpretation IV/ Action repertories	IV / Action repertories
NL	II / Knowledge/Interpretation	
NO	II / Knowledge/Interpretation	
SE	II / Knowledge/Interpretation	I / Normative values
UK	II / Knowledge/Interpretation IV / Action repertories	I / Normative values
Mode	II / Knowledge/Interpretation	

Matrix 4: Cultural factor summarized evidence of impact on the four types of gap, per country

Country	Comprehensive approach at national level	Comprehensive approach at European level	Lack of comparable security strategies and approaches to governance	Split in thematic thrust	*Sum of overall cultural effect on gaps*
AT	+	0	-	-	- -
FR	+	0	0	-	0
DE	-	-	-	-	- - - -
ES	-	0	-	0	-
IT	+	+	+	-	+ +
NL	+	0	-	+	+
NO	-	0	-	-	- - -
SE	0	0	+	+	++
UK	+	-	+	0	+
Sum	+ +	-	- -	- - -	- - - -

Majority of related entries in matrix 2;

"+" positive (part of solution), "-" negative (part of problem), "0" neutral evidence of summarized impact of all four cultural factors on type of gap

Annex 3: National Matrix: Priorities and Governance Pattern (Overall Co-ordination v. Standardisation)

	Security of Citizen	Security of Critical Infrastructure	Border Security	Crisis Management	Transverse issues: standardisation interoperability
Italy	Strategic natural disaster reduction/enhancement of preparedness and rapid response civil protection action, both based on comprehensive risk assessment by real-time early warning			- Prevision and risk reduction, linking up local, regional and national authorities as well as expertise from the technical and scientific side. - Reactive dimension	international import and export of scientific (technological) knowledge.
Norway	Critical ICT social infrastructure				Contribute to international development of standards within information security
UK	Conventional crime/violence	Protection against terrorist attacks			U.S. government, esp. on science and technology cooperation for CIP and Homeland Security as well as agency, industry and academia co-operation on Com-
Sweden	**Network based solutions:** - Mobile and integrated telecommunication - Biotechnology - Information technology - Sensors - Information systems in a broad sense - Detection of biological and chemical substances				Support of industry participation in U.S. security research programmes
Spain	**National R&D&I Plan** Critical ICT				Focus on national innovation; governed by the Inter-Ministerial Commission for Science and Tech-0no-logy; facilitation of access to inter-national projects
Netherlands	**National security programme** - climate change; - polarisation and radicalisation; - energy supply assurance				National approach to be aligned of that of other states and organizations
Germany	- Protection and rescue of people - Protections of transport infrastructures - Protection against failure of the supply infrastructures and securing the supply chains.		Biometrics	- ICT - Prevention and response strategies and organisational forms	Focus on inter-ministerial rather than international standardisation/ cooperation. Joint development of the research programme by the ministries of research, science and business
France	-Conventional crime/violence - Protection of vital infrastructures and networks		Land, sea, air flow management of goods and immaterial goods	Crisis management whatever its origin (malicious intent, natural or accidental catastrophe)	National focus; joint development of the security research programme by the National Research Agency, the General Delegation for Armament and General Direction of the National Police
Austria	**KIRAS** - Public authorities and security - Energy - Traffic and transport - Water and health				National focus; compulsory inclusion of humanities and social science aspects in all funding proposals

	Austria	France	Germany	Italy	Netherlands	Norway	Spain	Sweden	UK
Method of governance	Coordination	Coordination	Coordination	Coordination	Standardisation	Standardisation	Coordination	Standardisation	Standardisation
Locus of governance	Ministry	Research agency	Ministry	State organization as a whole	Ministry	Inter-ministerial/ inter-agency	Inter-ministerial	First-responder Agency	Ministry
Focus	National, Pluralistic analysis	National	National/ inter-ministerial	Local-regional-central link-up; import and export of scientific expertise	International link-up	Trans-national	National/ inter-ministerial	Cooperation with U.S.	Cooperation with U.S.
Responsibility	Ministry of Transport, Innovation and Technology; Convenes Steering Committee with representatives from all relevant ministries	Agence Nationale de la Recherche (in partnership with the General Delegation for Armament and the General Direction of the National Police	Ministry of Science	President of the Council of Ministers, Civil Protection Department	Ministry of the Interior and Kingdom Relations	Information Security Coordination Council; established by the Ministry of Government Administration and Reform, with members from seventeen ministries, directorates and government agencies	Inter-ministerial Commission for Science and Technology, with representatives from all ministries with an interest in science and technology	Swedish Emergency Management Agency	Home Office, Office for Security and Counter-Terrorism

Annex 4: European Matrix

This matrix presents examples of key topics and projects, and potential synergies for joint programmes and budgets)

	European Commission (FP7 Security)	**European Commission (Other FP7 themes, other DGs and programmes)**	**European Community Agencies (FRONTEX, EMSA, ENISA…)**	**EDA OCCAR**	**ESA**	**Eurocontrol**	**NATO**
Security of the citizens	X Supply chain security CBRNE	X DG SANCO DJ JLS fundamental rights programmes Galileo, GMES		X Biological defence	X GMES		X Counter IED
Security of infrastructures and utilities	X Mass transportation security (rail, airport…)	X DG JLS EPCIP FP7 ICT – security SESAR, ERTMS, SIS-II, European Space Policy	X FRONTEX Airport /check points security ENISA	X Space surveillance	X Space Surveillance Space infrastructure	X ATM / SESAR	X Energy security
Intelligent surveillance and border security	X Maritime Surveillance Port security Land border	X EUROSUR GMES	X FRONTEX Bortec and Medsea studies CLEANSEANET SAFESEANET	X Maritime Surveillance	X Maritime Surveillance	X UAVs insertion into	X Maritime Situational Awareness Port security

	UAVs	UAVs	UAVs	UAVs	Links space – UAVs	ATM	UAVs
Restoring security and safety in case of crisis	X First responder SDR	X ECHO, DG RELEX ESDP operations Helicopters	X FRONTEX joint operations	X Support to operations (helicopters…) SDR/ESSOR	X Support to crisis management		X NATO operations Helicopters
Transverse issues (standardisation, interoperability, etc.)	X Studies on standards, interoperability, market and procurement issues	X CEN ICT standards Market and procurement	X Border control standards	X Standardisation ICET	X Standardisation	X Standardisation	X STANAG

Annex 5: Abbreviations

This report employs the following abbreviations:

Abbreviation	Expansion
AAP	Allied Administrative Publication
ASD	AeroSpace and Defence (Industries Association of Europe)
ATM	Air Traffic Management
C3	Command Control and Communications
CBRN	Chemical, Biological, Radiological and Nuclear
CDP	Capability Development Plan
CEN	Centre européen de normalisation (European Centre for Norms)
CoE	Concept of Employment
CSCP	Common Security Capability Plan
DG	Directorate General
EC	European Community
ECHO	European Commission Humanitarian Aid Office
EDA	European Defence Agency
EDRT	European Defence Research and Technology
EDTIB	European Defence Technology and Industry Base
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
EPCIP	European Programme on Critical Infrastructures Protection
ERTMS	European Rail Trafficking Management System
ESA	European Space Agency
ESDP	European Security and Defence policy
ESRIA	European Science Research and Innovation Agenda
ESRIF	European Science Research and Innovation Forum
ESS	European Security Strategy
EU	European Union
FP	Framework Programme (Research & Development)
FRONTEX	Frontières Extérieures (External Borders)
GMES	Global Monitoring for Environment and Security
ICET	Innovative Common Emerging Technologies
ICT	Information and Communication Technologies
IED	Improvised Explosives Devices
IPSC	Institute for the Protection and Security of the Citizen
ISO	International Standards Organisation,

IT	Initial Tranche
JLS	Justice, Liberty, Security
JSCP	Joint Security Capability Plan
NATO	North Atlantic Treaty Organisation
PCRD	Programme-Cadre de Recherche et de Développement
PMS	Permanent Member State
RELEX	Relations Extérieures (External Relations)
SDR	Software Defined Radio
SESAR	Single European Sky ATM Research Programme
SIS	Schengen Information System
SRP	Security Research Plan
STANAG	Standardisation Agreement
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
WG	Working Group

Working Group 11: Human and Societal Dynamics of Security

Policy References

BERNHARD Christiane: Public private dialogue in security research. Directorate General Internal Policies of the Union. Policy Department C.

BOIN Arjen, 'THART Paul, STERN Eric, SUNDELIUS Bengt: The Politics of Crisis Management; Public Leadership under Pressure, Cambridge: Cambridge University Press, 2005.

BOIN Arjen, MCCONNELL Allan, THART Paul ´: Governing after Crisis; The Politics of Investigation, Accountability and Learning, Cambridge: Cambridge University Press, 2008.

BUZAN Barry, Ole Waever, Jepp de Wilde: Security: a new framework for analysis, London: Lynne Rienner, 1998.

DAVID Charles-Philippe, and Jean-Jacques ROCHE: Théories De La Sécurité. Définitions, Approches Et Concepts De La Sécurite Internationale. Paris: Montchrestien, 2002.

FREY B.: Blood and Ink: The Common-interest Game Between Terrorists and the Media Public Choice, 2007.

FREY B.: Protecting Cultural Monuments Against Terrorism. Defence and Peace Economics, 2007.

GIBSON Ed: "Tales of Two Cities - the Administrative Facade of Social Security." Administration & Society 35, no. 4 (2003): 408-37.

HAMILTON Donald, SUNDELIUS Bengt, GRONVALL Jesper: Protecting the Homeland: European Approaches to Societal Security, Washington, D.C., Johns Hopkins University, 2005.

JOHANSSON Anna C. H, SVEDUNG Inge, and ANDERSSON Ragnar: "Management of Risks"

MØLLER Bjørn: "Freshwater Sources, Security and Conflict: An Overview of Linkages."Copenhagen: DIIS, 2004.

NAJAM Adil: "The Human Dimensions of Environmental Insecurity: Some Insights from South Asia." ECSP report, no. 9 (2003): 59–73.

PARTHASARATHI A.: "Science and Its Applications to Societal Security." Current Science 87, no. 9 (2004): 1174-75.

Societal Planning - an Analysis of Scope and Variety of Health, Safety and Security IssuesMunicipality Plan Documents." Safety Science 44, no. 8 (2006): 675-88.

TURNER Barry, Nic Pidgeon: Man-made Disasters, London; Butterworth Heinemann, 1997.

WILDAVSKY Aaron: Searching for Safety, Berkeley; University of California Press, 1988.

EU-COMMISSIONED STUDIES ON RADICALISATION:

Les facteurs de création ou de modification des processus de radicalisation violente, chez les jeunes in particulier by Compagnie Européenne d'Intelligence Stratégique (CEIS), Paris.

http://ec.europa.eu/justice_home/fsj/terrorism/prevention/docs/ec_radicalisation_study_on_trigger_factors_fr.pdf

Beliefs, ideologies and narratives by The Change Institute, London.

http://ec.europa.eu/justice_home/fsj/terrorism/prevention/docs/ec_radicalisation_study_on_ideology_and_narrative_en.pdf

Recruitment and Mobilisation for the Islamist Militant Movement in Europe by King's College, London.

http://ec.europa.eu/justice_home/fsj/terrorism/prevention/docs/ec_radicalisation_study_on_mobilisation_tactics_en.pdf

Best practices in cooperation initiatives between authorities and civil society with a view to the prevention of and response to violent radicalisation by The Change Institute, London.

http://ec.europa.eu/justice_home/fsj/terrorism/prevention/docs/ecvr_best_practice_core_report_en.pdf

BECK Urban: Risk Society: Toward a new modernity, London: Sage Publications, 1992.

BILGIN Pinar: "Individual and Societal Dimensions of Security." International Studies Review 5 (2003): 203–22.

BJORGO Tore and HORGAN John (eds), *Leaving Terrorism Behind: Individual and Collective Disengagement* (Routledge, 2009)

BOVENS Martin, Paul ´THART: Understanding Policy Fiascoes, New Brunswick: Transactions Publisher, 1996.

BRAUCH Hans Günter: Security and Environment in the Mediterranean : Conceptualising Security and Environmental Conflicts. New York: Springer, 2003.

BROZSKA Michael: Internal and external dimensions of the EUs counter-terrorism policy (email attachment).

BRUECK Tilman: A survey on the Economics of Security. DIW Berlin: Politikberatung kompakt 41, 2008.

BURGESS J. Peter: "Social Values and Material Threat. The European Programme for Critical Infrastructures Protection." International Journal of Critical Infrastructures 3, no. 3/4 (2007): 471-86.

BURGESS J. Peter: "L'éthique politique du principe de Précaution." edited by Unpublished manuscript, 2007.

BURGESS J. Peter: "Human Values and Security Technologies." Oslo: International Peace Research Institute, Oslo (PRIO), 2008.

BURGESS J. Peter: "Security as Ethics." Oslo: International Peace Research Institute, Oslo (PRIO), 2008.

CAS Johann: Comments on the Esrif Interim report (email July 8 2008)

COOLSAET Ric (ed), *Jihadi Terrorism and the Radicalisation Challenge in Europe* (Ashgate, 2008)

CUNNINGHAM Karla J.: "Cross-Regional Trends in Female Terrorism." Studies in Conflict and Terrorism 26, no. 3 (2003): 171–95.

DIEU François, ed.: Questions De Sécurité: Sociétalisation Des Réponses, Globalisation Des Menaces. Paris: l'Harmattan, 2006.

ERIKSSON Johan: Threat Politics: new perspectives on security, risk and crisis management, Aldershot: Ashgate Publishing, 2001.

FLIN Rhoda: Incident Command: Tales from the hot seat, Aldershot: Ashgate Publishing, 2002.

FOSTER Gregory D: "Environmental Security: The Search for Strategic Legitimacy." Armed Forces & Society 27, no. 3 (2001): 373-+.

GLEICK Peter H: "Water and Terrorism." Water Policy 8 (2006): 481–503.

HAAS Michael: "Societal Approaches to the Study of War." Journal of Peace Research 2, no. 4 (1965): 307–23.

HELLMAN Maria and OLSSON Eva-Karin: The significance of Media and Communication for the field of crisis and security studies. Report to WG11, 2008.

HERD Graeme P. & LÖFGREN Joan: "'Societal Security', the Baltic States and Eu Integration." Cooperation and Conflict 36, no. 3 (2001): 273-96.

HUYSMANS Jef: "Migrants as a Security Problem: Dangers of Securitising Societal Issues." In Migration and European Integration: The Dynamics of Inclusion and Exclusion, edited by R. Miles and D. Thränhardt. London: Pinter, 1995.

HUYSMANS Jef: "Migrants as a Security Problem: Dangers of 'Securitizing' Societal Issues." In Migration and

European Integration: The Dynamics of Inclusin and Exlusion, edited by Robert Miles and Dietrich Thänhardt. London: Pinter, 1995.

HUYSMANS Jef: "Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security." Alternatives 27 (2002).

KELSTRUP Morten: "Societal Aspects of European Security." In Euroepan Security--2001, edited by Birthe Hansen, 172-97. Copenhagen: Copenhagen Political Studies Press, Nadar Elhefnawy: "Societal Complexity and Diminishing Returns in Security." International Security 29, no. 1 (2004): 152-74.

LEVASHOV Viktor K: "Globalization and Social Security." Sotsiologicheskie Issledovaniya, no. 3 (2002): 19-32.

National Research Council: Facing Hazards and Disasters; Understanding Human Dimensions, Washington, D.C.: The National Academies Press, 2006.

MASON Stephen: Books on digital evidence for lawyers. General Editor, Digital Evidence and Electronic Signature Law Review. http://www.deaeslr.org

MURESAN Liviu: http://www.stockholmresilience.org/researchbackground

OSBERG Lars & Andrew Sharpe: "An Index of Economic Well-Being for Selected OECD Countries." Review of Income and Wealth, no. 3 (2002): 291-316.

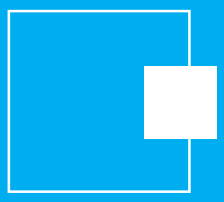
PATRA James: "Building Process of Science for Societal Security." Current Science 88, no. 1 (2005): 7-7.

The PRISE project: http://prise.oeaw.ac.at

RANSTORP Magnus (ed), *Understanding Violent Radicalisation* (Routledge, 2009)

ROSENTHAL Uri, Arjen BOIN, Louise COMFORT: Managing Crises: Threats, Dilemmas, Opportunities, Springfield; Charles Thomas, 2001.

SORELL Tom: http://www.globalethics.bham.ac.uk





ISBN 978-92-79-13025-0