

► 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.

► 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.

► 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.

► SECURITY RESEARCH: THE FUTURE

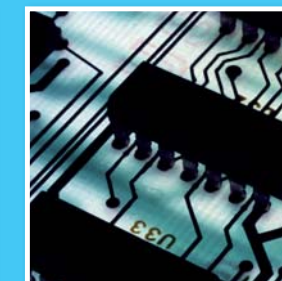
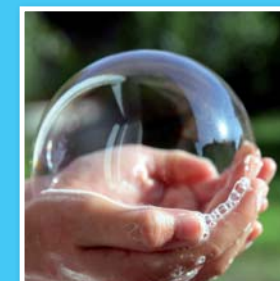
The proposed European Security Research and Innovation Agenda – ESRIA – should be seen as a living document.

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.

www.esrif.eu

ESRIF Final Report Executive Summary



Europe stands on the threshold of a **new global approach to security** – and of ways to use scientific research and innovation to reinforce and implement that new thinking.

The security of Europe and its citizens is linked to internal and external events and threats, as well as to the increasing convergence of civil and defence capabilities. Above all, it derives from societal imperatives that demand a balancing of the state's policy and technological exigencies with privacy rights, European cultural values and the tenets of democracy.

ESRIF, the European Security Research and Innovation Forum, has spent the past two years analyzing the medium and long-term challenges that Europe faces. These range from natural disasters to organised crime to man-made incidents, whether small-scale in impact or those with potential "mass disruption" effects.

Assisted by more than 600 experts, ESRIF and its 64 members from 31 countries have examined the full range of such threats and tied them to the EU's central civil security missions and to the capabilities required to carry them out.

A research and innovation agenda cannot be created and implemented in a vacuum. The framework is defined by principles given in the **Key Messages:**

- ▶ **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 must 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 fore front.

This collective effort has resulted in a set of key messages that encompass the logic and necessity of future European security and its related research. These messages point to the essence, as ESRIF sees it, of what security research and innovation should flow from – and what it should deliver to society.

Security research should be grounded in an industrial policy that frames a systematic approach to capability development which, in turn, promotes interoperability among the 27 EU nations and establishes common standards. Ultimately this effort must increase societal security in a globalised world, while fostering trust between European citizens, governments and national and European institutions. These and other ideas are among ESRIF's main recommendations included in this executive summary.

To reach an interoperable, trust-embedded and resilient society, however, Europe needs an R&D roadmap, and a mechanism should be set up to implement it in a balanced and rigorous manner. ESRIF thus proposes its European Security Research and Innovation Agenda – "ESRIA" which should go a long way toward achieving that goal.

- ▶ **Innovation**
Europe can only rely on its own scientific, technological and industrial competences.
- ▶ **Industrial policy**
A competitive European security industry is a prerequisite for future security. The EU must address the fragmentation of its security markets.
- ▶ **Interoperability**
A seamless approach to security is essential for Europe; Interoperability is essential to allow security forces to work together.
- ▶ **A systematic approach to capability development**
The increasing complexity of security, demands increasing sophistication of our Response.
- ▶ **Security by design**
Security features must become integral part of any given system: Europe's society needs a systemic approach to security.

ESRIF has defined a **European Security Research and Innovation Agenda (ESRIA)** that identifies and roadmaps key capabilities and research needs in line with the main work results.

The ESRIA has been organized into five content clusters and differentiates research topics according to short-, medium- or long-term needs.

The first cluster centres on the classic **security cycle preventing, protecting, preparing, responding and recovering**. It focuses on the securing of people, civil preparedness and crisis management.

The second cluster deals with the **countering of different means of attack**, as a way of dealing with specific, known and projected future risks. It examines ways to detect and identify conventional as well as non-conventional attacks, unintended impacts of other actions, and naturally

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:**

▶ 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 stake-

holders 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.

The third cluster aims at **securing critical assets**, such as energy, transport and other crucial infrastructures. It examines security economics and outlines the necessity to analyze and cope with limited access to critical natural resources as well as securing the existence of key manufacturing capabilities and capacities in Europe.

The fourth cluster is about **securing identity, access and movement of people and goods**. It mainly centres on border security and secure identity management.

Lastly, the fifth cluster lists **cross-cutting enablers** of special interest, due to cross-cutting characteristics or prior political strategic decisions. The crucial role of Information and Communication Technologies (ICT) is examined, as are security implications of European space programmes.

holders 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.