Research for a Secure Europe

Report of the Group
of Personalities
in the field of
Security Research

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

New freephone number:

00 800 6 7 8 9 10 11

LEGAL NOTICE

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information. The views expressed in this publication are the sole responsibility of the author and do not necessarily reflect the views of the European Commission.

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

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

Luxembourg: Office for Official Publications of the European Communities, 2004

ISBN 92-894-6611-1

© European Communities, 2004
Reproduction is authorised provided the source is acknowledged.

Printed in Belgium

PRINTED ON WHITE CHLORINE-FREE PAPER

EUR 21110

Research for a Secure Europe

Report of the Group of Personalities

in the field of Security Research

Contents

The Group of Personalities 4

Executive Summary 6

A. For a Secure Europe 8

1. A changing EU in a changing world 8
2. A new security environment 9
3. Security for Europe 10

B. Research & Technology – force enablers for a Secure Europe 12

4. New technological opportunities 12
5. Time for political action 13
6. The need for coherence 14

C. Towards a European Security Research Programme 16

7. Defining the focus 16
8. Making it work 22
9. Budget implications 25

Conclusions and Recommendations 28

Glossary and Acronyms 30

The Group of Personalities

The primary mission of the Group of Personalities in the field of Security Research is to propose principles and priorities of a European Security Research Programme in line with the EU's foreign, security and defence policy objectives and its ambition to construct an area of freedom, security and justice.

Co-chaired by European Commissioners Busquin and Liikanen, the Group is composed of eight Security Industry Chairmen and Chief Executives, four serving Members of the European Parliament, four Heads of major Research Institutes, two high-level European Defence Ministry officials and two high-level political figures (former European Member State Prime Minister and former European Member State President). Heads of various international organizations and the High Representative for the Common Foreign and Security Policy (CFSP), Javier Solana, also participated in the work.

Over the past six months, the group has been working towards developing the cornerstones of a EU Security Research Programme and the contribution that it could make to address the new security challenges in a changing world.

This report constitutes the fruit of their labours.

Martti Ahtisaari
Former President
of Finland

Carl Bildt
Former Prime Minister
of Sweden

Philippe Busquin
European Commissioner
responsible for Research

Jan Dekker
President, TNO
(until November 2003)

Thomas Diehl
President & CEO,
Diehl Stiftung & Co.

Pier-Francesco Guarguaglini
Chairman & CEO
Finmeccanica

François Heisbourg
Director, Fondation
pour la Recherche
Stratégique

Rainer Hertrich
CEO, EADS

Philippe Kourilsky
President,
Institut Pasteur

Erkki Liikanen
European Commissioner
responsible for
Enterprise and the
Information Society

Erik Löwenadler
President, Ericsson
Microwave Systems

Eryl McNally
Member of the
European Parliament

Javier Monzon
Chairman & CEO,
INDRA

Ilias Pentazos
Director General,
Defence Industry,
Research & Technology,
Hellenic Ministry of Defence

Denis Ranque
Chairman & CEO,
Thales

Maria João Rodrigues
President of SSHRA,
(Social Sciences Advisory
Group to the European
Commission)

Christian Rovsing
Member of the
European Parliament

Mike Turner
Chief Executive,
BAE SYSTEMS

Elly Plooij-van Gorsel
Member of the
European Parliament

Marc Vankeirsbilck
Lieutenant-General
Belgian Ministry
of Defence

Karl von Wogau
Member of the
European Parliament

Claus Weyrich
Senior Vice President,
Siemens

Victor Aguado
Director General,
EUROCONTROL

Nazzareno Cardinali
Director, OCCAR E.A.

Jean-Jacques Dordain
Director General,
European Space Agency

Javier Solana
EU High Representative
for the Common Foreign
and Security Policy

Ernst Van Hoek
Chairman WEAG,
WEAG/WEAO/NL MOD

Rapporteur

Burkard Schmitt,
Assistant Director of the
European Union Institute
for Security Studies

Executive Summary

In today's global society, the European Union faces new opportunities as well as new dangers. Political, social and technological developments have created a fluid security environment where risks and vulnerabilities are more diverse and less visible. New threats have emerged that ignore state borders and target European interests outside and within EU territory. The European Council recognized these threats in December 2003 with the adoption of the EU Security Strategy 'A secure Europe in a better world'.

These threats call for European responses and a comprehensive security approach that addresses internal as well as external security and can combine civil and military means. The closer the Union cooperates with the UN, OSCE, NATO and all its international partners, the more effective its contribution to international security will be. In particular, the EU needs to develop capabilities to protect its citizens at home as well as to deploy significant resources for peacekeeping, humanitarian aid and institution-building activities abroad.

To achieve these objectives, Europe must take advantage of its technological strengths. Technology itself cannot guarantee security, but security without the support of technology is impossible. It provides us with information about threats, helps us to build effective protection against them and, if necessary, enables us to neutralize them. Moreover, new technology trends offer new opportunities. Civil, security and defence applications increasingly draw on the same technological base – creating new synergies between different research sectors.

Using technology as a 'force enabler' for a secure Europe requires state-of-the-art industries, a strong knowledge infrastructure, appropriate funding and an optimal use of resources. Europe has high quality research institutes and a substantial and diverse industrial base from which to address technology requirements in the security domain. However, structural deficiencies at the institutional and political level hinder Europe in the exploitation of its scientific, technological and industrial strength. The dividing line between defence and civil research; the absence of specific frameworks for security research at the EU level; the limited cooperation between Member States and the lack of coordination among national and European efforts – all serve to exacerbate the lack of public research funding and present major obstacles to delivering cost-effective solutions.

To overcome these deficiencies, Europe needs to increase its funding and improve the coherence of its efforts. This implies (a) effective coordination between national and European research activities, (b) systematic analysis of security-related capability needs, from civil security to defence, (c) full exploitation of synergies between defence, security and civil research, (d) specific legal conditions and funding instruments for security-related research at the European level, and (e) institutional arrangements that are both efficient and flexible enough to combine Member State and Community efforts and to involve other interested partners.

Recent initiatives demonstrate a growing awareness of the necessity to act. In this context, the creation of the 'Agency in the field of defence capabilities development, research, acquisition and armaments' and the Commission's Preparatory Action in the field of security-related research are particularly important. The challenge will be to take these initiatives forward and to develop them into a coherent approach. The establishment of a European Security Research Programme (ESRP) from 2007 onwards would be a major contribution towards the achievement of this objective.

An ESRP should take advantage of the duality of technologies and the growing overlap of security functions to bridge the gap between civil and defence research. In support of a comprehensive security approach, it should fund research activities targeted at the development of systems and products that are useful:

- In particular for the protection of Member State territory, sovereignty, domestic population and critical infrastructure against transnational threats, and
- For EU missions 'outside the Union for peace keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter'[1].

An ESRP should maximize the benefits of multi-purpose aspects of technologies. In order to stimulate synergies, it should look at the 'crossroads' between civil and defence applications and foster cross-sector transformation and integration of technologies. Its focus should be on interoperability and connectivity as key elements of trans-border and inter-service cooperation. A core of architectural design rules and standards should be worked out at an early stage.

An ESRP should complement civil Community programmes on the one hand, and security and defence research activities conducted at the national or intergovernmental level on the other. Effective coordination between an ESRP and other relevant research activities is crucial to ensure coherence of efforts.

Moreover, an ESRP must take into account the specific aspects of the security market. This entails the creation of new funding instruments and technology transfer rules. At the same time, customers must be involved throughout the process to avoid disconnecting research and procurement.

An ESRP developed along these lines is of strong social interest and can give significant added value. It would help to enhance Europe's security, which is in itself a precondition of numerous Community policies (transport, energy, telecommunication, etc.). It would foster cross-border cooperation, increase European industrial competitiveness and strengthen Europe's research base. What is more, it would contribute significantly to the EU policy on growth and competitiveness as established in Lisbon and Barcelona.

For all these reasons, an ESRP should be Community-funded. It should have a minimum annual budget of € 1 billion with the possibility to progressively increase it further, if appropriate. In line with the objective for the EU to invest 3% of GDP in research, ESRP funding must be additional to any financing ensured today by the Community Research Framework Programme or national or intergovernmental sources. Such an investment would be an important contribution towards making Europe more secure for its citizens.

---

[1] *See Articles 40 and 42 of the draft Constitutional Treaty.*

A. For a Secure Europe

1. A changing European Union in a changing world

The Union will become wider and more diverse, and has developed new ambitions.

At the beginning of the 21st century, the European Union (EU) has started out on a far-reaching process of transformation. Once enlarged to 25 Member States, the Union will be wider and more diverse than ever before, and this process is likely to continue. At the same time, the EU has developed new ambitions: at the Lisbon summit of March 2000, the Member States embarked on a strategy to make Europe the most competitive knowledge-based economy in the world by 2010. This strategy was backed up two years later in Barcelona, when the European Council set the objective of raising the level of research investment to 3% of EU Gross Domestic Product by the end of the decade. In parallel, the evolving Common Foreign and Security Policy (CFSP) and the European Security and Defence Policy (ESDP) herald the Union's emerging role as a global actor and its growing participation in efforts to secure peace and stability in the world.

At the same time, globalization – with all its political, economic, financial and technological dimensions – is multiplying and strengthening Europe's links with the rest of the world and fostering its integration into an emerging global society.

These developments create new opportunities as well as new risks. On one hand, the increased flow of people, goods, services, and capital across borders boosts economic activity and enhances prosperity. The spread of ideas and information across the Internet and via other global media broadens cultural horizons and becomes a powerful tool to advance the cause of human rights and democracy. Technological innovation is faster and the spread of know-how is wider than ever before, offering new chances for greater wealth and prosperity.

Globalisation creates both new opportunities and new risks for Europe.

On the other hand, globalization also brings new dangers. In an interdependent world, conflicts in remote regions can destabilize the international order and directly affect Europe's security and interests. The growing dependence on interconnected infrastructures in transport, energy, information and other fields increases the vulnerability of modern societies. At the same time, the natural diffusion of technological know-how resulting from scientific and industrial development makes it easier for technological advancements to be used malevolently. Increasing mobility allows diseases to spread easily and rapidly across borders and continents. Humanitarian crisis situations can spring up on our borders and demand instant responses.

2. A new security environment

The main sources of anxiety are new threats, risks and vulnerabilities.

In Europe and elsewhere, the evolving global situation and some startling events have profoundly changed the understanding of the term 'security'. In the United States, the terrorist attacks of 11 September 2001 have brought about a new sense of vulnerability. This has led to the adoption of a new security concept, record-breaking investments in defence and security, and the establishment of a Department of Homeland Security to prevent terrorist attacks, reduce America's vulnerability to terrorism, and minimize the damage from potential attacks and natural disasters.

Europe's security environment has changed as well. Since the end of the Cold War, large-scale military aggression against EU territory has become improbable. This does not mean that high-intensity, purely military confrontation and conflict is no longer possible. It is increasingly clear, however, that the main sources of anxiety for both citizens and policy-makers alike are new threats, risks and vulnerabilities.

What do European Union citizens fear ?

Source: Eurobarometre, Sondage no. 58.1, Oct./Nov. 2002

According to the EU's Security Strategy 'A secure Europe in a better world'[2], Europe's security is compromised – directly or indirectly – by global challenges such as disease, poverty, competition for natural resources and energy dependence, and is confronted by a number of key threats:

- Terrorism, in particular catastrophic terrorism that acts worldwide and seems willing to use unlimited violence to cause massive casualties;
- Proliferation of Weapons of Mass Destruction (WMD), in particular in combination with international terrorism;

[2] *European Security Strategy – presented by Javier Solana, EU High Representative for CFSP, adopted by the Heads of State and Government at the European Council on 12 December 2003.*

- Regional Conflicts, which become themselves a source of other threats like extremism, terrorism, state failure, organized crime and WMD proliferation;
- State failure, often due to bad governance, creating the breeding ground for other threats like organized crime and terrorism;
- Organized crime, which has developed an important international dimension.

The diversity of new threats and vulnerabilities presents a major challenge and calls for common European answers.

These threats are more diverse, less visible and less predictable than those Europe faced during the Cold War. Driven by the large number of (potentially) unstable regions and the speed of technological development, they can evolve rapidly. They may or may not include a military dimension, are often asymmetric, and can threaten the security of Member States both from outside and inside EU territory. In general, these threats are multi-faceted and interrelated, combining, for example, bad governance, weak states, poverty, human trafficking, organized crime, drug smuggling and terrorism.

This diversity presents a major challenge for the formation of Security policies and calls for common European answers. Since current threats ignore national borders and can damage European interests at home and abroad, the distinction between external and internal security becomes increasingly blurred. Their trans-national nature has led nations to internationalize their security policies, intensifying cooperation and coordination in numerous areas and recognizing that each of these threats requires a specific combination of means in order to be tackled successfully. Military instruments can and do play a role, but in most cases intelligence, police, judicial, economic, financial, scientific and diplomatic means will be at least as important.

3. Security for Europe

Facing these changes and challenges, there is both a need and an opportunity for the EU to develop a comprehensive approach that links the external and internal dimensions of security and can combine the use of civil and military means.

As a union of 25 states with over 450 million people producing a quarter of the worlds GNP, the European Union is a global actor; it should be ready to share in the responsibility for global security*.

Given its international standing, the EU has a responsibility to play an active role in world affairs. The closer the Union cooperates with its partners, the more effective its contribution to international security will be. Since no single country or organization can cope with today's threats and vulnerabilities on its own, the EU must join efforts with the UN, OSCE, NATO and all its international partners.

The Union's engagement abroad is based on a preference for multilateral institutions and agreements, the rule of law and the treatment of root causes. 'Effective multilateralism' and 'preventive engagement' guide the EU's CFSP and ESDP. The latter combines military and civilian means to make the EU's international engagement more effective.

*) *'A secure Europe in a Better World'– European security strategy.*

The main responsibility for external security will rest for the foreseeable future with Member States. However, national governments will only be able to tackle the new security challenges if they combine their efforts. The types of conflicts, crises or state failures with which the EU has to deal require primarily civilian assets, including police, to rebuild societies. Enabling them to work together efficiently on the ground is already a challenging task. At the same time, interoperability is also a prerequisite for cooperation between European armed forces. Since many crisis management operations will draw on both civilian and military capabilities, seamless interaction and coordination between the two will be the key to the success of a comprehensive security approach.

The Union must protect its own citizens and its own territory as well. Internal Security[3] is particularly challenging in Europe, because it concerns not only national governments, but also regional and local authorities. What is more, responsibilities and organizational structures of the different security services (police, customs services, intelligence agencies, civil protection agencies, etc.) vary greatly within and between Member States. Given this diversity, on one hand, and the trans-national nature of current threats, on the other, it is particularly important to ensure a consistent level of security throughout the Union. Moreover, effective coordination and cooperation of services from different Member States would be vital in the event of a major terrorist attack or a disaster.

The Union must protect its citizens and defend at the same time its commitment to a pluralist, open and liberal society.

With this in mind, Europe must defend its commitment to a pluralist, open and liberal society. Striking the right balance between security and freedom will be a permanent challenge while respecting the highest ethical principles. Europe's vision of security must therefore embrace a notion of 'Internal Security' that can include a genuine feeling of well being and safety for its citizens, while respecting its values of human rights, democracy, rule of law and fundamental freedoms.

All this makes the provision of security an extremely complex management task that demands active participation by the EU. In particular, the Union must encourage an appropriate degree of security in all Member States and mobilize the necessary resources to tackle threats and vulnerabilities that concern all EU citizens and European societies as a whole.

Given today's security environment, there is an urgent necessity to act. The stakes are too high to trivialize threats, hoping that catastrophic events would spare EU territory. Europe must rapidly build up the capability to protect its citizens at home as well as to deploy significant resources for peacekeeping, humanitarian aid and institution-building activities abroad. To achieve these objectives, Europe must take advantage of its technological strengths. This requires state-of-the-art industries, a strong knowledge infrastructure, appropriate funding and an optimal use of resources.

The stakes are too high to trivialize threats, hoping that catastrophic events would spare EU territory.

[3] In this context, 'Internal Security' should be understood as a concept aimed at protecting citizens from threats like terrorism, organized crime, etc. The fundamental objective of 'Internal Security' is hence to protect the freedom and integrity of European citizens.

B. Research & Technology – 'force enablers' for a secure Europe

4. New technological opportunities

Technology itself cannot guarantee security, but security without the support of technology is impossible.

Technology itself cannot guarantee security, but security without the support of technology is impossible. It provides us with information about threats, helps us to build effective protection against them and, if necessary, enables us to neutralize them. In other words: technology is a key 'force enabler' for a more secure Europe.

At the same time, the security dimension of technology itself is changing, because technology is very often multi-purpose. Civil and defence applications increasingly draw from the same technological base and there is a growing cross-fertilization between the two areas.

Technologies initiated for defence purposes have already led to important commercial applications. The Internet and the Global Positioning System (GPS) are the most prominent examples of such dual-use technologies. However, 'spill-over' effects increasingly work both ways: the so-called 'Revolution in Military Affairs', in particular, is based on a combination of electronics, information technology and telecommunications. To a large extent, these technologies have not been developed by defence companies but by civilian firms for the commercial market. In the key area of 'network-enabled capability', there is a distinct technology flow from the civil to the defence sector.

Civil and defence applications increasingly draw from the same technology base.

As a result, the technology base for defence, security and civil applications increasingly forms a continuum. Across this continuum, applications in one area can often be transformed into applications in another area. This is particularly the case for defence and security: while the armed forces and the various security services will always have their specific needs, there is an increasing overlap of functions and capabilities required for military and non-military security purposes (such as is found between border police, coast guard and emergency response teams) that often allows the use of the same technology for the development of both security and defence applications. Space technologies are a perfect illustration of this: a decision as to whether global positioning or earth observation systems, for example, are to be used for defence and security purposes is primarily political in character, not technological. Biotechnology provides another example: The same tools which can detect and fight harmful biological aspects with high sensitivity can be used to protect the population from bio-terrorist attack and from natural epidemic outbreaks.

5. Time for political action

In today's technology-driven and knowledge-based world, excellence in research is a prerequisite for the ability to tackle the new security challenges.

Excellence in research is a prerequisite for the ability to tackle the new security challenges.

Europe has high quality research institutes and a substantial and diverse industrial base from which to address technology requirements in the security domain. A significant part of this industrial base specializes in the defence, aeronautic, space and professional electronics sectors, with capabilities running right through the supply chain from systems integrators/prime contractors to equipment and component suppliers, including a large number of innovative small and medium size enterprises. Europe also has world-class industrial expertise in pharmaceuticals, bio-technology and telecommunications. Each of these sectors is knowledge-based and enjoys significantly higher productivity levels than the industrial average for Europe. Targeted research investment in these areas will therefore not only enhance security but also contribute to EU productivity and growth.

If Europe is to take full advantage of its industrial, technological and scientific strengths, it will have to increase funding in these areas and improve its political and institutional efficiency. Greater harmonization of requirements and more effective coordination at the European level would enhance operational effectiveness and provide the market scale necessary to support the development and exploitation of the technology base. However, time is of the essence. Europe needs to act quickly if it is to remain at the forefront of technology research, and if industry is to be able to exploit the results competitively in response to the rapidly emerging needs for sophisticated security-related products.

Europe should be able to get a much better return on its defence research investment. European efforts are limited in this area and remain fragmented at national level. Wasteful duplication persists, particularly in product development, with only a small portion of resources spent on European cooperation. This dispersion is another consequence of fragmented defence markets where the absence of a single customer with a single set of requirements increases costs and leads to inefficiencies.

If Europe is to take full advantage of its strengths, it will have to increase funding and improve its political and institutional efficiency.

In the field of non-military security, these shortcomings are even more prominent, since it involves a variety of customers within each Member State with very different tasks and requirements. In addition, the organizational and institutional affiliations of these customers differ greatly within and between Member States. Consequently, the definition of capability needs and acquisition are highly fragmented without any coordination at the European level. Moreover, public funding of non-military security research is generally limited.

Dispersion of efforts exacerbates the lack of funding and hinders Europe in the exploitation of its technological and industrial strength.

Until now, the EU has not had a role in defence research, while playing only a minor part in security research. In civil research, however, the Union is an important player. Its Framework Programmes contribute to competitiveness in specific technological fields while driving industrial collaboration at European level. Given the duality of modern technology, some of the Framework Programme's research activities have important security implications. This is the case in particular in the field of space, communication and information technology where civil research projects can often lead to security-related applications. However, this dual-use potential is the result of a 'technology push' rather than of a 'requirement pull': it has not been actively sought, but has happened 'coincidentally' and is often politically sensitive. In addition, the Framework Programme does not offer the necessary conditions for 'secured' research in terms of confidentiality, Intellectual Property Rights (IPR) and funding.

In short, there is a dispersion of effort and a lack of coherence in research that hinders Europe in reaping the full benefits of its technological and industrial strength and creates enormous difficulties for interoperability between 'security users'. The need for more cooperation and coordination is increasingly recognized, and some initial steps to improve the situation have been taken. However, structural deficiencies still persist. The dividing line between defence and civil research funding, the absence of specific frameworks for security research at the European level, the limited cooperation between Member States and the lack of coordination between national and European efforts exacerbate the lack of public research funding and present major obstacles to achieving cost-effective solutions.

6. The need for coherence

To overcome these deficiencies, Europe needs to increase the coherence of its efforts. Drawing lessons from existing instruments and arrangements, it needs to target in particular:

- **Involvement of all Member States;**
- **Effective coordination between national and European efforts;**
- **Systematic analysis of security-related capability needs, from civil security to defence;**
- **Sufficient funding;**
- **Full exploitation of potential synergies between defence, security and civil research;**
- **Providing specific legal conditions and funding instruments for security-related research at the European level;**
- **Creating institutional arrangements that are both efficient and flexible enough to combine the efforts of Member States and the Community, and to involve other partners with mutual benefit.**

Organizing research along these lines would strengthen Europe's scientific and technological base, foster industry's international competitiveness and promote research activities in support of other EU policies.

The European Union has a broad set of policies that can help to achieve these objectives. It has developed ESDP, both the military and civilian aspects, and has begun to tackle the relevant shortfalls. The EU has proven experience in the management of civil research programmes and it constitutes a common framework to coordinate Community, CFSP/ESDP and national activities. This framework could be used to set up mechanisms for better coordination and the development of a more coherent approach to security research.

The European Union has a broad set of policies that can help to develop a more coherent approach to security research.

Real 'political will' will be necessary to achieve these objectives. However, recent events have provided some positive signs.[4] Two initiatives are particularly important:

- In November 2003, the General Affairs Council decided to create, in the course of 2004, an Agency in the field of defence capabilities development, research, acquisition and armaments. One of the tasks of this Agency will be to promote, 'in liaison with the Community's research activities where appropriate, research aimed at fulfilling future defence and security capabilities requirements and thereby strengthening Europe's industrial potential in this domain'.[5]
- Following its Communication on 'European Defence – Industrial and Market Aspects', adopted on 11 March 2003,[6] the Commission launched a Preparatory Action entitled 'Enhancement of the European industrial potential in the field of security research 2004-2006'[7] that will prepare the basis for a fully-fledged European Security Research programme starting in 2007.

The Preparatory Action

The Preparatory Action (foreseen for 2004-2006) will fund Research and Technology and support mission-oriented projects via calls for proposals and public procurement. It is an important first step in addressing the need for Community action and aims at establishing a fully-fledged Programme for Security Research in Europe from 2007.

Importantly, the Preparatory Action will also address issues related to serving an end user Community essentially composed of public service organizations and, in particular, government departments and services, security agencies, non-governmental organizations, industry and the wider public sector.

The Preparatory Action should prepare the groundwork for a successful Security Research Programme. To achieve this objective, it must investigate new rules and procedures, explore future research areas and build networks between sponsors, companies, research centres and customers.

---

4) See EP Resolutions #0172 (April 2002), asking the Commission to investigate the possibility of establishing an Advisory Council for security research; STAR 21 group (July 2002), asking to consider the possibility of developing a multi-institution defence industry body to pool and co-ordinate research in the defence field; Presidency Conclusion of the European Council (March 2003), recognising 'the role that defence and security related R&D could play in promoting leading-edge technologies and thereby stimulate innovation and competitiveness'; Conclusion of the European Council of Thessaloniki (June 2003), tasking the Council bodies to prepare the creation of an 'Agency in the field of defence capabilities development, research, acquisition and armaments'.

5) See GAERC of 17/18 November 2003, External relations, p. 14.

6) COM (2003) 113.

7) See COM (2004) 72, adopted on 3 February 2004.

C. Towards a European Security Research Programme

An ESRP should take advantage of both the duality of technologies and the growing overlap of defence and non-military security functions.

The challenge will be to take these initiatives forward and to develop them into a coherent approach. In this context, the establishment of a European Security Research Programme (ESRP) from 2007 onwards is crucial.

Straddling civil and defence research, an ESRP should take advantage of both the duality of technologies and the growing overlap of defence and non-military security functions to bridge the gap between the various research sectors.

In support of a comprehensive security approach, an ESRP should be targeted at the development of systems and products that are useful:

- In particular for the protection of Member State territory, sovereignty, domestic population and critical infrastructure against trans-national threats, and
- For EU-missions 'outside the Union for peacekeeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter'.[8]

Such an ESRP would have the potential to foster cross-border cooperation and contribute to the EU policy on growth and competitiveness as established in Lisbon and Barcelona. Moreover, it would help to enhance the EU's security, which is in itself a precondition of numerous Community policies (transport, energy, telecommunication, etc.). For all these reasons, an ESRP should be Community-funded. It should complement existing civil Community programmes on one side, and security and defence research activities conducted at the national or intergovernmental level on the other – thus becoming a key element of a more coherent research approach.

7. Defining the Focus

A capability-related approach

In order to spend the EU taxpayer's money in the most cost-effective way, an ESRP must take the EU's political objectives into account and focus on technology areas that meet the Union's security needs as precisely as possible. To identify these areas, a capability-related approach would be appropriate and should be based on a full assessment of the situation:

1) What are the threats?

2) What are the missions required to tackle these threats?

3) What are the capabilities needed to accomplish these missions?

4) What are the technologies – or combination of technologies – that can provide the necessary capabilities?

[8] *See Articles 40 and 42 of the draft Constitutional Treaty.*

There are, however, two problems with this approach:

- First, the instability of the new strategic environment makes it difficult to foresee the future evolution of threats and thus future technological needs;
- Second, the absence of a single customer makes it hard to define common requirements. This is true for military needs, but even more so for non-military security needs.

The EU Security Strategy provides a general framework for the definition of future research priorities and investments.

While the Union has established some, albeit modest, mechanisms for identifying and tackling defence capability shortfalls, a common approach to address Internal Security needs is still missing. However, the EU Security Strategy provides at least a general framework for the definition of future research priorities and investments. It identifies a number of key threats that can give guidance for both CFSP/ESDP and the protection of the EU territory. Based on these assumptions, one can establish a set of missions and capability needs:

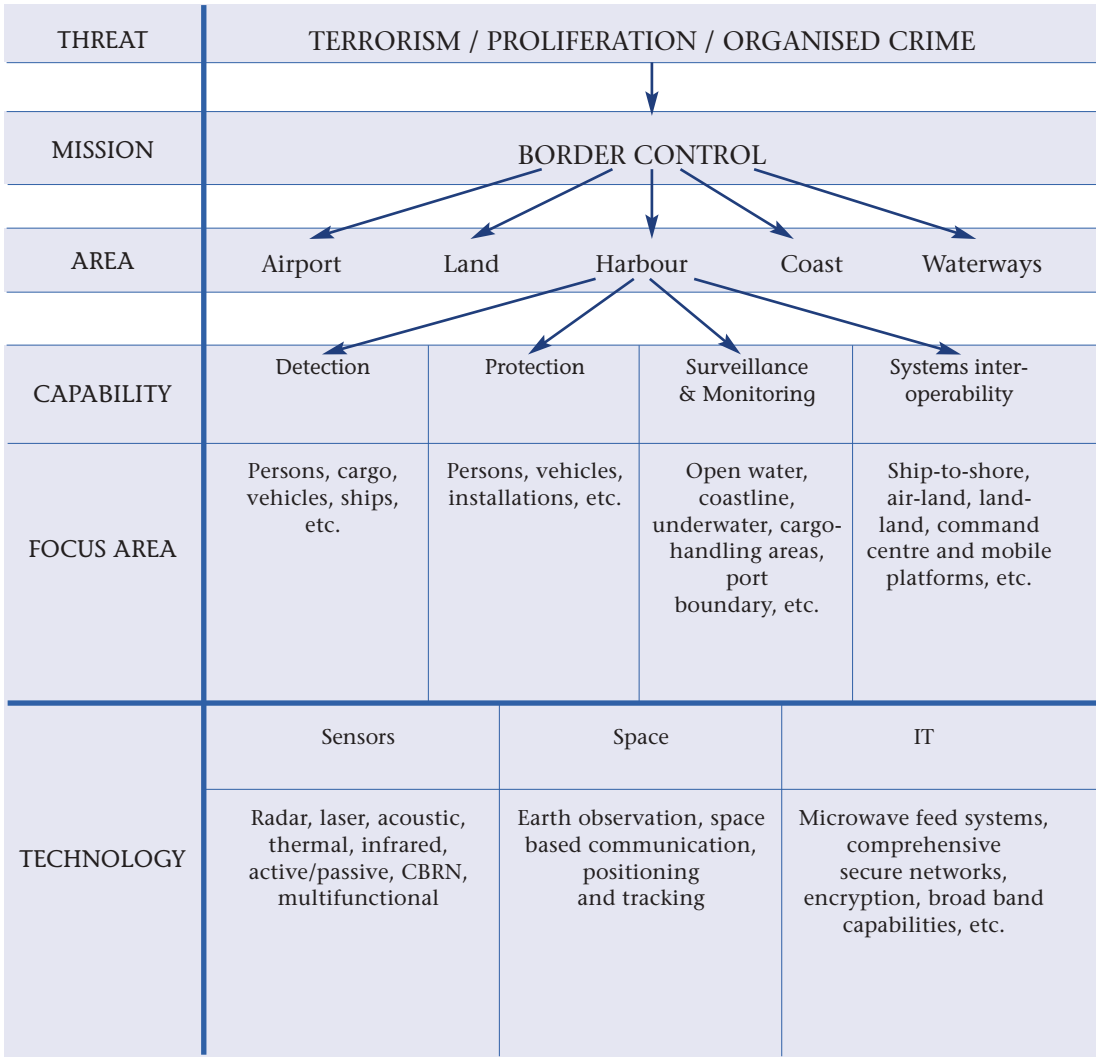
Table 1: Examples of the link between threats, missions and capability needs

		International Terrorism	Organized Crime	Proliferation of WMD
Missions	Protection of Critical Infrastructure	X	X	
	Border Control	X	X	X
	Civil Defence/Protection	X		
	Disaster Management	X		
	Law enforcement (Arrests / Neutralization)	X	X	X
	Law enforcement against trafficking	X	X	X
	Law enforcement against financial crimes	X	X	
	Treaty verification			X
	Export control			X
Capabilities	Intelligence	X	X	X
	Assessment and Analysis	X	X	X
	Surveillance (of borders and critical sites)	X	X	X
	Monitoring (of trade and financial flows)	X	X	X
	Secured Communications	X	X	X
	Identification (IDs, access control)	X	X	
	Detection (persons, CBRN, explosives)	X	X	X
	Disposal (explosives, CBRN)	X		X
	Decontamination	X		
	Modeling/Simulation	X	X	

Table 1 is not meant to be exhaustive, nor does it claim to be a comprehensive threat assessment.[9] Even so, it does demonstrate that although each threat may have its specificities, an effective defence against them will often require the same missions. Border control, for example, is an important mission in the fight against proliferation, organized crime and terrorism, and the protection of IT networks (as elements of critical infrastructures) is essential in the fight against terrorism, organized crime, etc.

Although each threat may have its specificities, an effective defence against them will often require the same missions.

Table 2: Examples of the link between



[9] *These examples consider the internal dimension of the fight against the three threats that European citizens fear the most. The other two key threats identified in the EU Security Strategy, state failure and regional conflicts, are more difficult to use to define missions and capabilities, since they are sources of threats rather than threats themselves: Regional conflicts 'can lead to extremism, terrorism and state failure; it provides opportunities for organised crime [and] can fuel the demand of WMD.' […] Collapse of the State failure can be associated with obvious threats, such as organised crime or terrorism. See 'A secure Europe in a better world'.*

It is also clear that many capabilities serve internal and external as well as military and non-military security purposes. Surveillance, for example, is needed for both the protection of national borders and for crisis management operations abroad. The same is true for secured communications, intelligence and assessment capabilities.

Table 2 goes one step further and gives some examples of how a capability-related approach can help to identify more specific technologies and applications.

Many capabilities serve internal and external as well as military and non-military security purposes.

threats, capabilities and technologies

TERRORISM / ORGANISED CRIME			TERRORISM			
PROTECTION OF CRITICAL INFRASTRUCTURE			DISASTER MANAGEMENT			
Electricity	IT	Oil & Gas / Transport	Conventional attack	CBRN attack		Hostage
Security against Cyber-attack	Secure digital communication	Protection of network hardware	Protection	Detection	Deconta-mination	Systems inter-operability
LAN (local area networks), WAN (internet infrastructure and other wide area networks)	Hardware or software based communication privacy, fidelity and reliability	Building security, infrastructure redundancy, etc.	Persons, critical infrastruc-tures,strate-gic assets, etc.	CBRN agents and materials, etc.	Surfaces, buildings, persons, critical infrastruc-tures, etc.	Inter-agency-communica-tion, response concepts, hardware Interopera-bility, etc.

Fire walling and Virus protection	Encryption and Trusted Computing	Neutralizers	Sensors	IT
Hard and soft fire walling, protection against virus, Spam, Spim, Trojan, Worm, VP Networking, DDOS resistance for root- and web servers and DNS	Client/server authentica-tion; privacy and digital signatures in e-mail; authenticating web servers and encrypting communications with a web server. data integrity: message digest or hash algorithm.	High-pressure systems, vaporizers, Filters, vaccines, etc.	Microfluidic scanners, “smart dust” scanners, etc.	Secure networks, modeling and simulation, contamination response soft- and hardware, etc.

The list of missions, capabilities and technologies related to each threat is, of course, not exhaustive. Even so, Table 2 confirms the multi-functionality of capabilities and technologies, both within the spectrum of Internal Security missions and across the boundary between external and internal security. Intelligence and Secure Communications, in particular, are crucial for all missions and actors. Surveillance is needed for the protection of national borders and for crisis management operations abroad. In both cases, the means used to fulfill the capability can often be the same. Unmanned Aerial Vehicles (UAV), for example, can be used for surveillance both by armed forces in crisis management operations and by coast guards to control maritime borders. In each case, the application would be adapted to the specific needs of the customer – in terms of performance, complexity and operational requirements – but the basic technology will probably be quite similar.

Capabilities and technologies are often multi-functional, both within the spectrum of Internal Security missions and across the boundary between external and internal security.

Another key aspect is the importance of networks for both Internal Security and crisis-management operations. Security management is inherently distributed across different authorities and operators, with their respective roles, capabilities and resources. In such a decentralized environment, interoperability of communication and information systems and the links between different networks are crucial. All relevant security services should be able to exchange information rapidly and securely. This information should be coordinated, and agreed parts should be combined into a common situation picture. The latter would then be redistributed among all services linked to the network and, via mobile and wireless communication means, made available to individual security agents on the spot. Common standards worked out in early stages would facilitate interoperability and information security.

Given the multi-functionality of many capabilities and technologies, specific military requirements (such as availability, reliability, protection, miniaturization, redundancy, etc.), which are normally quite onerous, can increase the performance of systems and provide a technology push that can further increase their utility and competitiveness for both civilian and security uses. Security developments in information technologies and telecommunications in particular can have important technological spin-off effects into the commercial market, which confirms the significance of security research for economic growth and industrial competitiveness in general.

We conclude that:

a) A European Security Research Programme should take advantage of the multi-functionality of capabilities and technologies;

b) A flexible approach to security research has the potential to bridge the gap between civil and traditional defence research.

An ESRP should seek to maximise the benefits of multi-purpose technologies and open the door to cross-sector interaction.

As a consequence of all this, an ESRP should seek to maximize the benefits of multi-purpose aspects of technologies (without excluding support for key specific areas if their interest is demonstrated). In order to allow for a maximum of cross-sector interaction, it should in particular:

- **Look at the 'crossroads' between civil and defence applications;**
- **Foster the transformation of technologies across the civil, security and defence fields;**
- **Define multi-functionality as positive criteria for the selection of research proposals.**

An ESRP should concentrate on interoperability and connectivity as key functions for security management in a distributed environment. Emphasis should also be placed on security areas that require a particularly high degree of cross-border and inter-service cooperation. This is the case for measures against bio-terrorism, for example, where investments would bolster existing health and emergency infrastructures and thus be beneficial for society as a whole. In addition, architectural design rules for European efforts as well as common standards and protocols for 'systems-of-systems' should be defined at an early stage to enhance IT security and interoperability between different systems and user communities.

Emphasis should be placed on security areas that require a particularly high degree of cross-border and inter-service cooperation.

The Transatlantic Dimension

In the United States the creation of the Department of Homeland Security (DHS) has focused the nation's effort on its domestic security task. In 2004, the DHS directly manages a budget of $36 billion and co-ordinates an overall budget exceeding $100 billion distributed among various other Departments and in individual States. This aggregate is expected to rise considerably in the coming years. The DHS budget includes a significant percentage devoted to equipment, and around $1 billion dedicated to research. This effort is in addition to those activities funded by other agencies related to Homeland Security and defence R&T and procurement programmes funded by the Department of Defense (DoD). The scale and scope of the U.S. investment in Homeland Security research has a number of effects, including:

- The U.S. is taking a lead and will develop technologies and equipment which, subject always to U.S. technology transfer permission, could meet a number of Europe's needs;
- U.S. technology will progressively impose normative and operational standards worldwide;
- In certain areas, where the U.S. authorities prioritize their investment and achieve fast product 'speed to market', U.S. industry will enjoy a very strong competitive position.

Europe will need to find realistic responses to the effects of U.S. security investment.

Europe's response to these developments will need to be realistic. On one hand, global interoperability requires universal solutions: for example, a system seeking to track and control the international movement of freight containers will have to comply with regulations for containers destined for the U.S., which alone account for 50% of international container traffic. Similarly, there is limited value in duplicating research already conducted elsewhere if the results can be shared in a mutually beneficial way. Furthermore, the evaluation of the case for investment in Europe will need to take into account the dynamics of the market. On the other hand, technology transfer restrictions limit the availability and potential for exploitation of such research in certain areas, and requirements in Europe

may differ from those defined elsewhere. For example, the networking of existing information and communications systems between diverse agencies in different Member States is a particularly challenging priority in Europe.

Selection of areas for investment will need to recognize these factors, and should also take into account sectors where European industry can expect to generate competitive advantage. The selection should be guided by the following outline principles:

For critical technologies, Europe should aim for an indigenous competitive capability.

- For critical technologies, Europe should aim for an indigenous competitive capability, even if this involves duplication of effort;
- For less critical technologies and/or in areas where requirements in Europe are distinct or in advance of those sought elsewhere, specific assessments should be made of the merits of development in Europe, justifiable on requirements or industrial competitiveness grounds;
- In other cases, a co-operative approach should be pursued.

8. Making it work

Two points are crucial for an ESRP to become a success. First, it must be effectively coordinated with other relevant research activities in order to improve the coherence of European efforts. Second, it must take into account the specific nature of security research. To achieve these objectives, we suggest that the following principles should underpin the development of an ESRP:

Complementarity

An ESRP should support and complement – and not duplicate – activities funded nationally, under intergovernmental cooperation agreements or by other organizations. While certain tasks will remain at national or intergovernmental level, there is a wide domain where only an EU-wide approach can bring the necessary results. These include, among other things:

- A core of architectural rules, system design and standards;
- Application of new technologies to improve interoperability between EU Member State services and/or between the EU services and others;
- Non-recurring investment costs that can be spent most effectively at EU level.

An ESRP must be effectively coordinated with other research activities and take into account the specific nature of security research.

Flexibility

The multi-functionality of many technologies and the overlap of security functions necessitate a high degree of flexibility concerning the decision on 'who funds what'. Flexibility should also extend to 'how' and 'where' the execution of an ESRP should be conducted. In general, an ESRP should be managed in an effective non-bureaucratic way. However, this should not be at the expense of either accountable management of the Programme or of proper democratic scrutiny in accordance with the Community's co-decision procedure.

Focus on capability-related research

An ESRP should focus on capability-related research, i.e. research activities that are oriented towards defined capability needs of security 'users'. This should not exclude the possibility to fund exploratory research on emerging technologies that can lead to technological breakthroughs. In general, however, it should neither sponsor 'pure' research (which follows a different logic and seeks innovation per se without any link to capability needs) nor product development (which can already be considered as 'phase 0' of the procurement process). An ESRP should thus concentrate on research up to the level of demonstrators.

An ESRP should concentrate on research up to the level of demonstrators.

Market specificities

The Community Framework Programme offers a solid basis of experience in setting up and implementing collaborative research projects over a range of fields in civil markets. However, if the crossover between technologies employed for civil and security purposes is evident, the applications and the market conditions under which research and product development are funded are markedly different. A substantial part of the Programme will be destined for public authorities' exclusive use, with similar constraints that exist in defence markets. An ESRP must recognize that:

- The technological, financial and demand risks of research destined for limited governmental requirements are higher, justifying a higher ratio of public funding. As in defence research, co-funding schemes for an ESRP should therefore allow for flexibility to fund up to 100%. New funding instruments will therefore need to be created for the implementation of an ESRP.
- An intellectual property regime to match these instruments, and rules governing technology transfer and the protection of information (both within the EU and with third country partners) relating to programmes classified for security reasons, will be required. In this context, the provisions of the EUROPA MoU could serve as a particularly useful reference.[10]
- To ensure market coherence for research destined primarily for public sector applications or requiring public normative certification, it is crucial to achieve a common understanding about requirements between the authorities sponsoring the research and those funding product development or acquisition. Continuous dialogue between research sponsors, customers and industry will be a critical factor in the successful delivery of the overall Programme.

New funding instruments, IPR and technology transfer rules will need to be created.

[10] In May 2001, the defence ministers of WEAG member states signed a Memorandum of Understanding (MOU) entitled 'European Understandings for Research Organisation, Programmes and Activities', known as the EUROPA MOU. EUROPA is a general umbrella for cooperative defence R&T projects: it does not contain detailed rules for the conduct of projects, but it allows participants to develop their own rules, with a large degree of flexibility. Any two or more EUROPA signatories can propose the creation of a European Research Grouping (ERG) to carry out either a number of individual R&T projects or a single major programme. Membership of ERGs is variable – depending on who is interested in joining the Grouping, and on who agrees on the content of the ERG arrangement in which the particular rules for that ERG are set out. These rules cover the usual necessary subjects in the area of R&T co-operation, such as contracting, finance, security and intellectual property rights. The EUROPA MOU itself explains in detail how ERGs can be set up.

Involvement of Customers

While the market for security products is vast and also involves private customers, the main clients are national, regional and sometimes local public services. In order to accurately define future capability and technology needs and priorities, it is crucial to involve these customers from the very beginning of the process. As stated above, this is particularly difficult since a large number of very different security authorities are concerned and some information will be highly classified. However, there is a need to agree on threats, missions and capability needs first to allow convergence on operational requirements for specific applications. This can be done at higher political and operational levels through a mechanism that brings together representatives from Member States, the Commission and, possibly, relevant EU-Agencies. However, potential customers should be directly involved in the evaluation of research proposals.

There is a need to agree on threats, missions and capability needs first to allow convergence on operational requirements for specific applications.

Joining efforts

The preparation and implementation of an ESRP present enormous management challenges. If an ESRP is to add value, it needs to be orchestrated with the efforts of all other relevant actors.

- Vis-à-vis Member States, this implies establishing exchange of information on national and intergovernmental research activities, proposing solutions to overcome potential redundancies, and coordinating an ESRP with Member State programmes. This is particularly important to avoid unnecessary duplication and to determine the necessary level of Community-funding.
- An ESRP must be closely coordinated with other EU research activities, both in the civil and the defence field. This concerns in particular the Seventh Research Framework Programme and research activities resulting from a possible new 'Headline Goal 2010' for defence capabilities. Whether the ESRP is run as a programme in its own right or set up as part of the next Framework Programme or whether the 'Agency in the field of defence capabilities development, research, acquisition and armament' should play a role in this field, remains to be seen. However, the relationship with the future Agency will be highly important.
- Attention should also be paid to WEAG's and NATO's research activities. Many European nations are involved in these activities, which could overlap in certain areas with the EU's Security Programme. Information exchange, mutual reinforcement and complementarity of activities must be ensured to make the best use of resources.

A 'Security Research Advisory Board' should be established to prepare the ground for an ESRP.

All these principles need to be spelled out in detail before an ESRP begins. A 'Security Research Advisory Board' should therefore be established to prepare the research agenda of an ESRP as well as to advise on the principles and mechanisms for its implementation. It should also identify critical technology areas where Europe should aim for an indigenous competitive capability. The Board should consist of high-level experts from public and private customers, industry, research organizations and any other relevant stakeholders.

9. Budget Implications

If an ESRP is to add value, it will need to have a budget that is both credible and realistic. In other words, while the level of funding will inevitably be determined by the general situation of public finances in Europe, it must be high enough to 'make a difference'. Moreover, security research funding must not replace, but come on top of financing that is currently ensured by the Community Research Framework Programme or national or intergovernmental sources. Only as additional funding to existing sources will security research become an important contribution towards the objective of the European Union investing 3% of GDP in research.

The funding level of an ESRP must be high enough to 'make a difference'.

The complexity of the new security tasks makes the calculation of an appropriate funding level of the ESRP particularly challenging. In general, Community funding should be focused on Research and Technology (R&T), that is research that is not linked to specific procurement projects, but is more upstream in nature. Such an approach is best suited to the capability-related focus of an ESRP and leaves the costs for product development to the (national, regional or local) customer.

Based on this assumption, different approaches are possible. Calculations could be made on the basis of:

- Security research funding per citizen;
- Research funding for Internal Security missions only;
- Security research funding in combination with defence research expenditure;
- Security research funding as part of the overall research effort.

In this context, a comparison with the U.S. may be useful. It is true that the EU has neither the same worldwide interests nor the same security concept as the U.S. Consequently, the benchmark for European defence budgets should be Europe's declared ambitions rather than U.S. spending levels. However, this is not necessarily the case for Internal Security: The EU is equally exposed to the new threats, it has to cope with the same vulnerabilities of modern societies, and the borders of the enlarged Union are considerably more difficult to protect than those of the U.S. Consequently, while priorities for internal security may differ, a comparable level of investment on security research seems justified.

Priorities for Internal Security in the EU may differ from those in the U.S., but a comparable level of investment on security research seems justified.

At the same time, the U.S. budget illustrates perfectly well the blurring of the distinction between military- and non-military security functions and capabilities. Research spending on 'Homeland Defence' is in fact funded by a variety of Departments and Agencies from different backgrounds:

Federal Homeland Security R&D
(budget authority in millions of dollars)

	FY 2002 Actual	FY 2003 Estimate	FY 2004 Request	Change Amount
Agriculture	175	173	80	-93
Commerce	19	16	19	3
Department of Defence	259	597	157	-440
Department of Energy	0	19	0	-19
Department of Homeland Security	266	669	907	238
Environmental Protection Agency	4	50	29	-21
Health and Human Services	177	1651	1708	57
National Aeronautics and Space Agency	73	65	55	-10
National Science Foundation	229	269	286	17
Transportation	55	58	4	-54
All Other	104	180	177	-4
Total Homeland Security R&D	**1361**	**3747**	**3422**	**-325**

Sources: AAAS R&D Funding Update, 'Homeland Security R&D in the FY 2004 Budget', October 1, 2003

Department of Defense RDT&E
(budget authority in millions of dollars)

	FY 2002 Estimate	FY 2004 Request	FY 2004 Confirmed	Change Amount
Army	7516	9123	10310	1187
Navy	13597	14207	14969	862
Air Force	18763	20336	20366	29
Defense Agencies	17424	17974	18961	987
DARPA	2690	2954	2834	-119
Missile Defense Agency	6682	7729	7630	-99
Chemical and Bio. Defense Program	634	599	684	85
Defense Threat Reduction Agency	406	382	412	29
Office of Secretary of Defense	2198	1551	2024	473
Other	4814	4760	5278	618
Director of Operational Test & Evaluation	237	287	303	17
Total RDT&E	**57536**	**61827**	**64909**	**3082**
Total DOD S&T	**11232**	**10297**	**12581**	**2284**

Sources: AAAS R&D Funding Update, 'DOD Receives Record R&D Portfolio, $12.6 Billion for S&T Programs', September 29, 2003 (revised Dec. 11, 2003)

Given the blurred dividing line between defence and security functions and technologies, a comparison of military and non-military security-related research would theoretically make sense. However, since the idea of matching the U.S. defence research budget is unrealistic (and may not even be desirable), an ESRP should rather take the U.S. spending on Homeland Security research as a reference.

In the field of Homeland security research, where the need for emerging and innovative technologies is particularly high, one third of R&D funding is spent on upstream research (Science and Technology, S&T, according to U.S. budget terminology). Based on a total Homeland Security R&D budget of $ 3.7 billion (FY 2003), American S&T investment in this area represents roughly $1.2 billion per annum. On top of that come numerous security-related research activities that are funded by the DOD.

The minimum budget of an ESRP should be €1 billion p.a., on top of existing funding.

There is no reason why European security research should not be funded at a level similar to the U.S. Calculated as a per capita investment, the U.S. spend more than four dollars on security-related S&T for each citizen. Using the same reasoning, this would mean that an overall EU security R&T budget of 1.8 billion for 450 million Europeans would be desirable. Such an investment would be an important contribution towards bolstering an EU-wide area of freedom, security and justice.

Although a precise assessment of national security R&T spending in Europe has not been established, it can nevertheless be assumed that Member States' efforts in this area are generally limited. Moreover, one must suppose that security research in the EU will not benefit as much from investments in defence research as in the U.S. To narrow the gap in security R&T, and to complement national and inter-governmental efforts, the minimum threshold of a Community-funded ESRP should therefore be 1 billion per annum.

In order to ensure an optimal use of resources, the ESRP funding level should increase progressively. The exact growth rate of the investment should be calculated during the Preparatory Action phase, based on a proper assessment of actual national expenditure in this area. The overall objective should be to bring the combined EU (Community, national and intergovernmental) security research investment level close to that of the U.S.

The ESRP level should be reached rapidly, with the possibility to progressively increase it further.

Conclusions and Recommendations

Considering the vast challenges that an enlarged European Union faces, this report has identified an urgent need to adapt the funding and the organization of European research activities to new security and technology realities.

To make this happen, we advocate:

a) Combining national, intergovernmental and Community research efforts across the civil-military continuum in the most efficient way;

b) Developing a specific European Security Research Programme (ESRP).

At the same time, we insist that the respect for civil liberties and ethical principles must govern all European research activities.

An ESRP can add value to the European project and is of strong social interest. It has the potential to foster industry's competitiveness and strengthen Europe's research base. It would promote cross-border cooperation and contribute to the EU policy on growth and competitiveness as established in Lisbon and Barcelona. Most importantly, it would help to enhance the EU's security, which is in itself a precondition of numerous Community policies (transport, energy, telecommunication, etc.). For all these reasons, an ESRP should be Community-funded.

An ESRP should not replace or duplicate Member States efforts. Its aim should be to support and supplement them, and to give them new coherence.

Having this in mind, we put forward the following recommendations:

1. A Community-funded ESRP ensuring the involvement of all Member States should be launched as early as 2007. Its minimum funding should be €1 billion per year, additional to existing funding. This spending level should be reached rapidly, with the possibility to progressively increase it further, if appropriate, to bring the combined EU (Community, national and intergovernmental) security research investment level close to that of the U.S.

2. An ESRP should fund capability-related research projects up to the level of demonstrators that are useful in particular for Internal Security in the EU and for CFSP/ESDP-missions.

3. In closing the gap between civil and defence research, an ESRP should seek to maximize the benefits of multi-purpose aspects of technology. In order to stimulate synergies, it should encourage transformation, integration of applications and technology transfer from one sector to the other.

4. An ESRP should focus on interoperability and connectivity as key elements of cross-border and inter-service cooperation. In this context, a kernel of architectural design rules and standards should be worked out at an early stage.

5. The rules governing an ESRP must suit the specificities of security research. The Commission should, in consultation with all relevant stakeholders, develop the necessary rules for IPR and technology transfer.

6. Recognizing that many requirements will be government-specified, new financing instruments should be created to enable research funding to be disbursed, if justified, at up to 100% of cost.

7. A 'Security Research Advisory Board' should be established to draw strategic lines of action to prepare the research agenda of an ESRP as well as to advise on the principles and mechanisms for its implementation. Moreover, it should identify critical technology areas where Europe should aim for an indigenous competitive capability. The Board should consist of high-level experts from public and private customers, industry, research organizations and any other relevant stakeholders.

8. Definition of customer needs will be key for the successful implementation of an ESRP. A mechanism should therefore be established at EU level to identify in consultation with potential customers, future capability needs for Internal Security missions.

9. Effective coordination must make sure that the ESRP does not duplicate but complements other European research activities whether funded at Community, national or intergovernmental level.

10. The Commission and the Council should ensure an effective and efficient liaison between an ESRP and the future 'Agency in the field of defence capabilities development, research, acquisition and armaments'.

11. The ESRP should take into account and, where appropriate, coordinate with research efforts of international organizations with responsibilities for global or regional security issues.

12. An ESRP should aim at fostering the competitiveness of the European security industries and stimulating the development of the market (public and private) for security products and systems. Implementing the Proposals for Action put forward in the Commission's Communication 'Towards a European defence equipment market' would greatly help to achieve this objective and to maximize the benefits of an ESRP.

Glossary and Acronyms

Asymmetric	Threat with consequences disproportionate to the means involved
CBRN	Chemical, Biological, Radiological, Nuclear
CFSP	Common Foreign and Security Policy
DoD	Department of Defense (U.S.)
ESDP	European Security and Defence Policy
ESRP	European Security Research Programme
FP	Framework Programme – the Community's multi-annual Research Programme
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security and Cooperation in Europe
R&D	Research and Development – research including the effort for the development of new products
RDT&E	Research, Development, Testing and Evaluation
R&T	Research and Technology – research for the development of new technologies, up to the level of demonstrators
S&T	Science and Technology
UAV	Unmanned Aerial Vehicle
UN	United Nations
WEAG	Western European Armaments Group

European Commission

Research for a Secure Europe – Report of the Group of Personalities in the field of Security Research

Luxembourg: Office for Official Publications of the European Communities

2003 — 30 pp. — 21.0 x 29.7 cm

ISBN 92-894-6611-1

This report was prepared by the Group of Personalities in the field of Security Research and published on their behalf by the European Commission.

For more information, contact:

European Commission
E-mail: rtd-pasr@cec.eu.int
http://europa.eu.int/comm/research/security/

15 KI-NA-21-110-EN-C

Research for a Secure Europe

Report of the Group of Personalities
in the field of Security Research

Publications Office
Publications.eu.int

ISBN 92-894-6611-1