EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Review of security measures in the Research Framework Programme

STUDY

EN 2010

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Review of security measures in the Research Framework Programme

STUDY

Abstract

This study provides an assessment of the EU "public-private dialogue" in security research and of the projects currently funded under the 7th Research Framework Programme (FP7), from the point of view of their contribution to the development of an area of freedom, security and justice. In this study, we ask two simple questions, deriving from the general objectives defined by the Stockholm programme. To what extent is EU-funded security research placed at the service of citizens? To what extent does it contribute to the strengthening of a single area of fundamental rights and freedoms?

PE 432.740 EN

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs

AUTHORS

Mr. Julien Jeandesboz
Mr. Francesco Ragazzi

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C: Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: alessandro.davoli@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

Manuscript completed in October 2010
© European Parliament, Brussels, 2010

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
ASD	AeroSpace and Defence Industries of Europe
CFR	Charter of Fundamental Rights
ESRP	European Security Research Programme
ESRAB	European Security Research Advisory Board
ESRIA	European Security Research and Innovation Agenda
ESRIF	European Security Research and Innovation Forum
FP	Community Research and Development Framework Programme
PASR	Preparatory Action on Security Research
PPD	Public-Private Dialogue
TFEU	Treaty on the Functioning of the European Union

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

Background

In February 2004, the European Commission launched a "Preparatory Action in the field of Security Research" (PASR) endowed with an estimated budget of 65 M€ for the period 2004-2006. This was complemented by a number of projects funded under the Community"s 6th Framework Programme (FP6). In September 2004, it further proposed the establishment of a "European Security Research Programme" (ESRP), to be funded over the period 2007-2013 under the Community's 7th Framework Programme, endowed with an envisaged budget of 1.4 Bn€.

Security research at the EU level is to be conducted through what the Commission, in a 2007 communication, has called a "public-private dialogue", involving key companies in the defence and security industry and "end-users" from national and European security agencies and services. High-profile venues established to bring together these constituencies, in particular the *Group of Personalities on Security Research* (GoP, 2003-2004), the *European Security Research Advisory Board* (ESRAB, 2005-2006) and most recently the *European Security Research and Innovation Forum* (ESRIF, 2008-2009), have been instrumental in establishing the priorities and outlook of current EU-funded security research.

In this study, we ask two simple questions, deriving from the general objectives defined for the EU's area of freedom, security and justice by the recently adopted Stockholm programme: **to what extent is EU-funded security research placed at the service of citizens? To what extent does it contribute to the strengthening of a single area of fundamental rights and freedoms?**

Aim

- Provide an overview of the "public-private dialogue" advocated by the European Commission.
- Propose a qualitative and quantitative analysis of research currently undertaken under the FP7's Security Theme.
- Examine the future development of EU security research and development activities as foreseen in the final report of the *European Security Research Forum* (ESRIF) and the Commission's "European Security Research and Innovation Agenda" of December 2009.

GENERAL INFORMATION

KEY FINDINGS

- **With regard to the "public-private dialogue":** EU security research and development activities have been mainly driven by a concern to bring together representatives from the ministries of Defence and Interior of the Member States and Associate countries, and representatives of major companies from the defence and security industries. In the process, representatives from civil society and parliamentarians, as well as bodies and organisations in charge of civil liberties and fundamental freedoms, including data protection authorities and fundamental rights bodies, have been largely sidestepped. **The outcome of this process is a dialogue that is limited in its scope, addressing security research through the concerns of security agencies and services and the industry, without taking into account the requirements flowing from the EU's internal area of freedom.**

- **With regard to security research undertaken in the framework of FP7-Security theme:** an overview of current security research projects sponsored through FP7 show an unequal distribution of funding, which is concentrated on a small number of participating countries and a small number of organisations, mostly major defence and security companies and applied research institutions. In addition, a large proportion of these projects is dedicated to developing technologies of surveillance, to the detriment of a broader reflection on the impact of such technologies for citizens and persons concerned with the EU's security policies.

- **With regard to future developments in the field of security research in the EU:** plans for the future development of EU-level security research, including the *European Research and Innovation Agenda* recently proposed by ESRIF, do not fundamentally challenge the abovementioned trends. While these proposals indicate a growing awareness for questions of fundamental freedoms and rights, they remain overly framed by the concerns of the defence and security industry and national and European security agencies and services.

KEY RECOMMENDATIONS

- The main **short-term recommendation** is that an in-depth evaluation of EU-sponsored security research should be conducted. We propose **four options**: an accounts and budgetary evaluation **through the European Court of Auditors**, a data-protection and privacy evaluation conducted by **the EDPS and/or the Art.29 Working Party**, a fundamental rights and freedoms assessment conducted **by the EU's Fundamental Rights agency**, and finally a full-spectrum evaluation conducted **under the auspices of the European Parliament's STOA unit**.

- The main **medium-term recommendation**, informed by the fact that the Commission is expected to table its first discussion paper on the future FP8 in the first months of 2011, is for the European Parliament to insist on: **1) reintegrating**

EU security research under the responsibility of DG Research instead of DG Enterprise; 2) earmarking a certain amount of future funds to be dedicated to security research for projects in the field of fundamental freedoms and rights (10 to 15%); 3) considering the development of a specific research theme on fundamental freedoms and rights, including in the context of EU internal and external security policies, in the future FP8.

1. INTRODUCTION[1]

Since the beginning of the decade, security research and development has become an important aspect of the European Union's policies with regard to the area of freedom, security and justice (AFSJ). In February 2004, the European Commission launched a "Preparatory Action in the field of Security Research" (PASR) endowed with an estimated budget of 65 M€ for the period 2004-2006. This was complemented by a number of projects funded under the Community's 6th Framework Programme (FP6)[2]. In September 2004, it further proposed the establishment of a "European Security Research Programme" (ESRP)[3], to be funded over the period 2007-2013 under the Community's 7th Framework Programme (FP7), endowed with an envisaged budget of 1.4 Bn€.

This briefing note presents a mid-term evaluation of the FP7 Security theme and more broadly of EU activities in the field of security research and development, paying particular attention to the so-called "public-private dialogue" in this area launched by the European Commission in 2007.

This assessment is all the more timely as the European Council has recently adopted the Stockholm programme for the AFSJ, which aims at "serving and protecting citizens". To a certain extent, the Stockholm programme does away with some of the misgivings of its predecessor the Hague programme, by giving priority to the AFSJ as "a single area in which fundamental rights and freedoms are protected"[4]. These elements provide us with two simple questions against which EU security research and development should be evaluated: **to what extent is it placed at the service of citizens? To what extent does it contribute to the priority of a single area of fundamental rights and freedoms?**

This briefing note will:

- Provide an overview of the "public-private dialogue" advocated by the European Commission.
- Propose a qualitative and quantitative analysis of research currently undertaken under the FP7"s Security Theme.
- Examine the future development of EU security research and development activities as foreseen in the final report of the *European Security Research Forum* (ESRIF) and the Commission's "European Security Research and Innovation Agenda"[5] of December 2009.

[1] The authors would like to thank Didier Bigo for his precious comments and insights in the researching and writing of this note.

[2] Mainly under the thematic area "Towards a global dependability and security framework" of the "Information Society Technologies" priority. See Bigo & Jeandesboz, 2008, for an assessment of PASR and FP6 security research.

[3] European Commission. *Security Research : the Next Steps*. COM(2004) 590 final.

[4] Council of the European Union. *The Stockholm Programme – An open and secure Europe serving and protecting citizens*. 5731/10, p.10.

[5] European Commission. *A European Security Research and Innovation Agenda – Commission's initial position on ESRIF"s key findings and recommendations*. COM(2009) 691 final, 21 December 2009.

2. PUBLIC-PRIVATE DIALOGUE IN SECURITY RESEARCH: OVERVIEW AND ASSESSMENT.

KEY FINDINGS

- While the notion of a "pubic-private dialogue" in security research was officialised in 2007, the European Commission (through its DG Entreprise and DG Research) **has in fact sponsored such a "dialogue" since the early 2000s**.
- As it currently stands, the public-private dialogue in security research at EU level is both **closed** and **limited.**
- It is a **closed dialogue**, because it has only involved representatives from national ministries of Defence and Interior and representatives of the defence and security industry, sidestepping representatives of civil society and parliamentarians as well as bodies and organisations concerned with fundamental freedoms and rights.
- It is, accordingly, a **limited dialogue**, because it has focalised almost exclusively on matters of security and industry, to the detriment of a broader discussion of the impact of technology for security purposes on fundamental freedoms and rights.

The notion of a "public-private dialogue" (PPD) in security research was coined in an eponymous communication tabled by the European Commission in September 2007, prepared jointly by the services of DG Enterprise and Industry (hereafter DG Enterprise) and DG Justice, Liberty, Security (hereafter DG JLS). **It has to be noted, however, that the 2007 communication merely officialised a process that had already been taking place for some years**:

- The issue originally surfaced in 1996-1997, when the Commission attempted to persuade Member States to lift their opposition to the development of a European defence procurement market in a context of dwindling national defence spending and large-scale restructuring in the industry[6].
- In April 2002, the European Parliament adopted a resolution on European defence industries calling in particular for the development of "a defence equivalent of the Advisory Council on Aeronautics Research in Europe so that European research in the defence field can be better pooled and coordinated"[7].
- The European Commission was keen on addressing this matter in a context where initiatives with regard to the defence industry were stalled due to the reluctance of Member States to further liberalise a domain of sovereign importance. In its 2003 communication on 'Towards an EU defence equipment policy', it offered its auspices to develop "advanced research in the field of 'global security'"[8] bringing together the European defence and security industry and European and national security agencies and services. It is from this initial move that the EU 'public-private dialogue' in security research was initiated.

[6] European Commission. *Implementing European Union strategy on defence-related industries*. COM(97) 583 final.

[7] European Parliament. *European defence-related industries : European Parliament resolution on European defence industries*. P5-TA(2002)0172, p.1.

[8] European Commission. *European defence – Industrial and Market Issues: Towards an EU Defence Equipment Policy*. COM(2003) 113 final, p.16.

In the following pages, we provide an overview of the PPD (2.1.) and an assessment of its effects (2.2.)[9].

2.1. Overview of the PPD: high-level venues in the field of security research.

One of the most concrete manifestations of "public-private dialogue" in security research has been the convening by the European Commission of three consecutive high-level venues between 2003 and 2009, bringing together representatives from major companies in the European defence and security industry and high-level officials of European institutions and national ministries: the *Group of personalities on security research* (hereafter GoP), the *European Security Research Advisory Board* (hereafter ESRAB) and the *European Research and Security Forum* (ESRIF). While different in format, however, these different venues have brought together **very similar constituencies**, and have been **very influential in terms of policy-making**, **insofar as they have defined both the process and priorities of EU-funded security research**: the GoP and ESRAB final reports have laid the ground for and established the structures and priorities of the FP7-Security Theme, while the ESRIF final report purports to do the same with EU security research until 2030.

2.1.1. The *Group of Personalities on Security Research* (2003-2004).

The *Group of Personalities on Security Research* was convened in 2003. It brought together executives from several major European companies with activities in the field of defence and security (Diehl Stiftung, Finnemecanica, EADS, Ericsson, INDRA, Thales, BAE Systems, Siemens), higher level officials from the European institutions (commissioners Busquin – Research – and Liikanen – Entreprise and Information Society – as well as CFSP High representative Javier Solana) and members of the European Parliament, former senior governmental executives (former president of Finland Martti Ahtisaari, former prime minister of Sweden Carl Bildt) and selected representatives of think tanks and national research institutions (EU Institute for Security Studies, Fondation pour la recherche stratégique, TNO). The GoP published its final report, entitled *Research for a Secure Europe*, in 2004[10].

The GoP report establishes the rationale that has been informing PPD in security research since. **Security research is first and foremost about "market coherence"** since it involves "research destined primarily for public sector applications". In order to achieve "a common understanding about requirements", it is therefore considered crucial to ensure "[c]ontinuous dialogue between research sponsors, customers and industry"[11]. In other words, the PPD has, from the onset, been established as **a process aiming at establishing the proper market conditions for the industry to develop and commercialise technological products in the field of security**, by creating meeting points between so-called "end-users" (European and national security services and agencies) and producers.

[9] This section will also draw from previous research conducted on this question – see Bigo & Jeandesboz, 2008, 2010 ; Burgess & Hanssen, 2008 ; Hayes, 2009.

[10] European Commission. *Research for a Secure Europe: Report from the Group of Personalities in the field of Security Research*, Luxembourg: Office for Official Publications of the European Communities, 2004.

[11] *Research for a secure Europe*, p.23.

2.1.2. The *European Security Research Advisory Board* (2005-2006).

The *European Security Research Advisory Board* was convened by the European Commission in April 2005[12], as part of the follow-up to the Commission's communication on next steps in security research[13] and **a direct development of the recommendations of the GoP final report**. It brought together fifty representatives from the defence and security industry, national governmental agencies in the field of security, defence and research, and from a selection of research bodies and think tanks. In terms of participation from the industry, one finds the same constituency that was already present in the GoP, *i.e.* major defence and security companies such as BAE Systems, Diehl, EADS, Ericsson, Finnemecanica, Sagem, Siemens, or Thales. The same holds true for the think tank and academic sectors, with major national institutions such as the Fondation pour la recherche stratégique (France), the Istituto Affari Internazionali (Italy), the EU Institute for Security Studies, TNO (Netherlands) or the Royal United Service Institute for Defence and Security Studies (RUSI, United Kingdom). It should be noted that ESRAB included a broader selection of representatives from national security agencies and services, whether police, border guards or defence ministries. ESRAB also featured a consistent participation from the European Commission's directorate generals[14].

The ESRAB final report largely endorses the orientations set out in the GoP report. Defining itself as a "successful vindication of the concept of bringing together 'demand' and 'supply'"[15], it advocates a "capability-based approach" for the FP7 Security theme, structured around four priority areas: border security, protection against terrorism and organised crime, critical infrastructure protection, restoring security in cases of crisis[16]. **Absent from these priorities, however, are considerations with the broader impact of these technologies, particularly with regard to data protection and privacy, but also more widely in terms of fundamental freedoms and rights.**

2.1.3. The *European Security Research and Innovation Forum* (2008-2009).

The *European Security Research and Innovation Forum* was established in September 2007, and counted 65 members. While the GoP and ESRAB were Commission initiatives, ESRIF was established under the joint auspices of the Member States and the Commission. Chaired by the former EU Counter-Terrorism Coordinator Gijs de Vries, its September 2008 intermediate report describes ESRIF as "an informal and voluntary group of experts coming from the demand and supply side of security technologies and solutions as well as from societal organisations"[17]. In terms of constituency, ESRIF is comparable to ESRAB: a **similar selection of representatives from larger corporate groups** in the field of defence and security and research institutions, with a broader group of representatives from ministries of Defence and Interior and police forces (including non-EU countries such as Croatia, Switzerland or Turkey). The objective of ESRIF, as stated by chairman Gijs de

[12] Commission Decision of 22 April 2005 establishing the European Security Research Advisory Board (2005/516/EC), Official Journal of the European Union, L191, 70-72, 22 July 2005.

[13] COM(2004) 590 final.

[14] Budget, Entreprise and Industry, Environment, Information Society and Media, Justice, Liberty and Security, Joint Research Centre, Internal Market and Services, External Relations, Research, Health and Consumer Protection, Taxation and Customs Union, and Energy and Transport.

[15] European Commission. *Meeting the challenge: the European Security Research Agenda, a report from the European Security Research Advisory Board*. Luxembourg: Office for Official Publications of the European Communities, 2006.

[16] *Meeting the challenge*, p.18.

[17] European Commission. *European Security Research and Innovation in support of European security policies: intermediate report*, Luxembourg: Office for Official publications of the European Communities, 2008, p.7.

Vries in the foreword to the report, is to "propose a European agenda for research and innovation in the field of security capable of guiding European institutions, governments and the private sector in the coming two decades"[18].

ESRIF delivered its final report in December 2009[19]. Insofar as it aims at defining future directions of EU-sponsored security research up to 2030, the conclusions of this report require a more detailed discussion, which will be developed in the last part of this briefing note (Section 4 below).

2.2. Assessment of the PPD.

As we have seen, high-level venues for dialogue between public and private stakeholders in the field of security research have been characterised so far by a fairly strong degree of homogeneity in terms of constituency, and a notable policy impact. This, we argue, raises a twofold issue with regard to the PPD promoted by the European Commission: more precisely, it establishes the PPD both as a **closed** dialogue and a **limited** dialogue. In this respect, the PPD runs the risk of reproducing a situation that used to characterise national defence procurement markets, *i.e.* **the constitution of intimate links between specific sectors of the public administration and a set of industrial "champions", which is arguably an obstacle to the constitution of a dynamic market as well as to transparency of the process for citizens**.

2.2.1. A closed dialogue for the sake of "market coherence": making security policy without the citizen.

The ESRIF final report argues that "ESRIF role is not to define security policy: it strives to inform decision making at industrial, national and European level"[20]. One nonetheless has to acknowledge that **venues such as the GoP, ESRAB and ESRIF have a policy impact, which in turn raises a number of questions with regard to accountability**. This, incidentally, is openly recognised by the co-chairmen of ESRAB who, in their preface, stress that "[i]t is rare on a national level, but even more so at European level, that end-users of security research results jointly define the required medium-term research developments alongside the suppliers and performers of security research"[21].

Security research, in this respect, does not only involve technical discussions about "capability development" or technological efficiency, **it is part of the policy-making process**. Indeed, the GoP report laid the ground for the ESRP, and the establishment of ESRAB, and the ESRAB report, in turn, framed the priorities for the FP7 Security theme and the creation of ESRIF. The European Parliament has pointed out this fact in its 2006 resolution on the Commission's communication on "Next steps in security research" where it "urges […] a balanced involvement of industrial representatives, research sponsors and public and private customers, scientific research bodies, public institutions and representatives of civil society"[22]. The Commission has officially responded to this request by highlighting that ESRIF would include "**a balanced representations of all stakeholders** in security research from the public and private sectors, i.e. industry,

[18] ESRIF intermediate report, p.5.

[19] ESRIF. *ESRIF Final Report*. Brussels, December 2009.

[20] ESRIF Final Report, p.12.

[21] *Meeting the challenge*, p.5.

[22] European Parliament. *Security Research: European Parliament resolution on Security Research – the Next Steps (2004/2171(INI))*. Official Journal of the European Union, C133 E, 8 June 2006, p.138 (p.135-140).

research establishments, public and private end-users, civil society organisations, European institutions, in particular the European Parliament, and European organisations"[23].

The need for a "balanced representation" appears to have come as an afterthought, and the extent to which this has been realised in the context of ESRIF is questionable. As we have shown in our overview of the PPD, there is a strong degree of homogeneity within the core participants in the GoP, ESRAB and ESRIF. Out of the companies that participated in the GoP, three (EADS, Finmeccanica, Thales) counted representatives in the two subsequent venues, while the other were also represented in ESRAB (with the exception of Spanish company Indra). Some, such as Sagem, came in at a later stage (ESRAB and ESRIF). "Research establishments", in this context, comprise mainly a handful of established think tanks such as the *Fondation pour la recherche stratégique* (Paris), *Istituto Affari Internazionali* (Roma), the EU Institute for Security Studies or the *Royal United Service Institute for Defence and Security Studies* and research sponsoring bodies such as the *Netherlands Organization for Applied Scientific Research* (TNO, in GoP, ESRAB, ESRIF) or the *Fraunhofer-Gesellschaft* (ESRAB and ESRIF). The progressive widening of participation in these various security research venues, in this respect, **has played out mostly to the benefit of officials from national and European[24] security agencies and services**, whether police or military bodies. ESRIF, the latest and arguably farthest reaching of these venues, is a case in point:

- Former Ministry of Interior of Slovenia Dragutin Mate replaced Gijs de Vries at the head of ESRIF in November 2008. ESRIF vice-chairs were Giancarlo Grasso, senior advisor to the chairman of Italian defence and security company *Finmecannica* and Jürgen Stock, vice-president of the German Federal Police (*Bundeskriminalamt*, BKA).
- Out of 65 official members in the forum, 34 are officials from national and European security agencies and bodies, 16 represent the defence and security industry, 9 originate from the academic sector and 5 from public or private think tanks: out of this count, only 5 ESRIF members can be construed, due to overlapping responsibilities mainly, as representing "civil society"[25].
- Within the 660 "stakeholders" participating in the 11 working groups established for the purpose of drafting the ESRIF report, Statewatch researchers find that 66% (433) come from the defence and security industry (ASD[26], EADS, Finmeccanica and Thales account for 102 participants), 30% (200 participants) from national and European security services and agencies, **and only 1,4% (9 participants) from "civil society", out of whom no representative from a civil liberties or privacy organisation[27]**.

[23] COM (2007) 511 final, p.10.

[24] Europol was represented both in ESRAB and ESRIF, while the head of the Capacity Building Unit of Frontex participate in ESRIF.

[25] See Hayes, 2009, p.23 ; Bigo & Jeandesboz, 2010, p.5.

[26] The *Aerospace and Defence Industries Association of Europe* which brings together European national associations of aerospace and defence companies. It is currently chaired by PierFrancesco Guarguaglini (chairman and CEO of Finmeccanica) and counts among the corporate members of its governing council a number of companies that have been very involved in the various venues related to European security research, such as BAE Systems, Diehl (Aerospace division), EADS (Astrium division) or Finmeccanica.

[27] Hayes, 2009, p.24.

To be more accurate, all three venues have involved members of the European Parliament, but the GoP is the only one that acknowledges them as formal members[28], while ESRIF for instance mentions the involvement of MEPs as "observers" only.

The "dialogue" advocated by the European Commission has thus turned out to be a **closed dialogue** with a narrow definition of stakeholders centred as developers, sellers and buyers of technical products. This, as we will show below, has had an important effect on how security issues have been framed in the context of the PPD.

2.2.2. A limited dialogue focused on "capability development": privileging security and industry over fundamental freedoms and rights.

A crucial element of concern with regard to the PPD is the way in which it has contributed to frame security policy. Two elements surface in the GoP report, which have become recurrent features in the rationale of the EU-level PPD in security research:

- **Technology as a mandatory component of security policies.** The GoP report suggests that "technology itself cannot guarantee security, but security without the support of technology is impossible […] In other words: technology is a key "force enabler" for a more secure Europe"[29].
- **A capability oriented security research programme.** The GoP's main recommendation is the establishment of the ESRP, which it suggests should be "capability-driven", *i.e.* dealing with the following questions: "[w]hat are the threats?", "[w]hat are the missions required to tackle these threats?", "[w]hat are the capabilities needed to accomplish these missions?" and "[w]hat are the technologies – or combination of technologies – that can provide the necessary capabilities?"[30]. In other words, the report advocates **a research programme exclusively geared towards the preoccupations of so-called "users"** – *i.e.* national and European security agencies and services – to the detriment of a broader agenda which would incorporate preoccupations with the legal, political and social implications of technology-intense security policies.

In this regard, it is worth recalling again the wording of the European Parliament's resolution on security research, which called "on the Commission **to take account of the notion of the 'public interest' of security research**, both for the European Union and the Member States in order to avoid the risk of funding projects which are **not in line with political priorities or with certain public interest or privacy protection obligations, or with the protection of human rights, civil liberties and private life**"[31].

In the ESRAB final report, however, this concern for "public interest" is addressed through a discussion on "ethics" – and is awarded a single page in a document numbering eighty:

- The main recommendation of the report lies in the suggestion to "review existing codes of conduct, best practices, etc. as to the ethical use of security technologies, and to develop new ones where shortfalls exist"[32]. It is important to recall, however, that **fundamental rights and freedoms are not only about ethics, but about rule of law**, and as such, involve conformity with existing European and national

[28] Karl von Wogau (EPP), Eryl McNally (S&D), Christian Rovsing (EPP), Elly Plooij-van Gorsel (ELDR).

[29] *Research for a secure Europe*, p.12.

[30] *Research for a secure Europe*, p.16.

[31] 2004/2171(INI), p.139.

[32] ESRAB Final Report, p.60.

legislations regarding privacy[33], but also other fundamental rights such as the right to free movement or human dignity[34].

- Accordingly, the report suggests that "[i]n research projects dealing with sensitive issues where ethics and justice meet security all relevant actors (lawyers, industry, data protection officers) must work together to achieve a fair and effective balance"[35]. This **specification is self-defeating** in two respects. Firstly, because the involvement of stakeholders other than security agencies and services and industry in the development of security research has not been achieved so far. Secondly, because it is informed by the notion of a "balance" between security (framed in the ESRAB report as a "right to security") and fundamental freedoms and rights. **From a legal point of view, there is no such thing as a right to security**. The right to safety, embodied for instance in the British *Habeas Corpus*, is a different notion that includes **the right for the individual to be protected from the abuses of the state:** Article 6 of the Charter of Fundamental Rights specifies, in this respect, that **"Everyone has the right to liberty *and* security of person", which excludes the possibility of a "balance" type of reasoning.**

As we will see in the following sections, however, very little has been done in the way of either involving lawyers and data protection practitioners or scholars in the legal, political and social sciences, in the "public-private dialogue" and in security research broadly speaking.

[33] In particular new Article 16 of the Treaty on the functioning of the EU (TFEU) ("Everyone has the right to the protection of personal data concerning them"), Article 7 ("Respect for private life") and Article 8 ("Protection of personal data") of the Charter of Fundamental Rights (CFR), and the Convention ETS No 108 of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981).

[34] Article 1 of the CFR for human dignity, Article 45 CFR for freedom of movement and residence (including for third country nationals within the framework of the Treaty).

[35] ESRAB Final Report, p.60.

3. ANALYSIS OF SECURITY RESEARCH UNDER THE FP7 SECURITY THEME.

KEY FINDINGS

- Although the FP7 is open to institutions from all EU member states and associated third countries, **organisations from five states (France, U.K., Italy, Sweden, Israel) have obtained the majority of allocated funds**.
- Three types of institutions (transnational defence companies, applied research centres and governmental institutions) have obtained **the majority of funds**. They further account for the **largest share of individual participation in, and coordination of, projects**. This takes place **at the expense of universities and NGOs, which remain largely under-represented**.
- As a consequence, the overall assessment of the FP7 reflects **the marginal interest for the ethical, social and political impact of security technologies**; yet the reflection around these themes should develop in parallel to the evolution of security technologies.

As mentioned previously, EU-funded security research was initiated through the PASR, which sponsored 39 actions and pilot projects for a total Community contribution of 44.5 M€[36]. A third of these projects were coordinated by major defence and security companies such as Thales, EADS, Finmeccanica, Sagem and their European association ASD – most of which, incidentally, were involved in the proceedings of the GoP and ESRAB. These companies also participated in two-thirds of the actions and pilot projects funded under the PASR[37].

The European Commission established the FP7 Security Theme (hereafter FP7-ST) following the recommendations of the GoP on the creation of a European Security Research Programme. **Unlike the rest of FP7 research schemes that fall within the remit of DG Research, however, the Security Theme has been attributed to DG Enterprise and Industry.** According to the Commission's initial figures, funding earmarked for the FP7-ST amount to 4% of the FP7's Cooperation Theme[38]. This, incidentally, implies that the Community contribution to the FP7-ST over the 2007-2013 period represents more than 30 times the amount committed to the 3-year PASR.

Previous evaluations of security research conducted on behalf of the European Parliament focusing on FP6 and PASR projects[39], have:

- found them **to be driven mainly by a technical concern with more sophisticated technologies, rather than with political concerns for the limits of security, fundamental freedoms and rights.**
- **identified a lack of integration between technical research, on the one hand, and legal, social and political research, on the other.**

An early assessment (as of May 2009) of security research schemes under the FP7-ST identified two problematic trends:

[36] For an overview see Bigo & Jeandesboz, 2008 ; Hayes, 2006.

[37] Hayes, 2009, p.12.

[38] Totalling about 1.350 M€ out of a total of 32.650 M€ for the whole Cooperation Theme.

[39] Bigo & Jeandesboz, 2008.

- The first one was the **continuing predominance of the companies that had participated in the GoP and ESRAB**: out of 45 projects, these organisations totalled 32 individual participations, and had taken the lead on 7 projects – the strongest record being Thales, which was leading 3 projects and participating in 10[40]. This, in turn, raised two questions:
  - firstly, of the political implications of having private companies defining public policies and being major beneficiaries thereof;
  - secondly, of the economic objective of fostering through FP7-ST research the strengthening of the "European industrial and technological basis", particularly with regard the low participation of small and medium enterprises (SME).
- The second problematic trend was **the overall focalisation of FP7-ST research on engineering issues and technological demonstration and development**. Within the 45 projects documented under FP7-ST at the time, only three (DETECTER, INEX and the social science component of the GLOBE project) offered to investigate the legal, political and social implications of technological developments within FP7-ST. It is fair to say, in this regard, that the Commission has altogether disregarded the call of the European Parliament for "a more balanced interaction between research in the natural sciences and technology and other sciences, in particular political, social and human sciences"[41] in the selection of the projects to be funded under FP7-ST.

The next pages will propose a full mid-term assessment of the FP7-ST, in order to evaluate whether earlier concerns about EU-funded security research have been addressed. Although there are undoubtedly other programmes within which security research has been and is currently sponsored by EU funds[42], we will concentrate on the projects currently registered (as of September 2010) under the Security Theme within the Commission's CORDIS database.

3.1. General remarks about FP7 projects.

In order to clarify our analysis of FP7-ST, it is necessary to briefly summarize some key elements about the general functioning of the FP7.

Coordinating and partner institutions. Each FP7 project is organized around a main coordinating institution and a certain number of partners, which varies in the case of the security theme from 0 (single partner projects) to up to 28 in addition to the main partner (for example for the PROTECTRAIL project). Since the lead institution or coordinator is the institution that acts as the point of contact with the European Commission – **for FP7-ST, DG Enterprise and not DG Research** - it should be considered a primus inter pares institution. In addition, the number of projects a certain institution coordinates gives an indicator of the centrality of the actor within the FP7 financing networks.

Funding. To analyse funding patterns in FP7, one needs to take into account the Community contribution, which comprises the funds effectively allocated from the EU budget, and the project's total cost. The Community contribution sometimes covers the totality of the costs of a given project, but in most cases only a part of the project's costs. Apart from a few exceptional cases, the majority of projects are funded from 50% up. The

[40] Bigo & Jeandesboz, 2010, p.4.

[41] 2004/2171(INI), p.138.

[42] For instance the EU framework programme on "Security and Safeguarding Liberties", divided into two specific instruments – "Prevention of and Fight against Crime" and "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks". This programme was established for the period 2007-2013 and endowed with an overall budget of 745 M€, under the auspices of DG Home.

totality of the projects costs evaluated in this note amount to € 443,225,175 with a FP7 contribution of € 304,371,907, i.e. a participation of 68.67%.

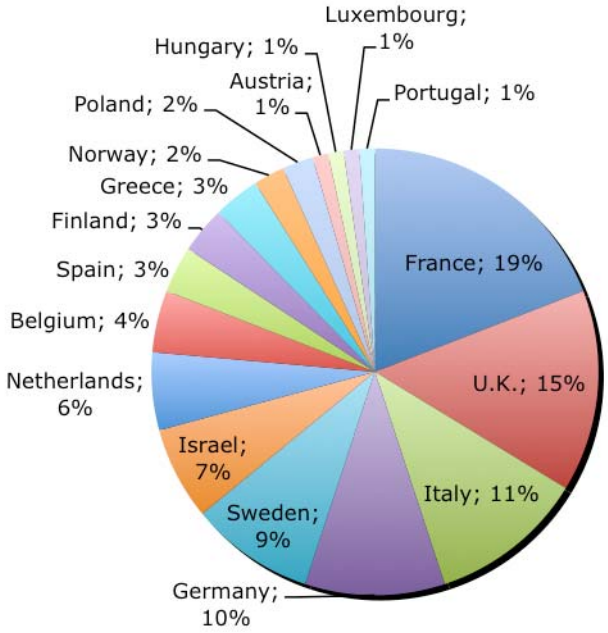
Eligible countries. In theory, any country in the world can apply for FP7. However, not all countries have equal access to funding. Institutions from EU member states enjoy unrestricted access, as well as third countries associated with the program (which pay a share of the overall budget of FP7). These are the EEA countries (Iceland, Norway, Lichtenstein), candidate countries Croatia, Turkey, as well as Israel and Switzerland[43].
Eligible institutions. Institutions that are entitled to apply for FP7 funding include: 1) research groups at universities or research institutes; 2) companies intending to innovate, 3) small or medium-sized enterprises (SMEs); 4) SME associations or groupings; 5) public or governmental administration (local, regional or national); 6) early-stage researchers (postgraduate students); 7) experienced researchers; 8) institutions running research infrastructures of trans-national interest; 9) organisations and researchers from third countries; 10) international organisations; 11) civil society organisations.

3.2. An unequal geographical distribution.

The first point in the assessment of FP7-ST is that the geographical repartition of projects reflects the predominance of large EU member states, at the expense of smaller countries.

3.2.1. Coordinated projects.

A first indicator of the dominance of large EU member states in the attribution of FP7-ST funding is the number of projects per country of origin of the main coordinating partner: France (19%), the United Kingdom (15%), Italy (11%) and Germany (10%) account for more than 55% of FP7-ST projects in this regard (See figure 1 and Table 1).



When looking at the geographical distribution of the total amount of FP7 funding per country of coordinating institutions (Figure 2), a similar pattern can be found. France, Italy, the U.K. and Sweden alone represent about 59% of the EU contribution. An exception is the percentage of total projects coordinated by Germany, which represents 10%, while only 7% of EU allocated funds go to German Institutions.

Figure 1. Number of Coordinated Projects per country of origin

COUNTRY OF COORDINATOR	PROJECTS	TOTAL COST	EU CONTRIBUTION
France	17	EUR 85,528,083	EUR 56,530,448
U.K.	13	EUR 69,406,722	EUR 46,671,386
Italy	10	EUR 67,655,012	EUR 34,364,059

[43] For more information about eligibility, please refer to http://ec.europa.eu/research/fp7/understanding/fp7inbrief/who-apply_en.html

Germany	9	EUR 25,870,000	EUR 19,570,718
Sweden	8	EUR 45,271,960	EUR 30,646,558
Israel	6	EUR 35,835,079	EUR 23,499,631
Netherlands	5	EUR 28,170,000	EUR 20,960,000
Belgium	4	EUR 10,178,548	EUR 7,567,430
Spain	3	EUR 5,629,891	EUR 4,488,428
Finland	3	EUR 5,842,208	EUR 4,281,376
Greece	3	EUR 21,787,478	EUR 15,689,026
Norway	2	EUR 7,362,082	EUR 5,470,248
Poland	2	EUR 34,766,815	EUR 13,989,332
Austria	1	EUR 831,279	EUR 831,279
Hungary	1	EUR 1,210,000	EUR 850,596
Luxembourg	1	EUR 3,200,000	EUR 2,110,000
Portugal	1	EUR 1,080,000	EUR 820,032

Table 1. Coordinated projects per country of origin

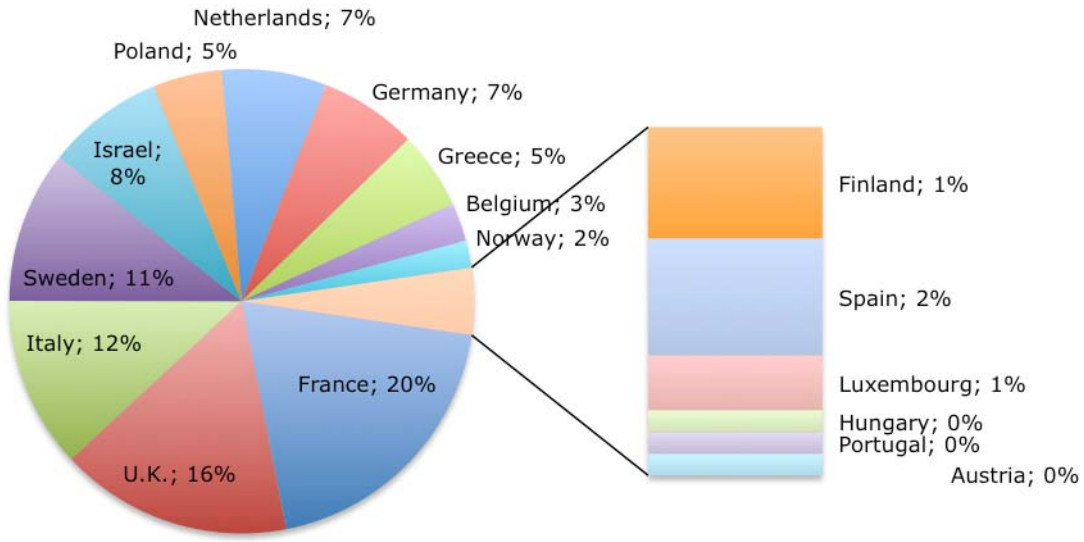


Figure 2. FP7's financial contribution per coordinator's country of origin

3.2.2. Number of individual participations.

Another indicator of the predominance of certain countries is the total number of participation of institutions, both as coordinators and partners, within FP7-ST projects. French, British, Italian, German and Spanish institutions account for the majority of participating institutions (55%) within the European Union.

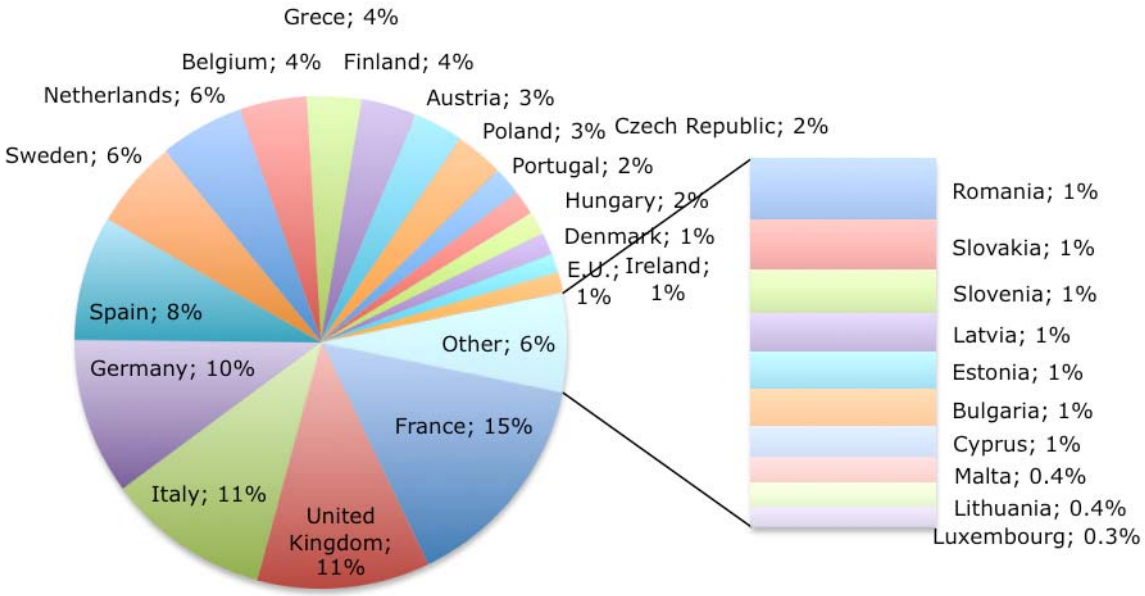


Figure 3. Number of participations per country of origin (EU)

In terms of the participation of non-EU countries, we witness an important number of companies located in associated countries, with Israel accounting for 33% of the non-EU funding, followed by Norway (27%), Switzerland (15%) and Turkey (9%).

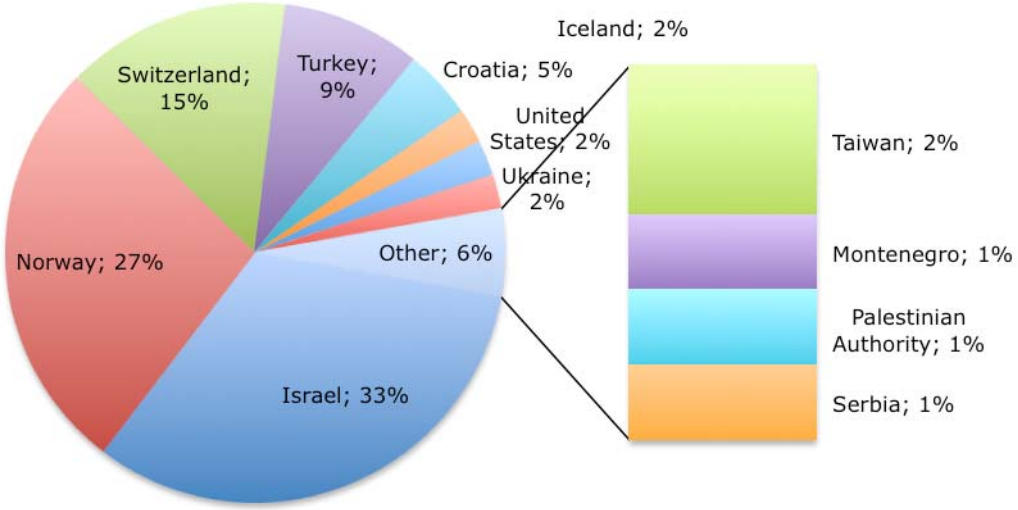


Figure 4. Number of participations per country of origin (Non-EU)

3.3. An industry-oriented research scheme: the predominance of major defence and security groups and the marginalisation of social science research.

3.3.1. The persistent domination of major defence and security companies

As outlined in 3.1.2. a wide variety of organizations and institutions are encouraged to apply for EU funding through the FP7 scheme. The analysis of coordinating institutions as well as partner **institutions confirms, however, the trend outlined in previous evaluations. It is mostly large defence companies, the very same who have participated in the definition of EU-sponsored security research which are the main beneficiaries of FP7-ST funds**.

This can be observed, firstly, at the level of number of coordinated projects, as shown in Figure 5

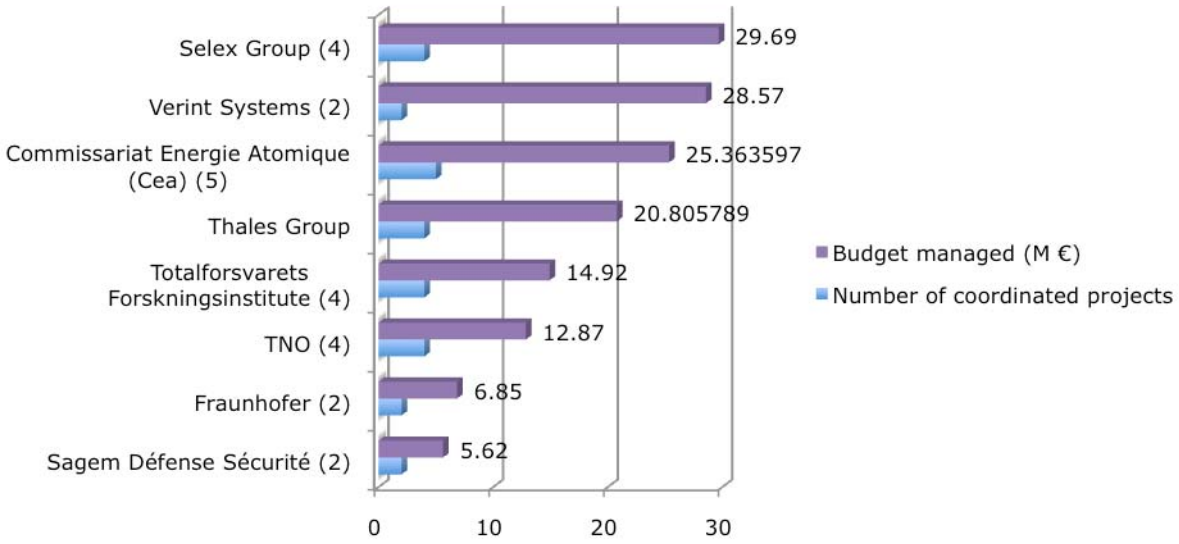


Figure 5. Organisations coordinating more than one project (Top 8)

But also in the number of participations obtained by these organisations in FP7-ST research projects, as Figure 6 shows:

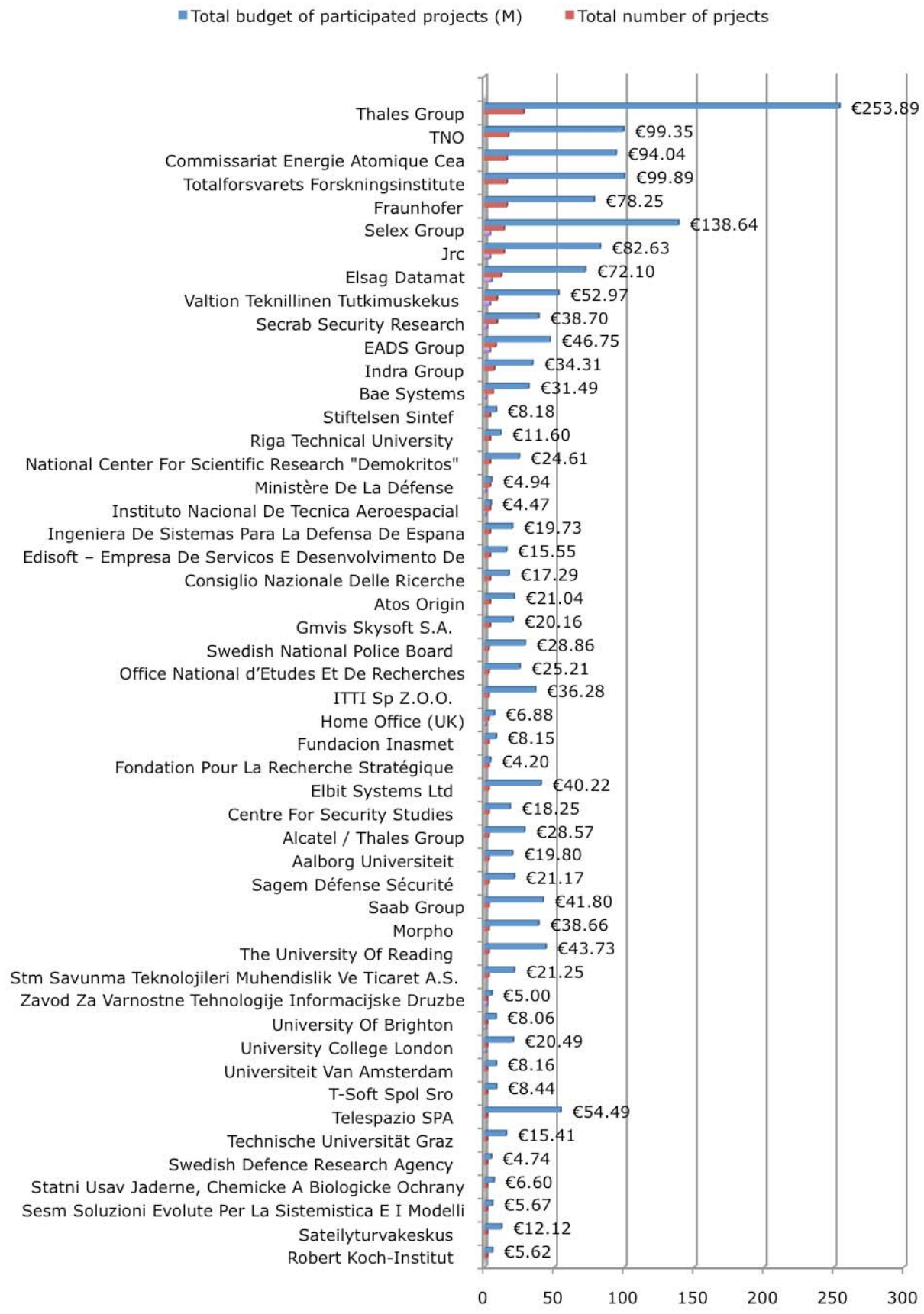


Figure 6. Top 50 of individual participations (per project budget).

Figure 6 highlights several features of the distribution of FP7 funds:

- Organisations which obtain the largest number of projects are mostly of three kinds:
  - Major defence and security companies (Thalès, Selex, Sagem etc)
  - Major "applied research" institutions, (TNO, Fraunhofer, VTT etc.)
  - Public research institutions (Forsvarets Forskninginstitut, CEA etc.)

- The overall quantity of funds linked to specific organisations is unevenly distributed. For example, on the total sum of € 443,2 million for the 91 FP7 projects analyzed in this note, **companies such as the Thales group are involved in roughly one third of the projects (27), representing more than half the FP7-ST (57%) in terms of projects' total worth (€ 253.8 million).**

- Only 6 universities (Riga, Reading, Brighton, UCL, Amsterdam, Graz) and no NGOs are part of the top 50.

3.3.2. A marginal interest for social and political impact of security policies and technologies.

Security research conducted under FP7-ST highlights an evolving landscape of security practices and uses of technology for security purposes. In what follows, we provide an overview of the initiatives distributed by key domains of research:

- Biometrics and identification
- Detection and surveillance
- Exchange of information, risk analysis and risk anticipation
- Critical infrastructure protection, crisis management and public safety
- Freedom and privacy

3.3.2.1. Biometrics and identification

Biometrics and identification projects represent € 21 million, i.e. about 4.76 % of the total costs of the 91 FP7s. The two projects specifically focused on biometric technologies are EFFISEC, which aims at developing efficient biometric checkpoints, and MIDAS, aimed at the development of a self-contained portable instrument for producing DNA database compatible results.

3.3.2.2. Detection and surveillance

The focus on detection and surveillance – e.g. better communicating or integrated sensor systems, and improved imaging techniques – **constitutes a very large share (40.1%) of the projects, for a total budget of € 177 million**. This category counts 26 projects, such as IMSK aimed at developing an integrated Mobile Security Kit combining area surveillance, checkpoint control, CBRNE detection and VIP protection for mobile and temporary deployment; TALOS (Transportable Autonomous patrol for land border surveillance system) or SeaBILLA (Sea Border Surveillance) aimed at defining the architecture for European sea border surveillance systems, apply advanced technological solutions and develop and demonstrate improvements in detection, tracking, identification and automated behaviour analysis of vessels. Projects include proactive and behavioural detection, such as INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment). Among the main objectives of the INDECT project are for example to develop a platform for the registration

and exchange of operational data, acquisition of multimedia content, intelligent processing of all information and automatic detection of threats and recognition of abnormal behaviour or violence.

3.3.2.3. Exchange of information, risk analysis and risk anticipation

Another grouping of projects in FP7-ST focuses on technologies for exchanging information, either in a generic form or with security agencies as end-users. Work on exchange of information involves, in this context, research to make platforms more secure, as well as the enhancement of information exchange system in terms of inputs (the mixing of information from differentiated sources) and access (access via mobile devices for instance). Exchange of information, in this regard, it is also frequently associated with the capacity to anticipate risks, and to run risk analysis based on available stocks of information.

With 16 projects amounting to € 39.4 million this category represents about a tenth of all projects (8.9%). Projects are aimed at developing communication infrastructures and interoperability between security and government agencies (COMPOSITE, EMILI, SCIIMS), others develop tools based on new information technologies. The INDIGO project aims for example to research, develop and validate an innovative system integrating the latest advances in Virtual Reality, Simulation and Artificial Intelligence. A final type of projects is aimed at risk assessment, such as EURACOM, aimed at the integration of security systems, interconnectivity and interoperability as well as risk assessment and contingency planning for interconnected transport or energy networks.

3.3.2.4. Critical infrastructure protection, crisis management and public safety

Critical infrastructure and public safety, including the development of methodologies and tools for crisis management, constitute another major part of FP7 funded security research. Most of the projects detailed below focus on protective/reactive steps, but in some cases, they also involve the building of threats scenarios and risk analyses. **This category of projects represents another sizeable share of FP7-ST funding: €194,3 milion, ie 43.9% of the total number of projects analyzed.**

Projects are oriented in part towards the protection of critical infrastructure. PROTECTRAIL, for example, one of the largest projects of FP7-ST with a budget of € 21,7 million is aimed at the protection of the rail system. SUPPORT aims at the development of technologies for upgraded preventive and remedial security capabilities in European ports. First responder systems constitute another part of the projects, such as the E-SPONDER project, aimed at the development of information, command and control systems for first responders in the case of critical infrastructure events. Similar programs are SERICOM, SECUREAU CRISIS, COPE. In this respect, many programs put the emphasis on response to CBRNE threats (SPIRIT, FRESP, DECOSTESSC1).

3.3.2.5. Security knowledge, mapping and harmonization.

Although not very important in number and budget (€ 5,2 M, approximately 1.2%) several projects have as their explicit goal the survey of current knowledge in the security field. SECURECHAINS's work is oriented at reviewing the existing security sector industry, identifying available resources and developing links between primarily SMEs (similarly to OSMOSIS). ESCorTS aims at developing a roadmap for standardization in the area of cybersecurity of control and communication systems in Europe. LOGSEC aims at identifying the most promising R&D areas and gaps in logistics and supply chain security in order to develop further research.

3.3.2.6. Freedom and privacy

Research on freedom and privacy in the context of security technologies is clearly the weak component of FP7-ST. **Only 2 projects within FP7-ST have adopted a reflection on the ethical, legal, political and social implications of security technologies as well as research on "privacy preserving" technologies. Together, these two projects represent only € 4,8 M, i.e. 1.09% of the total budget.**

One project is the INEX project (Converging and conflicting ethical values in the internal/external security in continuum in Europe). The goals of the project are to explore the ethical consequences of the proliferation of security technologies, the legal dilemmas that arise from transnational security arrangements, the ethical and value questions that stem from the shifting role of security professionals and the consequences of the changing role of foreign security policy in an era when the distinction between the external and internal borders grows less distinct. In a similar vein, DETECTER aims at increasing the compliance of counter-terrorism with human rights and ethical standards in the rapidly changing field of detection technologies. The project addresses the increasingly international character of counter-terrorism, the increasing use of informal mechanisms for altering law-enforcement practice to meet the threat of terrorism, and the great variety of detection technologies and their uses.

3.4. Conclusion

This overview of security measures funded under FP7-ST requires further discussion.

Firstly, and although this is not the main concern of the present briefing note, the predominance of a handful of participating countries and organisations insofar as the coordination of, and participation in, FP7-ST projects**, raises a number of questions as to the industrial pertinence of such a funding scheme**. The aim of a EU-level industrial policy should aim at supporting economic, social and territorial cohesion, in accordance with Title XVIII Article 174 of the TFEU for instance[44].

With regard to the main concern of this briefing note, *i.e.* the contribution of EU-sponsored security research to an area of fundamental rights and freedoms, the overview of FP7-ST highlights that **EU-supported security research has strongly focused on meeting security "challenges" through technologies that allow for pro-activity, prevention, and generally speaking anticipation, including by means of individualisation of control and surveillance**. Projects aiming to increase interoperability between databases and the enhancement of information exchange systems multiply in this regard the possibility of personal data being used for purposes beyond the ones for which this data was initially connected. In the meantime, only two projects out of the 91 FP7-funded projects do address the question of the ethical and political implication of the multiplication of databases, datamining and biometric technologies of identification.

These trends, as we have shown, have characterised EU-sponsored security research since its inception. As the next section will argue, furthermore, they remain dominant in the framing of future developments in this field.

[44] Which establishes in particular that the Union "shall aim at reducing disparities between the levels of development of the various regions".

4. FUTURE DEVELOPMENTS IN THE FIELD OF EU SECURITY RESEARCH: REVIEW, CONCLUSIONS AND RECOMMENDATIONS.

KEY FINDINGS

- Proposals for the future development of EU-funded security research **demonstrate a broader attention** to the questions that security technologies raise for the fundamental rights and freedoms of persons.
- However, both the *European Security Research and Innovation Agenda* (ESRIA) developed by ESRIF for EU security research until 2030 and the Commission's initial position paper on ESRIA **remain overly framed in terms of capabilities and technologies and, with regard to persons, of acceptance and reassurance.** These orientations, we argue, call for a number of initiatives to be taken, in particular by the European Parliament, in the perspective of future discussions on the establishment of the 8th Research Framework Programme (FP8) to start in 2011.

In the final section of this note, we review the ESRIF final report and the Commission's position paper on its recommendations, which together sketch out possible future directions for EU-funded security research (4.1.). The second half of the section is dedicated to our conclusions on the assessment of the PPD and FP7-ST, together with recommendations for consideration by the European Parliament LIBE Committee (4.2.).

4.1. Review of the ESRIF Final report and the Commission's position.

The main contribution of the ESRIF final report is the so-called *European Security Research and Innovation Agenda* (ESRIA) that proposes a roadmap for EU security research and development in the next 20 years. The Commission has issued a position paper on ESRIA, where it endorses most of the conclusions of ESRIF. In this section, we examine what ESRIF has dubbed its "vision" of security and technology, its recommendations encapsulated in the ESRIA, and the Commission's position.

4.1.1. The ESRIF "vision": the problem of seeing security as acceptance and reassurance.

The cornerstone of ESRIF's recommendations is their focus on what the report calls "societal security", *i.e.* the idea that security research should "address the long-term vulnerability" of European social, cultural and political values. A key issue, in this regard, is **whether the "vision" of ESRIF makes room for considerations about the way in which the effects of security research might question these very values**.

While the attention to values is welcome, the framing of the matter in the ESRIF report does raise certain concerns: "Research and innovation in security demands a framework of legal and ethical guidelines – a "legitimacy perimeter" – to ensure social acceptance and trust, alongside effective political leadership and communication. This will open markets for trusted new solutions"[45]. Trust, in this perspective, involves the notion that "[t]he public must be reassured that […] a sufficient level of protection is in place against the main known threats" and that "[m]ain infrastructures and services are resilient […] people and organisations in charge of security and crisis management are well prepared"[46].

[45] ESRIF Final Report, p.13.

[46] ESRIF Final Report, p.14.

Such a perspective is related to the overall framing of security issues in the ESRIF report, *i.e.* the idea that the EU is currently confronted with a radically new "threats environment" that requires strong measures. We lack the space to discuss this notion properly, but it does lead to assertions – found in the report of the ESRIF Working Group on CBRN[47] - that "it does seem relatively likely that non-state actors motivated by ideas that are more apocalyptic would find it attractive to construct and possibly employ a CBRN weapon"[48]. **Notwithstanding questions as to the necessary empirical backing that such assertions require, they are also problematic in the equivocal way in which they play on the unease of policy-makers and citizens[49].**

The emphasis on the legal dimension of security research, as opposed to the solely "ethical" considerations of previous strategic documents (such as the ESRAB final report) should, again, be welcomed. **The narrowing down of these matters, however, to the question of acceptance and reassurance remains problematic**. This appears clearly in a later paragraph of the ESRIF final report, which mentions that "[s]urveillance is increasingly a central element of security management […] As these tools are developed, the impact on European values of the relation between surveillance and civil and human rights, the place of new technologies in society role, their role in security crises and their consequences for the individual remain poorly understood"[50]. Firstly, as recent examples, from the steps being taken by the U.S. administration to curtail several border surveillance programmes to the recent decision of the British government to cut down on surveillance programmes show, **reliance on surveillance is not inevitable**. Secondly, the issue at stake does not solely lie in understanding the consequences of security technologies on fundamental freedoms and rights, **but also to reflect on the ways in which the latter can be made to evolve to better protect persons (and not only citizens) rather than to accommodate an increase in surveillance.**

A question to address, in this respect, is whether the core ESRIF proposal – the *European Research and Innovation Agenda* which should define the priorities of EU-funded security research up to 2030 – meets this challenge.

4.1.2. The *European Research and Innovation Agenda*: capabilities, technologies, and the instrumentalisation of social sciences.

The core proposal of the ESRIF final report is the establishment of the ESRIA, a roadmap for security research until 2030. In line with earlier guidelines from the GoP and ESRAB reports, the ESRIA proposal is capability – *i.e.* "the ability to perform a specific task or operation"[51] – centred. The roadmap identifies 5 main clusters divided into 14 components for security research, summarised in Table XX on the next page.

The overall aim, as embodied in the ESRIF concept of "Security cycle", is of "preventing, protecting, preparing, responding and recovering" from threats and attacks. In all these areas, the linkage between technology and efficiency is strong: technology is assumed to make security policies more efficient, but **little attention is paid to the possibly unwanted effects of this very technology on the persons it claims to be protecting**.

One exception, in this regard, is laid down in the section on "Identity management and protection", where the report "advocates **implementation of a 'privacy-by-design' data protection approach** that should be part of an information system's architecture from the start", and comprise "general privacy controls, a separation of data from different data streams, privacy management systems, and effective 'anonymisation' of personal data"[52].

[47] Chemical, bacteriological, radiological and nuclear weapons.

[48] ESRIF Final Report, p.140.

[49] For further analysis, see e.g. Bigo, Carrera & Guild, 2009.

[50] ESRIF Final Report, p.21.

[51] ESRIF Final Report, p.19.

[52] ESRIF Final Report, p.31.

It is regrettable, however, that these issues were not taken for consideration as a cluster by itself in the ESRIA proposal.

Even more regrettable, in this perspective, is the **rather limited role envisaged for legal, political and social science research in the ESRIA**. The report of the ESRIF Working Group on Border Security, for instance, establishes that: "Social science research is needed for understanding and modelling threats"[53]. This argument, which reflects an instrumentalisation of legal, political and social sciences, is highly questionable. Such disciplines have **arguably another role to play than just to validate and enable the assumptions embedded in technology-oriented research projects:** they should be included in order to provide the necessary analytical depth as to the implications of defining such and such development as a threat. **More generally speaking, research does not only involve validating policy orientations or evaluating their efficiency, but also questioning their premises and underlining their effects**.

Table 2. The ESRIA research clusters and cluster components.

ESRIA Clusters	ESRIA Cluster Components
Cluster 1: Preventing, Protecting, Preparing, Responding and Recovering.	Securing People
	Civil Preparedness
	Crisis Management
Cluster 2: Countering different means of attack.	Explosives
	Chemical, Biological, Radiological, Nuclear
	New technologies, new threats
Cluster 3: Securing critical assets	Security of Critical Infrastructures • Security of natural resources • Energy • Transport
	Security economics
Cluster 4: Securing identity, access and movements of people and goods	Border Security
	Identity Management and Protection
Cluster 5: Cross-cutting enablers	Information and Communication Technology
	Space
	Evidence and forensics
	Informed Decision Making

Source: ESRIF Final Report, p.17-32.

[53] ESRIF Final Report, p.99.

The assessment of the ESRIA proposal, in this respect, inevitably generates mixed conclusions.

- It **does take into account**, to a larger extent than previous security research initiatives, **preoccupations linked to the impact of security technologies on fundamental freedoms and rights**. In this perspective, the reference to "privacy-by-design" as an important element of research in the field of identity and movements of persons is welcomed.
- Overall, however, the ESRIA is still largely oriented towards the development of capabilities and technologies, and demonstrates an instrumental perspective on research, including legal, political and social research, which is problematic.

4.1.3. The Commission's position on the ESRIA.

The Commission expressed its initial position on the ESRIF final report by means of a communication tabled on 21 December 2009[54]. The communication is essentially a summary of the ESRIF report and of the ESRIA proposal, but some elements are nonetheless worth noting.

A key point in the document as regards the specific questions raised by the present briefing note is the indication, in the introductory section, that "[s]ince security technologies are becoming more and more present in modern societies prompting at time concerns on the part of citizens, it is important to ensure ethical scrutiny and transparency of security research and development projects"[55]. The communication, however**, never specifies the concrete steps through which this objective of transparency (to which one should add an objective of accountability) is to be achieved**.

A second point worth underlining is brought worth in the communication, regarding the "legal and ethical dimension" of security research. The Commission argues "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 social acceptance and always applied in accordance with the rule of law"[56]. **This specification is important, and the reference to the rule of law beyond mere ethical considerations an important step in reframing security research.** The stated need for "social acceptance", however, is problematic, as we have argued previously. **Acceptance cannot be considered as a viable substitute for transparency and democratic accountability**.

In the meantime, however, the document fails to develop how exactly this will be pursued. An element featured in the conclusions opens up an interesting perspective, namely the mention that "the role of the European Union Agency for Fundamental Rights to undertake research concerning the relationship between security and private life and data protection"[57] should be considered. This orientation, in our view, would certainly need to be pursued more intensively in the upcoming Commission discussion paper on the future 8th Framework Programme (FP8).

[54] European Commission. *A European Security Research and Innovation Agenda – Commission's initial position on ESRIF's key findings and recommendations*. COM(2009) 691 final, 21 December 2009.

[55] COM(2009) 691 final, p.2.

[56] COM(2009) 691 final, p.3.

[57] COM(2009) 691 final, p.10.

4.2. Conclusions and recommendations

4.2.1. Conclusions: security research, service to the citizen and fundamental freedoms and rights.

Security research under its current (and, apparently, future) form fails to address the questions that should be at the heart of any security policy: **what is what we want to protect? And what is the impact of measures taken in the name of protection on what we want to protect?**

- Protection is not only about reassurance or physical safety. It is also about **guarantees**: guarantees of accountability, of transparency, of one's fundamental freedoms and rights, **for citizens but also for all persons who might have to face the effects of EU security policies**. Security research should be placed at the service of persons living in or travelling to the EU, beyond concerns with the "acceptability" of surveillance.
- Technological research and development, in this respect, is not only about capability and feasibility. As recent developments in the case of Swift and body scanners, as well as citizens' mobilisation against initiatives such as biometric identity cards in France and the United Kingdom, **technological developments are a central political issue**, which should involve elected representatives (members of national parliaments as well as MEPs) and civil society groups beyond think tanks.

We argue, in this respect, that EU-funded security research should first and foremost be oriented to serving citizens and, more broadly, all persons facing the effects of EU internal and external security policies. The following recommendations are developed within this perspective.

4.2.2. Recommendations.

These recommendations are informed by the fact that **the Commission should shortly be releasing its mid-term evaluation of FP7, before publishing a first discussion paper on the outlook of the future 8th Research Framework (FP8, 2013-2018) at the beginning of 2011**. In this perspective, we offer short-term recommendations aimed the forthcoming mid-term evaluation of FP7, and longer-term suggestions looking to the process of establishing FP8.

1/Short-term recommendations:

- Before any key decision is taken with regard to the future FP8, the European Parliament should adopt a resolution drawing from the wording of its 2006 text on security research, **calling on the Commission to provide a detailed analysis of the various funding schemes for security research and development**, and stressing **the necessity to take into account a broader notion of the "public interest"** – *i.e.* beyond questions of acceptability, capability and efficiency – in examining upcoming applications for FP7 research projects.
- We recommend running **an overall evaluation of EU-funded security research and development, including FP6, PASR and FP7**. Four options are available:
  - **From an accounts and budgetary point of view**, such an evaluation would fall within the remit of the European Court of Auditors as laid out in Article 287 TFEU[58]. Such a request could be issued by the Parliament in the resolution proposed in our previous point.

[58] Particularly Art. 287(4), "It shall assist the European Parliament and the Council in exercising their powers of control over the implementation of the budget".

- **From a data-protection and privacy point of view**, the European Data Protection Supervisor and/or the Art.29 Working Party could also undertake this evaluation. Again, such a request could be issued by the Parliament in the resolution proposed in our previous point.
- **From a fundamental rights and freedoms perspective**, such an evaluation could be conducted by the EU's Fundamental Rights Agency. This would fall within the FRA's mandate[59] and is congruent with the FRA's multiannual framework[60]. On the basis of Article 4(1)(c) of Regulation (EC) No 168/2007, Parliament is entitled to issue such requests to the FRA.
- A fourth possibility **would involve calling onto the European Parliament's own *Science and Technology Options Assessment* unit (STOA) to run this evaluation**. Such an evaluation falls within the remit of STOA as established by the STOA Rules adopted by the European Parliament Bureau on 4 May 2009[61]. The STOA Rules note in this respect (Art.2(3)) that "Any Member or Parliament body may submit a proposal to the STOA Panel for STOA activities to be carried out". Without prejudice to the possible decision of the STOA Panel, **we strongly recommend that this evaluation include groups and organisations involved in the field of fundamental rights and freedoms, including the FRA[62], privacy and data protection bodies and organisations, as well as scholars in the fields of law, political and social sciences** – and this beyond the established circles of research sponsoring bodies and think tanks which have been involved in FP7-ST.

2 / Medium to long-term recommendations:

- **Security research should be reintegrated within the remit of DG Research in the perspective of FP8**. Through its experience in successive Research Framework Programmes, DG Research has developed the expertise to handle both scientific institutions and private entities. DG Enterprise can certainly be associated with this process, but **it is important to ensure that the emerging European Research Area is not jeopardised by a fragmented policy-making framework, and that the same rules apply transversally to all areas of EU research sponsoring activities**.
- Should security research be maintained as a stand-alone theme in FP8, it is important to ensure that:

[59] As defined in Council Regulation (EC) No 168/2007 of 16 February 2007 establishing a European Union Agency for Fundamental Rights (OJEU L53, 22 February 2007, p.1-14), in particular Article 2(2) which states that the "objective of the Agency shall be to provide the relevant institutions, bodies, offices and agencies of the Community with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights".

[60] As established by Council Decision 2008/203/EC of 28 February 2008 implementing Regulation (EC) No 168/2007 as regards the adoption of a Multiannual Framework for the European Agency for Fundamental Rights for 2007-2012 (OJEU L63, 7 March 2008, p.14-15), Article 2.

[61] Article 1(2) of the STOA rules notes that it shall "provide Parliament's committees and other parliamentary bodies concerned with independent, high-quality and scientifically impartial studies and information for the assessment of the impact of possibly introducing or promoting new technologies and shall identify, from the technological point of view, the options for the best courses of action to take".

[62] In accordance with Article 6(1) and 6(2)(a) of Regulation (EC) No 168/2007 and Article 3(1) of Council Decision 2008/203/EC.

- **a certain proportion of this funding – 10 to 15% - is earmarked for research focusing on the legal, political and social implications of security technologies.**
- **transversality of research is ensured, by requesting that all technology development projects include a legal, political and social component**. Should the project foresee the use or development of data-intensive technologies (including, but not limited to, data-mining, data fusion, behavioural profiling, etc.), the involvement of privacy and data-protection experts, particularly practitioners from data-protection authorities, **should be mandatory**.
- **the possibility of developing a research theme on fundamental freedoms and rights, including with regard to EU internal and external security policies, is included in plans for establishing the future FP8.** The involvement of the FRA as well as of the EDPS and the Art.29 Working Party in the definition and conduct of this programme should be actively pursued.

REFERENCES

- Bigo, Didier, Carrera, Sergio, Guild, Elspeth. *The CHALLENGE Project: Final Policy Recommendations on the Changing Landscape of European Liberty and Security*. Brussels: CEPS, *CHALLENGE Research Papers* n°16, September 2009, available from: http://www.ceps.eu/book/challenge-project-final-policy-recommendations-changing-landscape-european-liberty-and-security.
- Bigo, Didier, Jeandesboz, Julien. *Review of security measures in the 6th Research Framework Programme and the Preparatory Action on Security Research*. Brussels: European Parliament, PE 393.289, May 2008.
- Bigo, Didier, Jeandesboz, Julien. *The EU and the European Security Industry: Questioning the "Public-Private Dialogue"*. Brussels: CEPS, *INEX Policy Briefs* n°5, February 2010, available from: http://www.ceps.eu/book/eu-and-european-security-industry-questioning-%E2%80%98public-private-dialogue%E2%80%99.
- Burgess, Peter, Hanssen, Monica. *Public-Private Dialogue in Security Research*. Brussels: European Parliament, PE 393.286, May 2008.
- European Commission. *Implementing European Union strategy on defence-related industries*. COM(97) 583 final.
- European Commission. *European defence – Industrial and Market Issues: Towards an EU Defence Equipment Policy*. COM(2003) 113 final.
- European Commission. *Towards a programme to advance European security through Research and Technology*. COM (2004) 72 final.
- European Commission. *Security Research : the Next Steps*. COM(2004) 590 final.
- European Commission. *Meeting the challenge : the European Security Research Agenda, a report from the European Security Research Advisory Board*. Luxembourg: Office for Official Publications of the European Communities, 2006.
- European Commission. *Public-Private Dialogue in Security Research and Innovation*. COM(2007) 511 final.
- European Commission. *European Security Research and Innovation in support of European security policies: intermediate report*, Luxembourg: Office for Official publications of the European Communities, 2008
- European Commission. *A European Security Research and Innovation Agenda – Commission's initial position on ESRIF's key findings and recommendations*. COM(2009) 691 final, 21 December 2009.
- European Parliament. *European defence-related industries: European Parliament resolution on European defence industries*. P5-TA(2002)0172.
- European Parliament. *Security Research: European Parliament resolution on Security Research – the Next Steps (2004/2171(INI))*. Official Journal of the European Union, C133 E, 8 June 2006, p.135-140.

- Hayes, Ben. *Arming Big Brother: the EU's Security Research Programme*. Amsterdam/London: Transnational Institute/Statewatch, 2006, available from: http://www.statewatch.org/analyses/bigbrother.pdf.

- Hayes, Ben. *NeoConOpticon: The EU Security-Industrial Complex*. Amsterdam/London: Transnational Institute/Statewatch, 2009, available from: http://www.statewatch.org/analyses/neoconopticon-report.pdf.

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

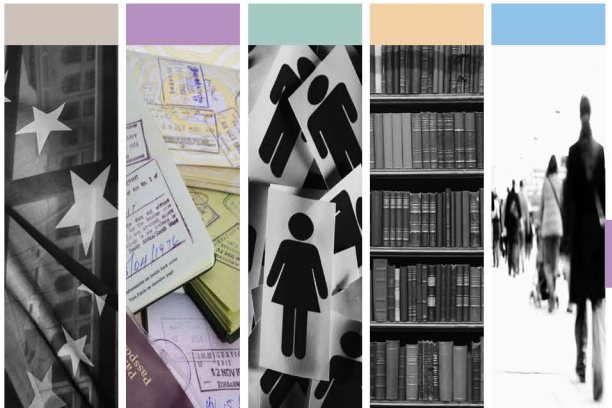
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.



ISBN