**H4 33074 PE European Security Research and Innovation Agenda**

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 21.12.2009
COM(2009)691 final

**COMMUNICATION FROM THE COMMISSION**

**"A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations"**

EN

**COMMUNICATION FROM THE COMMISSION**

**A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations"**

## 1. INTRODUCTION

One of the EU's main objectives is to preserve and develop the European values of justice, freedom, and security whilst addressing the increasingly complex security challenges.

The fight against terrorism and organised crime, the protection of the external European borders and civil crisis management have gained importance in our daily life. Climate change, if not properly addressed, could lead to major destabilizing effects at global scale. At the same time internal and external security are increasingly inseparable. Addressing them requires the use of modern technology.

Since security technologies are becoming more and more present in modern societies prompting at times concerns on the part of citizens, it is imperative to ensure ethical scrutiny and transparency of security research and development projects. Our security must be based on our European values. And, vice versa, security solutions are needed to protect our societal values.

Addressing these concerns in the years to come will require better understanding the interplay between the human and natural factors which may create security risks which is also often crucial to shape effective responses, alongside the use of modern technology and innovative solutions.

The Commission considered that in order to find the most effective solutions to these challenges it was indispensable to bring together representatives from industry, public and private end-users, research establishments and universities, as well as non-governmental organizations and EU bodies. In 2007, it therefore proposed together with Member States the establishment of the "European Security Research and innovation Forum" - ESRIF[1].

It was charged with developing a 'Security Research and Innovation Agenda' for the EU: a strategic roadmap for security research and innovation aimed at bringing greater coherence and efficiency to this area encompassing the EU, national and regional levels. It focuses beyond Research and Development putting the Innovation "I" into the European Agenda. Its orientation towards innovation and implementation of security technologies turned out to be even more important in the current context of global environmental and economic challenges.

On 23rd November ESRIF adopted its key findings and recommendations (for more information on ESRIF and its approach see also the attached Executive Summary of the ESRIF Final Report).

[1] COM (2007) 511 Final.

This Communication presents the **Commission's initial reaction to ESRIF's key findings and recommendations.**

## 2. SOCIETAL DIMENSION OF SECURITY

ESRIF rightly based its approach to security research on the perspective that security is first and foremost human and societal. People are not only the targets and victims of attacks and security threats, but also the rescuers, decision makers and those who respond to situations of insecurity.

To tackle these challenges, all security solutions must be founded on the European values of freedom and justice and fundamental ethical principles and legal requirements mainstreamed through all security R&D and innovation activities. This means:

a) Reinforcing the legal and ethical dimension

There can be no security measures without taking into account the respect for the rights and freedoms of individuals, especially for the protection of citizens' privacy. Security measures must be legitimate and proportionate in order to gain societal acceptance and always applied in accordance with the rule of law. Fundamental ethical principles and data protection requirements of security measures must be the foundation for developing and implementing security programmes. ESRIF advocates that privacy related requirements should feature alongside those of security enhancement requirements from the earliest stage of consideration of new security solutions. It calls this "Privacy by design".

Such an approach, which is welcomed by the Commission, will have profound consequences across the whole research and innovation cycle.

b) Reinforcing the societal dimension

A further societal dimension needs to be taken into account from the standpoint of effectiveness of the technologies. No security technology can in fact be a security solution in the long term without the active participation (and acceptance) by the public at large. Indeed ESRIF argues that a societal security approach implies a vision of security that does not focus on prevention and protection at all costs but rather, features in the capacity of our societies to face risks, and at times losses, and to recover from them. Such a "societal resilience" depends on the free will of informed citizens as much as on the quality of technical systems and on business continuity capabilities of companies and administrations.

To achieve resilience, specific programmes are required that reach out to the wider public, to raise awareness of threats, to improve understanding of the processes put in place to tackle challenges and also to debate acceptability of security solutions. Specific initiatives involving the media are a priority. Consistent with the ESRIF report, further research on the relation between new technologies and civil and human rights is required.

## 3. IMPROVING THE COMPETITIVENESS OF THE EUROPEAN SECURITY INDUSTRY

The EU security industry with an estimated market value in 2008 ranging from 26 to 36 billion Euro[2] is growing rapidly with a highly skilled labour force and a high R&D content. ESRIF recommends the pursuit of 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". It recommends that the EU should reach out for leadership in the security market, endorsing the idea of a Lead Market Initiative in the Security Sector.

This requires however investing now in an ambitious industrial policy for the security sector, in order to harvest innovation and growth tomorrow:

a) Overcoming market fragmentation

The security industry in Europe needs to become more competitive and efficient. Up to now the industry suffered from the fragmentation of the markets that lead them to be nationally or even regionally oriented. Their small size led to inefficiency and poor cost-effectiveness both for the industry and the end users. It is an important hurdle towards interoperability and integration of security solutions at national and European level. Tackling that issue by creating European wide markets will make this industry more competitive and attractive at global level and lead to more efficient public spending.

(i) Certification, validation and standardisation

Based on the requirements of the end-users and the results of research, new technologies and solutions need not only to be validated; they should also be certified and where appropriate standardised, so they can become part of an effective response to security threats. R&D activities should be linked to a clear validation and procurement strategy that takes into account the relevant policy issues as well as economic interests. This should promote the creation of a European security market and better cooperation among security stakeholders at national and European levels. ESRIF recommends that the Commission should evaluate the applicability and efficacy of a "European Security Label".

CEN and ETSI[3] have started working on standardisation in the area of security. CEN is initially concentrating on a number of issues for which it has received standardisation mandates (notably on supply chain security, critical infrastructure protection, and proofing products against crime). As standards can be an effective means for transferring research findings into innovative products, it is expected that work carried out in the 7th Framework Programme will lead to further standardisation. This work needs to be accelerated.

---

2 Security industry encompasses traditional security industry (based around the supply of general security applications such as e.g. physical access control), security-orientated defence industry (based on the utilisation of defence technologies in security applications or through acquisition and conversion of civilian technologies to security applications), as well as new entrants, i.e. mainly companies extending their existing (civilian) technologies to security applications, such as for example IT companies.

3 http://www.cen.eu/CENORM/sectors/sectors/security+and+defence/security/index.asp
http://www.etsi.org/WebSite/Technologies/Security.aspx

Meanwhile, the Commission is exploring ways in which the results of relevant research actions could be tested in view of developing future certification mechanisms. Such mechanisms should aim at certifying that security products and processes are in conformity with relevant standards.

(ii) Regulatory framework

ESRIF has underlined that given the fragmentation of the security market, often due to diverging national legislation, a harmonised regulatory framework in specific areas combined with upstream coordination would be advisable. The Commission considers that as a first step, a thorough analysis of the existing regulatory framework is needed.

(iii) Interoperability

Sharing of assets and information strengthens our ability to handle complex and cross-border security issues. Exchange of information between national authorities and other European players is vital for the fight against cross-border crime. However, today such exchange and sharing of information is hampered due to a lack of technical and organisational interoperability. There is, therefore, an urgent need for the development of interoperability standards.

b) Strengthening the industrial base

The European Union needs a strong industrial and technological base to provide the citizens in the EU and abroad with modern security solutions. The following issues need to be addressed in order to strengthen the European security industrial and technology base:

(i) Mapping the security industrial base

In order to get a precise picture of the European Security Technological and Industrial Base (ESTIB), it is important to map these competences. Such a mapping will allow the identification of the strengths and weaknesses of the ESTIB, and will allow the identification of appropriate measures with a view to strengthening the ESTIB. Particular attention should be paid to SMEs. "Critical manufacturing" sectors (such as for example electrical equipment manufacturing, etc.) – which play a similar role in manufacturing as critical infrastructure does in the infrastructure world - should also be highlighted.

(ii) Innovation policy

Innovation policy focuses on transforming knowledge into new products and methods, and at the same time into economic value and commercial success[4]. This is particularly relevant for security R&D. The Commission will therefore analyse how far the most innovative security sectors should be brought into the Lead Market Initiative.

[4] COM (2005) 488 final.

Furthermore, pre-commercial procurement is a useful tool in order to foster the procurement of innovative products and technologies[5]. The Commission will further analyse how to speed up pre-commercial procurement in the security domain. As regards public procurement, Directive 2009/81/EC[6] applies equally to the supply of defence equipment and sensitive equipment. The Commission will suggest ways to ensure that this Directive is applied in a transparent and harmonised manner in the security domain.

(iii) Security by Design

ESRIF recommends "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"*.

The Commission welcomes this Recommendation and will examine ways to ensure, whenever appropriate that Research activities with potential security effects take these in consideration from the earliest stages.

(iv) Synergies between civil and defence technologies

The evolving nature of the relationship between defence technologies on the one hand, and security technologies on the other, is particularly noticeable in the field of R&D, with technologies that show potential developments in both areas.

There is a need to strengthen complementarity and co-operation in specific areas where technologies can have civil and defence applications including in the border control and cybersecurity domains. Based on a call endorsed by the December 2008 European Council to further strengthen the synergies between activities conducted under the framework R&D programme and the defence domain, close cooperation with the European Defence Agency (EDA) needs to be ensured.

## 4. INVESTING INTO THE FUTURE

ESRIF has laid out in its European Security Research and Innovation Agenda (ESRIA) a security R&D roadmap for the next 15 years, including also systemic requirements. A distinction needs to be made between R&D measures and measures aimed at ensuring that technology advances made through R&D lead to the actual deployment of that new technology:

a) R&D security missions and priorities

In terms of R&D, ESRIF underlined that the main research in support of the security missions identified under FP7 remains valid for the immediate future. In the longer run they need to be reappraised and possibly strengthened and amplified.

ESRIF underlined that it is not possible to fully predict threats to Europe's security be they manmade or natural. Therefore security R&D needs to focus on strengthening Europe's

[5] COM (2007) 799 final.
[6] OJ L 216 of 20.8.2009.

resilience to threats and its ability to efficiently recover from crises. This includes also enhancing the cohesiveness and robustness of societal systems and their interface with technologies. In this context, ESRIF recommended that research on critical infrastructure protection needs to be strengthened and amplified, for example with regard to energy security research, transport network security[7].

(i) Evolving priorities

The European Security Research and Innovation Agenda covers the full spectrum of R&D support to current security missions. It is grouped in five clusters (see Executive Summary of ESRIF in Annex).

The Commission notes the emphasis given by ESRIF to an integrative approach across the whole of ESRIA. Whether referring to explosives or CBRN, critical infrastructures or crisis management, ESRIA focuses on the whole rather than the parts, highlighting the importance of networks, reference centres, interoperability, and system-of-systems solutions. Indeed, ESRIF recommends for instance preparing "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".

It advocates innovation underpinning a "holistic approach" to border management, which has in fact been developed by the EU and its Members States in the Schengen four-tier access control model[8], which forms the core of Integrated Border management. ESRIF highlights the importance of interoperability considering that "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".

It considers that 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" referring notably to the need of research to increase systemic resilience. ESRIF advocates research into legal frameworks to support forensic and evidence gathering in the ICT environment.

ESRIF has identified the role of space as "vital in different security-related technological domains" and pointed out the importance of GMES and Galileo in providing "a wide range of added value services in support of security" referring the need to protect space assets.

The Commission welcomes this comprehensive approach to security research and innovation.

(ii) Future missions

---

7 See also the related Council Directive 2008/114/EC.

8 The four tiers are: measures in third countries, cooperation with neighbouring countries, border control management and control measures within the area of free movement, including return.

Several of the security missions which were analysed by ESRIF in terms of their required capabilities and related research efforts are under active consideration. That is the case, inter alia, of border management and controls, of critical infrastructure protection including ICT, CBRN security policy, measures to enhance the security of explosives and detonators or the screening of goods and passengers. These security areas will further be defined in the future Stockholm Action Plan.

ICT security challenges are situated in different policy areas, and are to be addressed accordingly in the context of the information system architecture for the future EU internal security strategy.

ESRIF acknowledged that its mandate excluded research topics which are bound to grow in importance over coming years. This relates notably to some external security missions. ESRIF recommended "giving high priority to security's external dimension" considering that "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".

The Commission considers that while indeed these are evolving domains, it is appropriate to deepen the reflection on broadening security research and development programmes to such areas as civil protection and conflict prevention and post crisis stabilisation.

– Civil protection: civil protection and thus security research to underpin civil protection activities are prone to gain importance, not least in the light of climate change, as laid out in a paper from the High Representative and the European Commission to the European Council, in which climate change is described as a "threat multiplier"[9]. The paper calls for intensifying EU research capacities with regard to the link between security and climate change. Moreover, in its Communication on "Reinforcing the Union's Disaster Response Capacity", the Commission emphasised the need for improving disaster prevention, mitigation, the European civil protection response capacity, and the valuable support that research can provide.

– Conflict prevention and post crisis stabilisation: the Community has already operational funding in place via the Instrument for Stability[10]. It aims at establishing or re-establishing conditions essential to the proper implementation of the Community's development policies in case of crisis or emerging crisis, as well as to help building capacity to address specific global and trans-regional threats, as well as ensuring pre-and post-crisis preparedness building. However, research funding to support these activities is missing at Community level.

b) Beyond research and development

(i) End user involvement

---

9 See 7249/08, 03.03.2008. See also the Commission's Communication on "Reinforcing the Union's Disaster Response Capacity (COM(2008) 130 final.

10 Regulation (EC) No. 1717/2006, OJ L 327, p.1, 24.11.2006.

While recommending "*close consultation across Europe* among supply, demand and end-user stakeholders across the planning, execution and review cycles of security research policy" ESRIF identified the need for governments and end-users – to undertake "organisational re-alignment to both shape and respond to security innovation".

The Commission agrees there is often a need for an added effort on the part of security end-users, both public and private, to strengthen their security technology knowledge base and prospective analysis capabilities, to be in a position to fully seize the opportunity to ensure future solutions will be tailored to their real needs, for example through demonstration models.

(ii) Future programmes to disseminate innovative solutions

The Commission already indicated the usefulness of investing in the operational aspects of security, in particular for a number of areas where national and international authorities use technology solutions[11]. ESRIF considers that success in the global market strongly depends on EU market procurement references, and recommends that pre-commercial procurement of innovative solutions should be exploited.

ESRIF supports developing a model based on a strategic and coordinated approach to trans-European cooperation. It refers to the Trans-European Networks as an example which should be considered as a reference for the EU wide systemic integration in the Security area. Like for the TEN, funding would be provided to top up national funds to secure European critical infrastructure. Considering that the resources available for research and technological development must be harnessed to respond fully to users' expectations, ESRIF noted that such a process may be supported by setting up an Internal Security Fund.

(iii) Education and training

ESRIF highlighted the importance of linking research education and training considering it a responsibility of all stakeholders: security officers, policy makers, law enforcement agencies, civic society, industry, research organisations, academia and the media. It advocated new awareness raising programmes addressing 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.

## 5. IMPLEMENTING THE EUROPEAN SECURITY RESEARCH INNOVATION AGENDA

ESRIF's recommendations relating to governance look at how to keep the ESRIA up-to-date and how to involve all relevant stakeholders more closely. ESRIF recommends that *a transparent mechanism involving all stakeholders should be set up to implement ESRIA in a balanced and rigorous manner.*

[11] COM(2008) 68 final, COM(2008) 130 final, COM (2009) 262 Final.

As security research is user-oriented and capability driven, ESRIF notes that there is a need for adequate interfaces and exchange mechanisms between the end-user community and the research and industrial community.

## 6. CONCLUSION

This is a preliminary reaction of the Commission to the ESRIF final report. The Commission considers the results of the work of ESRIF as being important and welcomes its strategic orientation. It takes note of its recommendations and highlights the following topics that the next Commission might wish to consider to analyse further:

- the role of the European Union Agency for Fundamental Rights[12][13] to undertake research concerning the relationship between security and private life and data protection;

- the need to reinforce the "ethical scrutiny" of projects reviewed under the FP7 Security Theme and make the results of on-going R&D projects in the area of security as widely accessible as possible;

- the societal dimension as an inherent expected impact of all its FP7 Security Theme's call for proposals;

- the possibility to bring the most innovative security sectors into the Lead Market Initiative;

- how to speed up pre-commercial procurement in the security domain;

- the ways for speeding up certification, validation, and, as appropriate, standardisation work in the area of security, notably as regards the applicability and efficacy of a "European Security Label";

- how it can best respond to foreseeable new security missions and priorities, either within the framework of the current FP7, or in preparation of the future framework programme;

- the ways to better link, at EU and Member State level, European security research and development with more operational aspects of security;

- the establishment of a permanent working structure to implement ESRIF recommendations;

- the possibility to establish a forum to strengthen the competitiveness of the security industry active in the field of research and innovation, such as a High Level Group with the involvement of all public, private sector and civil society stakeholders.

---

12 Council Decision No. 2008/203/EC, OJ L 63, 7.3.2008.

13 Regulation No. 168/2007, OJ L 53, 22.2.2007.

## Annex: Executive Summary of the ESRIF Final Report

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.

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.

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.

- **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 event cycle of prevention, protection, 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 occurring incidents, to mitigate their effects, and it analyzes potential dangers inherent to coming technologies.

- 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 additional enabling capabilities 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.

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 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.

**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.