Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013

Bigo, D.; Jeandesboz, J.; Martin-Maze, M.; Ragazzi, F.

DOI
10.2861/62647

Publication date
2014

Document Version
Final published version

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 7th Research Framework Programme FP7 2007-2013

Study for the LIBE Committee

EN

2014

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 7th Research Framework Programme FP7 2007-2013

STUDY

Abstract

Upon request by the LIBE Committee, this study analyses how the public-private dialogue has been framed and shaped and examines the priorities set up in calls and projects that have received funding from the European Commission under the security theme of the 7th Research Framework Programme (FP7 2007-2013). In particular, this study addresses two main questions: to what extent is security research placed at the service of citizens? To what extent does it contribute to the development of a single area of fundamental rights and freedoms? The study finds that security research has only partly addressed the concerns of EU citizens and that security research has been mainly put at the service of industry rather than society.

PE 509.979 EN

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (LIBE)

AUTHORS

Prof. Didier BIGO (Director, CCLS – Professor at King's College London, United-Kingdom)

Dr Julien JEANDESBOZ (Associate Reseatcher, CCLS – Lecturer at the University of Amsterdam, Netherlands)

Dr Médéric MARTIN-MAZE (Associate Researcher, CCLS)

Dr Francesco RAGAZZI (Associate Researcher, CCLS – Lecturer at the University of Leiden, Netherlands)

RESPONSIBLE ADMINISTRATOR

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

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy Departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

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

European Parliament, manuscript completed in April 2014.

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

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
FP6	Framework Programme 6
FP7	Framework Programme 7
GoP	The Group of Personalities on Security Research
H2020	Horizon 2020
PASR	Preparatory Action in the field of Security Research
PPD	Public-Private Dialogue in security research
SecAG	Security Advisory Group
TTV	Teknologian Tutkimuskeskus
ISDEFE	Ingeniería de Sistemas para la Defensa de España
CEA	Commissariat à l'Energie Atomique

LIST OF FIGURES

EXECUTIVE SUMMARY

Background and aim of the study

The European Security Research Programme benefitted from € 1.4 billion between 2007 and 2013 under the Community's 7th Framework Programme (FP7). Previous briefing papers submitted to the European Parliament and dedicated to the analysis of FP6 Framework Programme concluded that while the priorities of the EU include 'serving and protecting citizens', security research had only partly addressed the concerns of EU citizens.

By analysing how the public-private dialogue has been framed and shaped and by examining the priorities set up in calls and projects that have received funding from the EU Commission under the FP7 programme, this study aims at exploring if this trend is confirmed. In particular, this study is concerned with two main questions:

- To what extent is security research placed at the service of citizens?
- To what extent does it contribute to the development of a single area of fundamental rights and freedoms?

Structure of the study and key challenges

In light of the above-mentioned elements, the study argues that funding has been overwhelmingly devoted to security and defence programmes of large transnational corporations, ministries of Interior and Defence and technical research institutions, with little funding for data protection, privacy and the respect of fundamental freedoms in security applications.

An examination of the genesis of the Public-Private Dialogue in security research endorsed by the Commission in 2007 confirms the importance and the influence of high-level venues and the security advisory group had in framing the parameters and rationale of EU-funded security research (section 2). In particular, the study finds that defence and security firms, as well as public security institutions, were over-represented in high-level venues that have yielded lasting influence on FP7 Security theme (FP7-ST). Virtually no representative from civil society in general, and civil liberties and privacy organisations in particular, were among the participants. Participating patterns in the security advisory group (SecAG) exhibit similar features. Security institutions and defence and security firms provided almost half of the participants, with DG Enterprise providing one third. SecAG has thus tended to represent mostly the interest of the security industry and security public institutions, with very little attention paid to political, juridical and ethical aspects of security research.

The study then examines the security research undertaken under the FP7-ST (section 3). An overview of the geographical, sectorial and thematic distribution shows the following:

- Most of FP7-ST funding has been allocated to large member states (France, Italy, UK, Spain, and Germany). As far as non-EU beneficiaries are concerned, Norway,

Israel, Switzerland and Turkey have provided more than 75 % of participating institutions.

- Organisations for applied research and transnational security and defence firms hold the most central positions in the network of research institutions sustained by FP7-ST. Both academic institutions and public security bodies play a marginal role.
- An examination of the projects funded under FP7-ST confirms the fact that most of them are strongly technologically driven with little attention paid to political and societal issues.

In light of these findings, it clearly appears that, under FP7-ST schemes, social science has too often been relegated to a mere 'ethical' afterthought, subordinated to concerns with technical deliverables and profit. This study argues that **technological tools and services cannot be developed without a thorough legal, social and political assessment, in order to determine their impact and effects**. It should rather be conceived as a specific research priority with its own agenda, informing more technology and industry-focused programmes.

This worrying trend is exacerbated in the security research and public-private partnerships that are foreseen in the developments within the framework of Horizon 2020 (H2020) (section 4). Only 8 topics deal with the ethical or societal aspects of security research in the 2014-2015 work programme of H2020. Furthermore, these topics tend to focus on enhancing the impact and effectiveness of security technology in terms of societal acceptance, sidestepping issues linked with their legitimacy. **The absence of ethical reflexion on the uses of technologies of digital surveillance, in particular the impact that these technologies can have on the rule of law is particularly striking in the post-Snowden era**. The analysis of the Commission's proposals for an EU security industrial policy further demonstrates that the question of fundamental freedoms and rights is reduced to a matter of commercial considerations and as a limit to the acquisition of otherwise high-performance products. We can thus anticipate that **funded security research in the future will be mainly put at the service of industry rather than society**.

Drawing from the analysis offered in these sections, the last part of the study makes a series of recommendations built on the conclusion that the respect of the rights and freedoms of individuals facing the effects of EU security policies should, now more than ever, become central in security research. The recommendations in particular: 1) insist on the need to clarify who are the 'end-users' of security research; 2) advocate for a stronger participation of universities in security research; and 3) call for more funding support for free and open source software in the domain of security and privacy.

1. INTRODUCTION

KEY FINDINGS

- The European Security Research Programme benefitted from 1.4 billion Euros between 2007 and 2013 under the FP7. In light of the conclusions drawn by previous reports, this study assesses to what extent security research programmes have addressed the concerns of EU citizens.
- This study confirms that funding has been overwhelmingly devoted to security and defence programmes of large transnational corporations, ministries of Interior and Defence and technical research institutions, with little funding for data protection, privacy and the respect of fundamental freedoms in security applications.
- The study argues that such trends have been exacerbated, in particular with the 'public-private dialogue' in security research launched by the EU Commission in 2007 and the substantial reduction of funding for ethical and social science aspects of the research programmes.

Substantial funding has been devoted to EU security research over the past 10 years. The Preparatory Action in the field of Security Research (PASR), endowed with € 65 million for the period 2004-2006 was launched in February 2004 by the European Commission, alongside with a number of projects funded under the Community's 6th Framework Programme (FP6). The European Security Research Programme benefitted from € 1.4 billion between 2007 and 2013 under the Community's 7th Framework Programme (FP7). In the current H2020 programme, €1.695 billion are currently earmarked for security research under the 'Secure societies – Protecting freedom and security of Europe and its citizens'.[1]

This study takes stock of previous reports that have evaluated the content and the distribution of funding for the various programmes[2]. These reports concluded that while the priorities of the EU, especially in the context of the area of freedom, security and justice (AFSJ), include 'serving and protecting citizens', security research programmes have only partly addressed the concerns of EU citizens. Funding has been overwhelmingly devoted to security and defence programmes of large transnational corporations, ministries of interior and defence and technical research institutions, with little funding for data protection, privacy and the respect of fundamental freedoms in security applications.

Public outrage over the recent Snowden revelations on the mass surveillance activities of the NSA and European intelligence services, and the recent adoption of a resolution concluding a six-month inquiry of the European Parliament into these mass surveillance

[1] European Parliament (2013). Regulation No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, Official Journal of the European Union L 347/104, p. 173.

[2] Peter Burgess and Monica Hanssen (2008). Public-Private Dialogue in Security Research. Brussels: European Parliament, PE 393.286. Didier Bigo and Julien Jeandesboz (2008). *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*. Brussels: European Parliament, PE 393.289; Julien Jeandesboz and Francesco Ragazzi (2010). *Review of security measures in the Research Framework Programme*. Brussels: European Parliament, PE 432.740.

schemes[3] backed by 544 votes to 78, however suggest that a change of direction is needed. **It is in the interest of 'serving and protecting citizens' that research in the field of security is not reduced to security and defence applications**. In the post-Snowden era, European funding for security research cannot continue with 'business as usual', and has to substantially revise its approach and priorities.

Technological tools and services cannot be developed without a thorough legal, social and political assessment, in order to determine their impact and effects. Social science should therefore not be relegated to a mere 'ethical' afterthought, subordinated to concerns with technical deliverables and profit. It should rather be conceived as a specific research priority with its own agenda, informing more technology and industry-focused programmes.

In light of these considerations, this study reviews the closing FP7 programme, as well as taking into account the upcoming H2020 programme. It argues that trends identified in previous reports have been exacerbated, in particular with the 'public-private dialogue' in security research launched by the European Commission in 2007 and the substantial reduction of funding for ethical and social science aspects of the research programmes. As for the three previous studies mentioned above, this study is concerned with two main questions: To what extent is security research placed at the service of citizens? To what extent does it contribute to the development of a single area of fundamental rights and freedoms?

Therefore, this study 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 new Horizon 2020 funding

[3] European Parliament (2014) *European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*. Brussels, P7_TA-PROV(2014)0230.

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

KEY FINDINGS

- An examination of the genesis of the Public-Private Dialogue in security research endorsed by the Commission in 2007 confirms the importance and the influence high-level venues and the security advisory group had in framing the parameters and rationale of EU-funded security research.
- In particular, the study finds that defence and security firms, as well as public institutions were over-represented in these venues that have yielded lasting influence on FP7-ST. Virtually no representatives from civil society in general, and civil liberties and privacy organisations in particular, were among the participants.
- Participating patterns in the security advisory group (SecAG) exhibit similar feature. SecAG has tended to represent mostly the interest of the security industry and security public institutions, with very little attention paid to political, juridical and ethical aspects of security research.

Although the European Commission officially endorsed it in 2007, the Public-Private Dialogue in security research (thereafter PPD) largely predates this formalisation[4]. As early as 2003, the European Commission called for "advanced research in the field of global security" bringing together supply and demand, i.e. security and defence industry and public security institutions. From there on, the PPD developed into two phases that one might fruitfully distinguish: high-level venues (2.1) and the security advisory group (2.2).

2.1. High-level venues

From 2003 to 2009, the European Commission has consecutively convened three different high-level venues with a view to contributing to the definition of security-related research in the EU:

- The Group of Personalities on Security Research (2003-2004 – thereafter GoP)
- The European Security Research Advisory Board (2005-2006 – thereafter ESRAB)
- The European Security Research and Innovation Forum (2008-2009 – thereafter ESRIF)

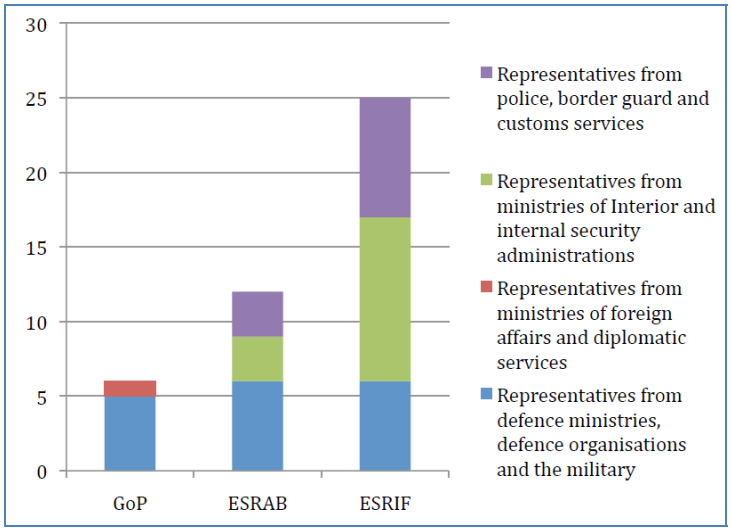
Previous assessments of these fora have outlined two dominant characteristics. First, most participants came from public security bodies and the security and defence industry. Relatively few of these participants came from research or civil society organisations. Secondly, these fora went beyond their advisory role and contributed significantly to framing the orientations and priorities of EC-funded security research[5].

[4] European Commission (2007). *Commission Staff Working Document on Public-Private Dialogue in Security Research and Innovation*. SEC(2007) 1138.

[5] Peter Burgess and Monica Hanssen, *PE 393.286 - Public Private Dialogue in Security Research* (Brussels: European Parliament, May 2008); Didier Bigo and Julien Jeandesboz, *PE 393.289 - Review of Security Measures in*

Looking at the composition of these high-level venues, it is clear that the public security bodies and organisations represented in the GoP, ESRAB and ESRIF have varied qualitatively as well as quantitatively. The number of participants has increased, from 28 for GoP to 66 for ESRIF. Furthermore, their institutional belonging has gradually shifted. While officials from the military and the defence ministries (in blue, in figure 1) represented the "end-users" in the GoP, they were outnumbered by representatives from internal security bodies and organisations (in green) in ESRIF, as the following figure illustrates:

Figure 1: Spokespersons from security agencies, bodies and services in high-level PPD[6]



Similarly, even though the European Commission advertises security research governance as "layers of structured consultations with Europe's public and private sectors and, *above all,* with civil society and its research communities (italic added)"[7] virtually no representative from civil society in general, and civil liberties and privacy organisations in particular, participated in the abovementioned venues. Statewatch researchers found that only 9 participants out of the 660 "stakeholders" who took part in the working groups under ESRIF came from civil society organisations[8]. The sidestepping of civil society organisations further underscores the role that the PPD played in establishing privileged relations between internal security institutions and a series of large security and defence companies in Europe.

This closed community in the making, interested in the development of huge margins of profits for the industry, has successfully framed the parameters and rationale of EU-funded security research, in which the main stakeholders have increasingly played a role of gatekeepers. Security research programmes have been thus chiefly defined as capability-oriented and have been devised to supposedly fulfil the

the 6th Research Framework Programme and the Preparatory Action for Security Research, Briefing Note (Brussels: European Parliament, May 2008); Julien Jeandesboz and Francesco Ragazzi (2010). Review of security measures in the Research Framework Programme. Brussels: European Parliament, PE 432.740.

[6] Rocco Bellanova and al. (2012). Supporting Fundamental Rights, Privacy and Ethics in Surveillance Technologies - Smart Surveillance - State of the Art. Oslo: PRIO, p.204.

[7] http://ec.europa.eu/enterprise/policies/security/governance/index_en.htm

[8] Ben Hayes, *NeoConOpticon. The EU Security-Industrial Complex* (Transnational Institute / Statewatch, 2009), 24.

needs of "end-users", almost exclusively defined as security institutions. Technology has been prescribed as a mandatory component of security policies. This move is grounded in a firm belief in technology as a tool capable of solving ethical, political and juridical issues embedded in security policies[9]. Such a framing not only isolates security research from concerns that might be voiced on behalf of European citizens: it also lays out the groundwork for co-opting those concerns within this technically driven and depoliticised agenda.

2.2. The Security Advisory Group

Alongside these high-level venues, the Public-Private Dialogue in security is also embodied by the Security Advisory Group (thereafter SecAG), which might be considered as a "second-track" PPD. The organisational layout of the FP7 as a whole makes provision for these groups. They are tasked with providing the European Commission with relevant expertise during the policy-making process[10].

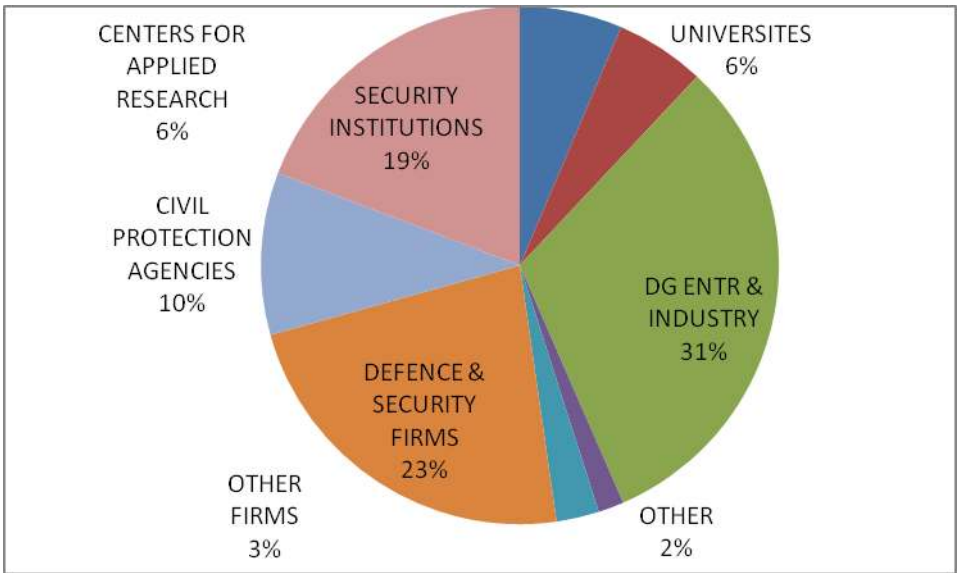
According to its mandate, SecAG is to assist the DG Entreprise & Industry in drafting annual calls for research proposals. To this end, it provides advice on "strategy, relevant objectives and scientific and technological priorities".[11] As such, SecAG does not replace the FP7 Committee for security research that is tasked with reviewing project proposals. The President and Vice-President of SecAG may nonetheless attend Committee Programme meetings.

Provisions are explicitly made so as to prevent conflicts of interests. Although participants of SecAG may work for partners of FP7-ST projects, they are requested to make any conflict of interest known to the European Commission and must refrain from participating where such conflicts may arise[12].

Members of SecAG are appointed by the Commission for 2-year terms. The 2011 annual report specifies that 20 % of the participants represent EU institutions, 35% end-users, 30 % the industry and 20 % the research community. Based on the number of actual and individual participations as well as finer-grained categories, our own observations lead to a somewhat different conclusion. As figure 2 illustrates, almost half (44%) of the actual participants came from public security institutions and transnational defence and security firms.

[9] Didier Bigo and al. (2008). INEX - Security Technologies and Society. A State of the Art on Security, Technology, Borders and Mobility, INEX. Paris: Centre d'étude sur les conflits. See: http://www.ccls.eu/en/la-recherche/
[10] "Advisory Groups for FP7", European Commission, http://ec.europa.eu/research/fp7/index_en.cfm?pg=eag visited 04/04/2014
[11] European Commission (2009). *Mandate for the Security Advisory Group for the 7th Framework Programme*. Available from: http://ec.europa.eu/research/fp7/pdf/advisory-groups/security-mandate.pdf
[12] Ibid.

Figure 2: Individual participations in the Security Advisory Group for FP7



According to our findings, participants to the SecAG come mainly from three types of institutions, besides DG Enterprise & Industry of the European Commission (31%). Defence and security firms (SELEX, MORPHO, THALES) represent 23 % of individual participations, with other firms accounting for only 3 %. The term "end-user" employed in the SecAG report actually encompasses security institutions (18%) and civil protection agencies (10%), both public and private. Finally, 'the research community' can be subdivided in centres for applied research (TNO, FRAUNHOFER – 6%) and Universities, the latter representing 6% of individual participations.[13]

From 2007 to 2012, the SecAG met 20 times for specific workshops, although members stayed in touch through constant email exchanges. The group submitted annual reports to the Commission, which were then used to draft the annual work programme of FP7-ST. Mostly, SecAG reviewed research topics proposed to the Programme Committee. Since tentative topics exceed largely the number of projects that could realistically be selected each year, the SecAG fulfilled an agenda-setting function. This is reflected, for example, in the Guidance paper that was published in the course of preparing the 2012 FP7-ST call, where this function is explicitly formalised[14].

SecAG members have underlined the necessity to include end-users organisations more closely into the drafting of project proposals as well as in their operational

[13] European legislation distinguishes between research centres and universities, although the grounds on which such a distinction should be made are not clearly laid down in the relevant legislative instrument. Regulation (EC) No 1906/2006 provides a general definition of 'research organisation' as meaning 'a legal entity established as a non-profit organisation which carries out research or technological development as one of its main objectives. It seems however that centres for applied research should be distinguished from universities in at least three ways: in terms of recruitment (the latter hire academic staff) and training (in contrast with technical universities for instance, centres for applied research do not train students), in terms of institutional links (centres for applied research do not have institutional links with higher education organisations), and in terms of type of research (between strictly applied research and a combination of fundamental and applied research). For the definition of research organisation, see: European Commission (2006). Regulation No 1906/2006 of the European Parliament and of the Council of 18 December 2006 laying down the rules for participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013), Official journal of the European Union L 391/1, 30.12.2006.

[14] European Commission (2010). *Report of the 2nd Meeting of the FP7 Security Advisory Group*. Available from: http://ec.europa.eu/research/fp7/pdf/old-advisory-groups/security-firstreport_en.pdf

implementation[15]. They have called for clearer opportunities as far as market outlets are concerned and asked for clearer routes to stimulate the participation of security industries[16]. SecAG therefore seemed inclined to represent the interests of security industries as well as those of security institutions. **The SecAG however recognised its shortcomings in terms of social science and civil organisations representation within FP7-ST**. The 2012 report clearly states that "[..] engagement from social sciences and legal departments has been lower, possibly because they lack awareness of the Framework Programme. There is a gap in representation of civil associations & NGOs, recognised in a specific topic on this aspect being included in the final work programme. [..] there is also consideration of how ordinary citizens might be engaged, especially in addressing 'privacy by design', and how techniques such as 'crowd sourcing' are applied to meeting Security needs". [17]

Although SecAG defined end-users as institutions involved in "preparing and responding to an event and recovering from it", participating patterns to SecAG show that end-users were, as a general rule, more narrowly defined as security agencies of Member-States and the EU. This claim is further substantiated by an analysis of the institutions participating in FP7-ST projects presented hereafter.

[15] European Commission (2012). *FP7 Security Advisory Group Annual Summary June 2011 - June 2012*, p.6. Available from: http://ec.europa.eu/enterprise/policies/security/files/secag-annual-summary-2011-2012-issue-1-0_en.pdf
[16] Ibid.
[17] Ibid., 9.

3. ANALYSIS OF SECURITY RESEARCH UNDER THE FP7 SECURITY THEME

KEY FINDINGS

- Geographically, most of the FP7-ST funding has been allocated to large member states. As far as non-EU beneficiaries are concerned, Norway, Israel, Switzerland and Turkey have provided more than 75% of participating institutions.
- Organisations for applied research and transnational security and defence firms hold the most central positions in the network of research institutions sustained by FP7-ST. Both academic institutions and public security bodies played a marginal role in FP7-ST.
- An examination of the projects funded under FP7-ST confirms the fact that most of them are strongly technologically driven with little attention paid to political and societal issues.

Before we proceed to an in-depth analysis of the projects funded under FP7-ST, an understanding of their main characteristics is needed. The basic features of FP7-ST projects are as follows:

- **Coordinating and partner institutions**. FP7-ST projects are carried out by consortiums composed of one coordinating institution associated with a series of partners whose number range from 0 in the case of single partner projects (such as European Security Conferences) to 41 for the project SECUR-ED. 1659 institutions have participated in the FP7-ST programme, which amounts to 6.48 average participants per project[18]. The lead institution ought to be considered a *primus inter pares* insofar as it designs the initial project proposal, secures the participation of partners and acts as the contact point with DG Enterprise. Furthermore, co-participations in projects pinpoint the links amongst participating organisations. They consequently reveal the network of security research institutions sustained through FP7-ST activities.

- **Eligible partners**. The following institutions are entitled to participate in FP7-ST project: 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. Although all countries can apply, only EU member states and third countries contributing to the overall FP7 budget enjoy unrestricted access to FP7 funding[19].
- **Funding**. In general, costs are only partially covered by Community funding. One must therefore distinguish project cost and EC contribution.

[18] It was impossible to retrieve information about 5 of the 260 FP7-ST projects on the CORDIS database because of broken links at the time of research. Therefore, only 255 projects are factored in the following calculations.
[19] These are EEA countries (Iceland, Norway, and Lichtenstein), candidate countries, as well as Israel and Switzerland. Cf. http://ec.europa.eu/research/fp7/understanding/fp7inbrief/who-apply_en.html

Costs in FP7-ST projects range from € 439,962 (project SRC-11) to € 43.6 million (project PERSEUS); they amount to an average of € 5.6 million, and a total of € 1.4 billion.

Community contributions range from € 200,000 (project SRC-09) to € 27.8 million (project PERSEUS); they amount to an average of € 3.9 million and a total of € 1.0 billion. These figures correspond to an average Community participation of 70, 43% of total costs.

- **Research themes.** ESRAB has defined the thematic areas that are eligible for funding under FP7-ST: 1) security of the citizens, 2) security of infrastructures and utilities, 3) intelligent surveillance and border security, 4) restoring security and safety in case of crisis, 5) security systems integration, interconnectivity and interoperability, 6) security and society, 7) security research coordination[20]. However, these thematic areas are largely theoretical in so far as most projects crosscut through them. For instance, in late 2012, the thematic area "intelligent surveillance and border security" comprised only 23 projects. However, our findings suggest that at least 44 other projects, which are allocated to other themes, feature components that are relevant to this area. One may regret the incoherence of this categorisation inasmuch as it hampers a clearer understanding of the actual priorities of security research under FP7-ST.

3.1. Geographical distribution of FP7-ST

The mid-term assessment of FP7-ST underlined the unequal geographical distribution of funding[21]. Most of the resources were allocated to the largest Member States, at the expense of smaller countries. As the following updated data demonstrates, this trend has been reinforced, both in terms of the number of projects coordinated per country (3.1.1) and of the number of individual participations (3.1.2).

3.1.1 Coordinated projects

The number of projects per country of origin of the coordinating institution ranks participating states in the following order: France (14%), Italy (13%), the UK (12%), Germany (12%) and Spain (9%) (see figure 3). 60 % of FP7-ST project coordinators are based in these 5 countries. A slightly different pattern is reflected in the geographical distribution of EC contribution per country of coordinators. France (16%), Italy (13%), the UK (12%), Spain (10%) and Germany (9%) coordinate 60% of the volume of available FP7-ST funding (see figure 4).

[20] European Commission (2006). *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.
[21] Julien Jeandesboz and Francesco Ragazzi, *Review of Security Measures in the Research Framework Programme,* Op.Cit.

Figure 3: Number of Coordinated Projects per country of origin

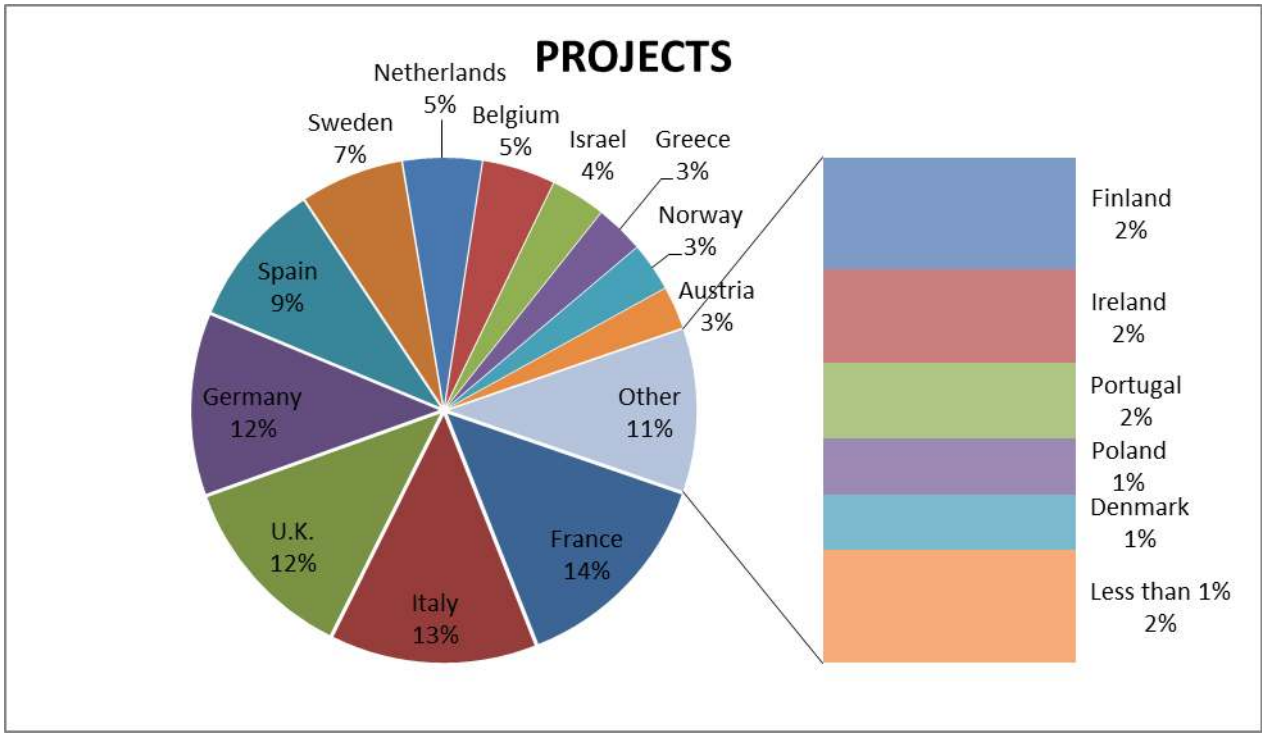
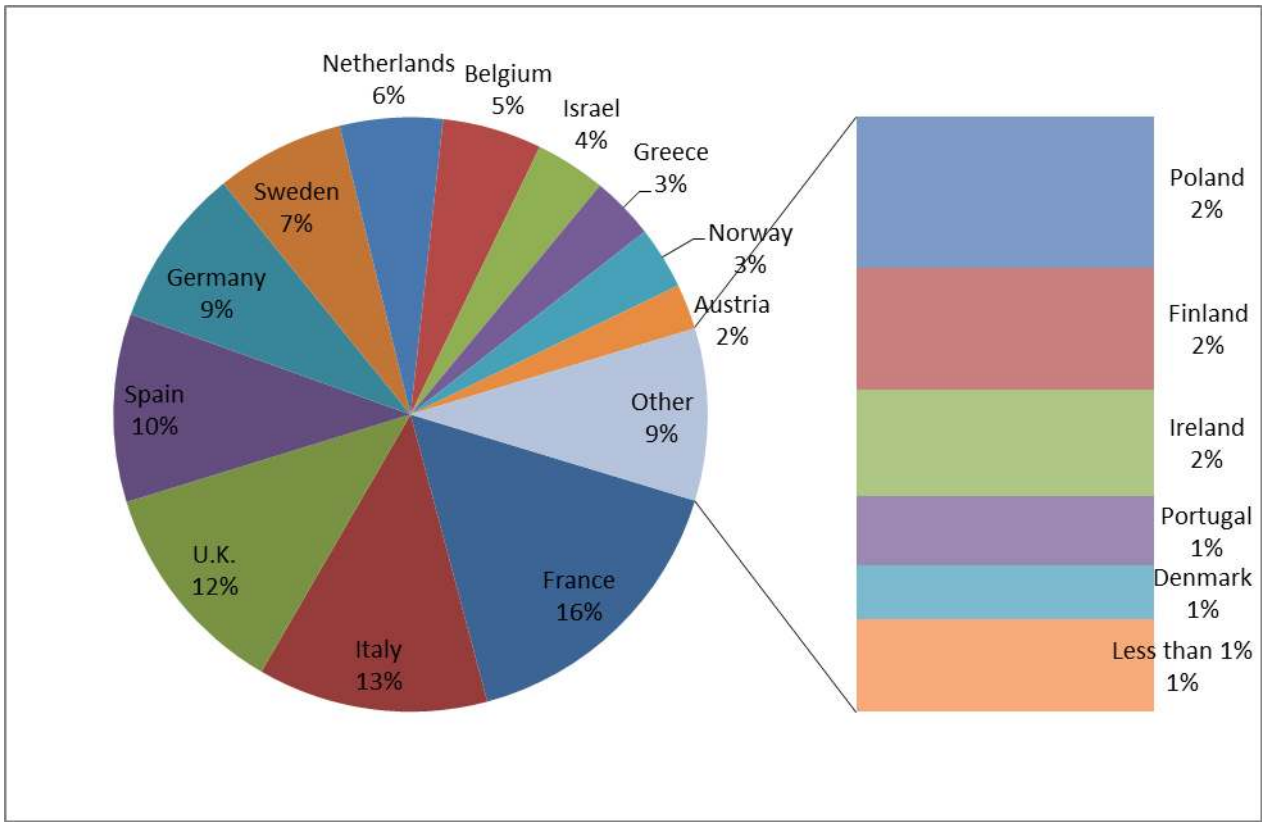


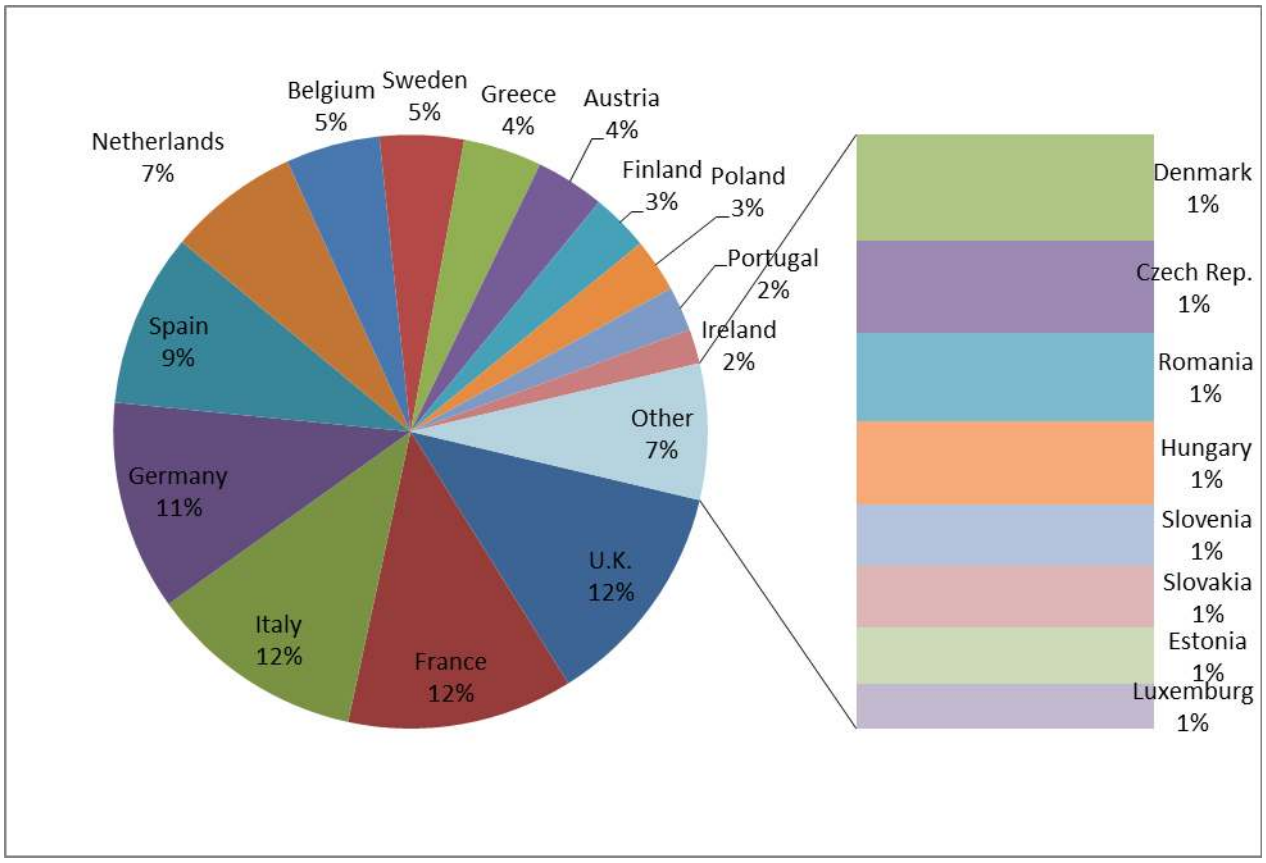
Figure 4: EU contribution per coordinator's country of origin



3.1.2 Number of individual participations

The analysis of individual participations, either as partner or as coordinator, confirms that the FP7-ST funding has been mainly allocated to the largest EU member-states. The United Kingdom (12%), France (12%), Italy (12%), Germany (11%) and Spain (11%) account for 56 % of individual participations for EU-based institutions.

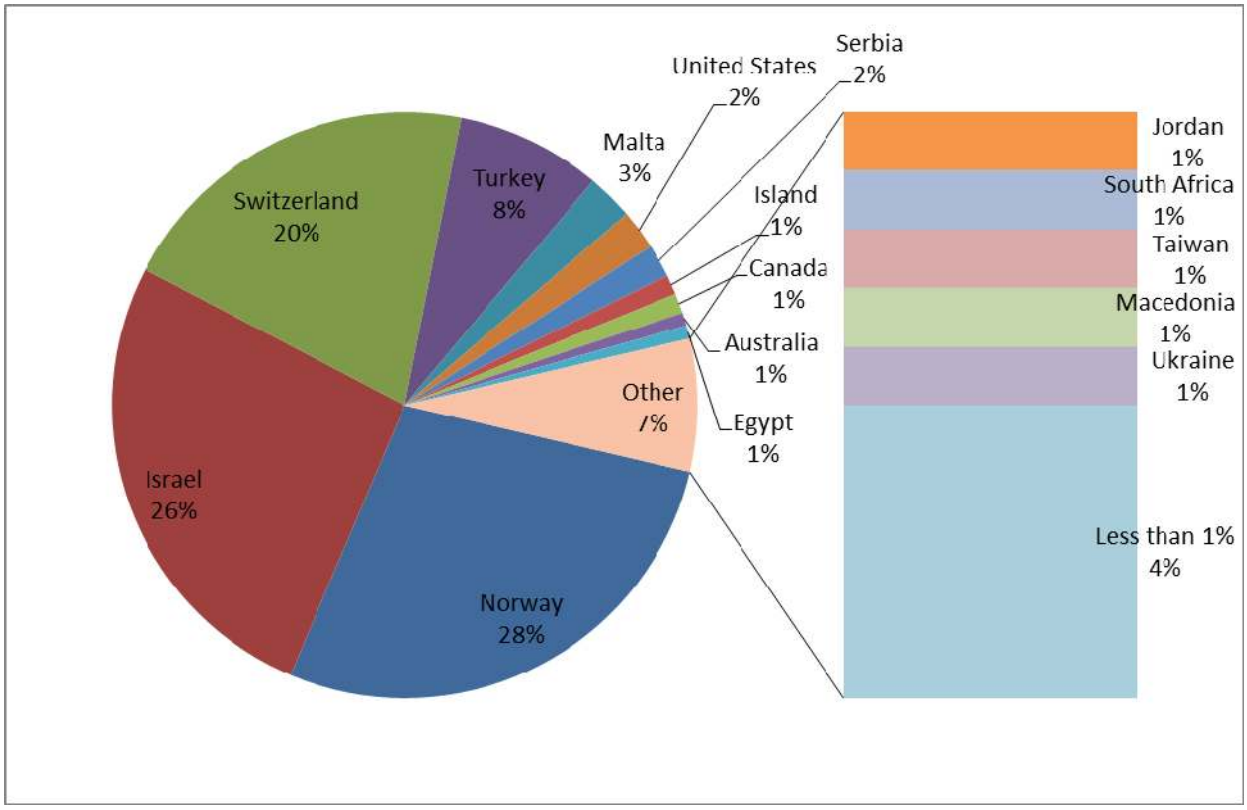
Figure 5: Number of participations per country of origins (EU)



The majority of participating institutions from non-EU Member States are found in Norway (28%), Israel (26%), Switzerland (20%) and Turkey (8%). The positioning of Israel as one of most central beneficiary of EU-funded research in security has raised concerns amongst civil rights organisations that the EU might be funding "Israel's military-industrial complex[22].

[22] See Ben Hayes (2013). "How the EU Subsidises Israel's Military-Industrial Complex", available from: http://www.opendemocracy.net/ben-hayes/how-eu-subsidises-israel%E2%80%99s-military-industrial-complex

Figure 6: Participations per country of origin (non-EU)



3.2. Sectorial distribution

A variety of institutions are eligible for FP7-ST funding. However, **updated data confirms the trend outlined in previous evaluations. Most of the funding has benefited to major European defence and security firms, as well as applied research centres**. Close examination of co-participation patterns and funding distribution yields a clearer view of the public and private network of security research institutions that FP7-ST has shaped over the past six years.

Figure 7: Top 28 institutions in security research

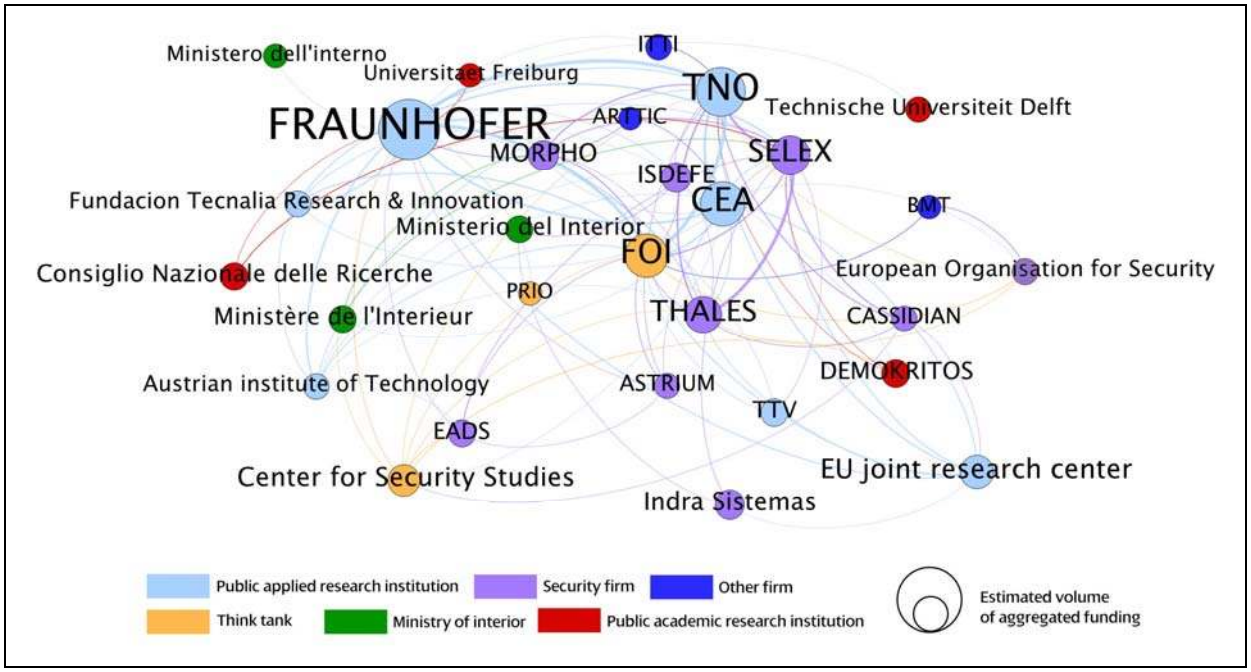


Figure 7 provides a network analysis of the participating institutions in FP7-ST. For the sake of clarity, only the 28 most central institutions appear on the graph. The size of the nodes corresponds to the estimated volume of aggregated funding that the institution has received through the programme. The density of the edges linking the nodes together varies according to the number of co-participation in one or more projects. Colours are set according to the type of institution: ministries of Interior (green), public academic institutions and universities (red), centres for applied research (light blue), think tanks (orange), security firms (purple) and other companies (dark blue).

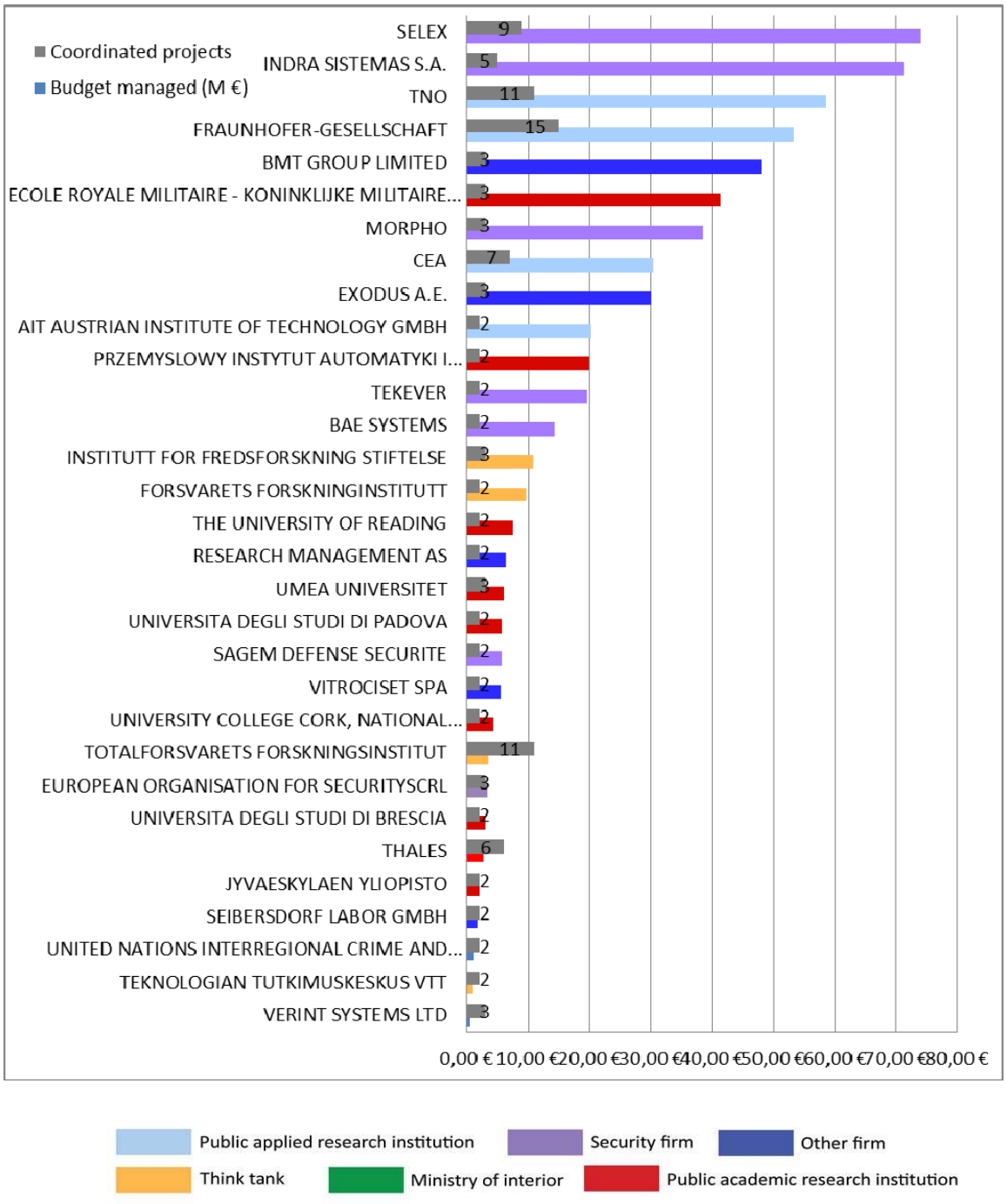
The structure of network shows the high centrality of security firms (Selex, Thales, EADS and, to a lesser extent, ISDEFE and Morpho) and applied research organisations (CEA, Fraunhofer and TNO). As far as the latter are concerned, they are located in the historical core of the European Union, e.g. France, Germany and the Netherlands. Moreover, these institutions have strong working relations with Norwegian think tanks specialised in security issues: Totalforsvaerts Forskningsinstitut and PRIO.

This centrality contrasts with the marginality of two other types of institutions**.** Universities, on the one hand, not only receive a limited amount of funding but also appear on the fringe of the network. This double constraint describes the situation of the Catholic University of Leuven, the Universities of Delft, Freiburg and Bologna, and other public research institutions (Centre national de la recherche scientifique, Consiglio nazionale delle recherche and Demokritos). This assessment confirms earlier findings on the marginalisation of academic and fundamental research, let alone social science, in the FP7-ST scheme.

Public security bodies and organisations, moreover, are hardly visible on the graph. Although the Spanish Ministry of the Interior occupies a relatively central position, its French, Italian and Dutch counterparts are much more marginalised in the network. This raises the question of the actual importance that public security bodies hold in the network of security research, despite the fact that they are considered as the main end-users in the description of FP7-ST projects.

In addition to the analysis of the budgets received from the EU per institution, the pattern of FP7-ST network is also captured by the number of projects and the total amount of funds coordinated (including the EU funding), as figure 6 illustrates. Graph 8 displays the global amount of funds and the number of individual projects managed per institution. As such, it provides different information than graph 7 where the size of the nodes depends on the evaluated amount of money that partners have actually received as opposed to coordinated. Therefore, institutions participating in projects with large budgets are central in graph 7, but may be marginal in graph 8 if they do not coordinate projects – as is the case for Thales, for instance.

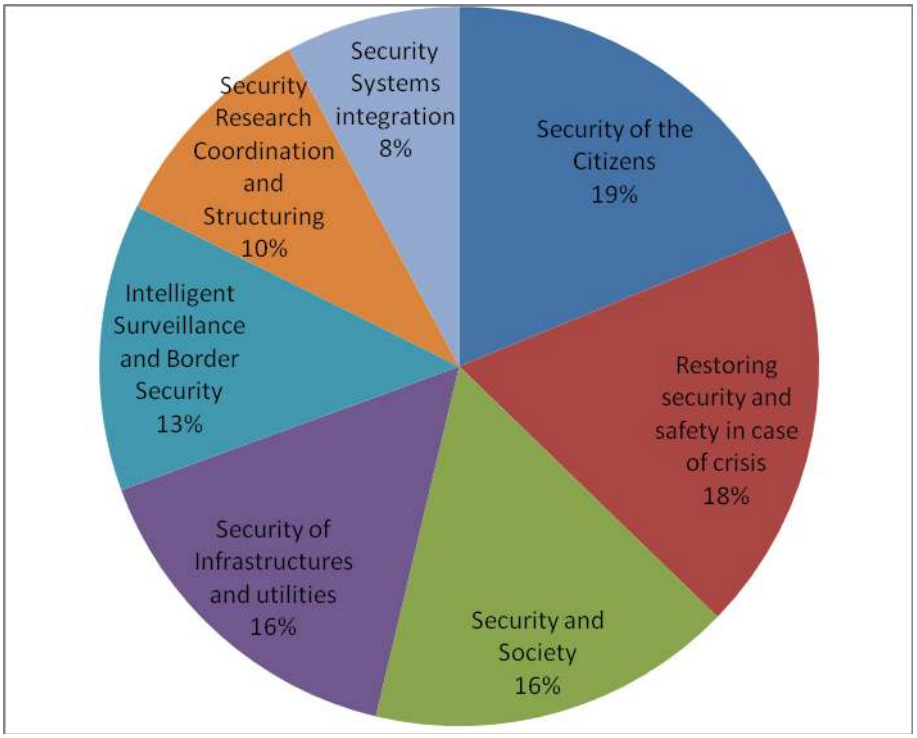
Figure 8: Top 31 coordinating institutions in FP7-ST



3.3. Thematic distribution

As previously outlined (see 3.1.), FP7-ST funds research in a variety of areas. However, the amounts of funding allocated to each of them vary significantly, and, as seen earlier, there is an incoherent categorisation of FP7-ST activities by the Commission. For instance, research in the area of *Unmanned Aerial Vehicles*, or drones, is distributed across different thematic areas such as border security or police and crime control. This kind of research therefore does not appear as such in the programming of FP7-ST. **This blurring of inter-sectorial boundaries within the FP7-ST tends to weaken democratic control over security research in the EU**[23].

Figure 9: Thematic distribution of FP7-ST funding - per project



3.3.1 Security Research Coordination and Structuring

This theme comprises 25 projects and has received € 50,3 million (4%) of the overall FP7-ST funding. Under this thematic area, some projects are dedicated to integrating more closely public security institutions – see for example ARCHIMEDES[24].

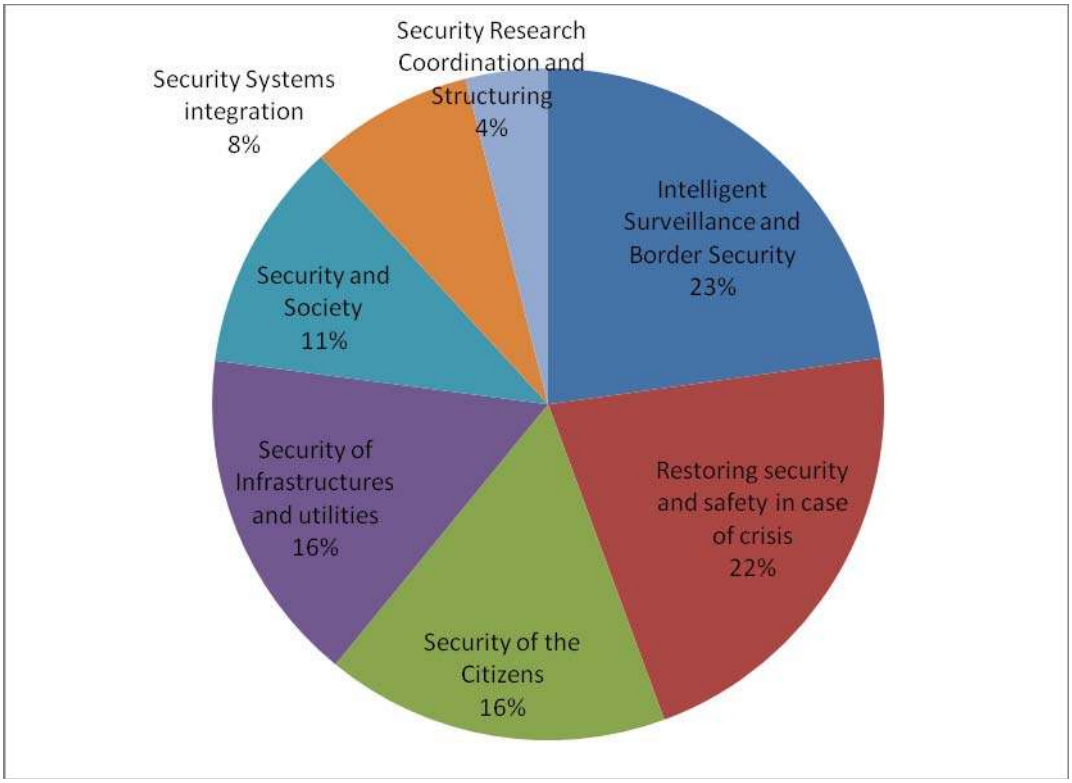
[23] Ben Hayes, Chris Jones and Eric Topfer, *Eurodrones Inc.* (Amsterdam: Statewatch / TNI, February 2014), 27–34.

[24] ARCHIMEDES (Support to security end users) pursues the following objectives : "1) Develop an Innovation Management methodology enabling EU&O to efficiently benefit from R&T results and promote a common innovation culture; 2) Start a sustainable process for the EU&O driven definition of common operational needs & early R&T demands aligning EU research agendas with EU & MS security policies; 3) Enhance EU&O participation in all stages of EU research activities: agenda-setting; participation in projects; improvement of the legal and operational environment; definition of testing, validation and certification procedures; implementation; 4) Promote security EU&O networking and a permanent public-private dialogue through the creation of a Forum to also reinforce cooperation with the supply side and explore a sustainable end-to-end approach to Research and Innovation."Cf. http://cordis.europa.eu/projects/rcn/101736_fr.html

3.3.2 Security Systems Integration, interconnectivity and interoperability

20 projects and € 118, 9 million were allocated to this thematic area, e.g. 8 % of overall funding. A sizeable proportion of these activities aims at enhancing communication systems that first responders use in case of crisis (see for instance DISASTER[25]). Other projects focus on the digitalisation of information, its storage, interconnection as well as building of automated data-mining capacities (see ADVISE). It should be noted that ADVISE carries some strong political significance in the context of massive digital surveillance as revealed by the PRISM scandal[26].

Figure 10: Thematic distribution of FP7-ST - per EC contribution



[25] DISASTER (Data Interoperability Solution At STakeholders Emergencies Reaction) aims at overcoming miscommunication amongst first responders to international crisis. It offers a 2-step solution:" "(i) As main objective and foundations of this proposal, the development of a common and modular ontology shared by all the stakeholders offers the best solution to gather all stakeholders knowledge in a unique and flexible data model, taking into account different countries cultural, linguistic and legal issues (ii) Taking advantage of the fact that most legacy Emergency Management Systems are based on Service-Oriented-Architectures (SOA), i.e. they collect information from services offered by other systems (e.g. Geographic Information Systems), the interoperability burden will be addressed by means of transparent SOA mediation algorithms compliant with current data formats and existing solutions., Taking into account the heterogeneity and diversity of all existing scenarios in crisis episodes, the potential results of this proposed ontology-based interoperability solution will be validated through the design and development of a realistic prototype scenario actively involving both emergency managers and emergency first responders."Cf. http://cordis.europa.eu/projects/rcn/102279_fr.html

[26] Didier Bigo and al. (2013). *Open Season for Data Fishing on the Web The Challenges of the US PRISM Programme for the EU*, CEPS Policy brief, Brussels: Centre for European Policy Studies.

3.3.3 Security and Society

This theme corresponds to 42 projects and amounts to € 112.3 million of the Commission's contribution (11% of the grand total). Two significant issues have received consideration: the relations between privacy and security (see PACT[27]) and societal security (see SECILE[28]). The involvement of partners with social science background has been instrumental in ensuring the high quality of these research projects, where political, ethical and juridical aspects of security research were tackled. However, in some cases, outputs translated into guidelines for "ethical" security research have sidestepped juridical approaches (see SURVEILLE[29]).

3.3.4 Security of infrastructures and utilities

40 projects and € 163.7 million (16%) were allocated to this theme. Those projects are strongly informed by a rationale of risk management, automatic detection of abnormal behavior and pro-active surveillance (see for instance IDETECT 4ALL[30]).

One may regret that little attention has been paid to the issues of privacy and societal security in these projects, and that these two areas of research remain marginal in this theme.

[27] PACT (Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action) aims "1) To assess existing knowledge about public perception of the tension between security and privacy and the role played by social trust and concern; 2) To collect empirical evidence about the way in which European citizens perceive and assets in real life novel surveillance technologies; 3) To analyze the main factors that affect public assessment of the security and privacy implications of given security technology. On the basis of such an investigation, the project will develop and validate a prototype Decision Support System, which may help end users to evaluate pros and cons of specific security investments also on the basis of the societal perception of privacy and liberty." Cf. http://cordis.europa.eu/projects/rcn/88217_fr.html

[28] SECILE (Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness) aims to "create an empirically-informed view of the legitimacy and effectiveness of European security legislation, taking into account legal, societal, operational and democratic perspectives. It aims to produce an interdisciplinary and multi-stakeholder understanding of mechanisms for measuring the impact, legitimacy and effectiveness of legal measures, connecting theoretical and practical perspectives with a sound and operationally-informed analysis of these measures in practice. In this way it aims to identify the strengths, weaknesses, assumptions and dissonances across and between existing theoretical, institutional and operational perspectives., The strategic approach of the project is to create dynamic synergies between the legal, sociological and ethical disciplines, authorities and end users in order to generate a holistic understanding of the operation of European legal measures from the perspective of impact, legitimacy and effectiveness." Cf. http://cordis.europa.eu/projects/rcn/108566_fr.html

[29] SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency) is described as follows : "SURVEILLE systematically reviews the impacts of different surveillance systems, and also helps manufacturers and end-users better to develop and deploy these systems. It is a multidisciplinary project combining law, ethics, sociology and technology analysis in a small number of highly collaborative, cross-cutting work packages. SURVEILLE will assess surveillance technology for its actual effectiveness in fighting crime and terrorism, for its social and economic costs, and will survey perceptions of surveillance in the general public and certain identified target groups. The investigation of societal and ethical aspects will focus on undesired side effects of surveillance systems. SURVEILLE will address legal limitations on the use of surveillance technologies as well as ethical constraints. SURVEILLE will include analysis of the potential of 'privacy by design' and privacy-enhancing technologies in the context of surveillance systems.." Cf. http://cordis.europa.eu/projects/rcn/102644_fr.html

[30] IDETECT 4ALL (Novel intruder detection & authentication optical sensing technology) aims at developing "an innovative, Optical Intruder Sensing and Authentication Technology, that will dramatically improve the Cost/Performance ratio of security systems, thus becoming an enabler for the widespread availability of reliable and affordable security, leading to more CIs being protected. iDetecT 4ALL proposes to develop a novel Photonic Sensing technology based on an innovative approach utilizing ultra low cost electro-optical components. This novel approach enables to detect and Authenticate objects by a single sensor. The suggested concept is based on illuminating the protected area with invisible, modulated light, and by using a solid state scanning and detecting technique, to continuously monitor the 3D surface profile within the protected area. Presence and location of intruders will be deyected from the variations inflicted on this 3D profile." Cf. http://cordis.europa.eu/projects/rcn/87259_fr.html

3.3.5 Security of Citizens

This theme comprises 48 different projects which have received € 167.3 million of EU contribution (16%). Beyond their high thematic heterogeneity, these projects feature a dominant preoccupation with regards to the detection, prevention or mitigation of classical or CBRN bombings in urban environments (see SUBCOP[31]). To this end, they resort to techniques of crowd-surveillance in a technologically driven approach that displays little awareness around more political issues, such as racially-biased surveillance.

3.3.6 Restoring Security and Safety in Cases of Crisis

47 projects and € 218.5 million (22%) were allocated to this thematic area. Dedicated to bolstering capacities in terms of crisis management as well as post-crisis recovery, this research theme entails many crosscutting activities with other thematic areas, such as "security systems integration". Above-mentioned concerns raised equally apply to this research area.

3.3.7 Intelligent Surveillance and Border Security

With 33 projects and € 230.7 million (23%), this theme comes off as the top priority of FP7-ST. It focuses heavily on automation of border policing, a priority which is also reflected in the creation of the EU Agency for large-scale IT systems[32]. In the case of border surveillance, it emphasises drones as a technique for bolstering surveillance capacity in wide maritime areas (see EUROSUR[33]). This orientation has drawn criticism from civil rights organisations, especially regarding the dehumanisation of European borders and the de facto dismantling of search-and-rescue capacities that it implies[34]. In the case of border control, automation of identity checks is informed by a firm belief in technology as a way to speed up movement while delivering security (see XP-DITE[35]).

[31] SUBCOP (Suicide Bomber Counteraction and Prevention) "sets out to develop technologies and procedures that can be applied by the Police Security Forces when responding to a suspected PBIED (Person Borne Improvised Explosive Device). (...) SUBCOP will develop guidance as to what response to a PBIED that is ethically and socially justifiable for a given situation. The core objective of SUBCOP is to consider: the available technological tools for less than lethal PBIED intervention, the novel procedures for their application, the development of new less than lethal capabilities." Cf. http://cordis.europa.eu/projects/rcn/108806_fr.html

[32] Cf. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/index_en.htm

[3333] EUROSUR (Sea Border Surveillance) aims to: "1) define the architecture for cost-effective European Sea Border Surveillance systems, integrating space, land, sea and air assets, including legacy systems; 2) apply advanced technological solutions to increase performances of surveillance functions; 3) develop and demonstrate significant improvements in detection, tracking, identification and automated behaviour analysis of all vessels, including hard to detect vessels, in open waters as well as close to coast. SeaBILLA is based on requirements for Sea Border Surveillance defined by experienced operational users. These requirements have been transformed into Scenarios, included in Annex to this proposal, representative of gaps and opportunities for fruitful cooperative information exchange between Members States a) for fighting drug trafficking in the English Channel; b) for addressing illegal immigration in the South Mediterranean; c) for struggling illicit activities in open-sea in the Atlantic waters from Canary Islands to the Azores; in coherence with the EU Integrated Maritime Policy, EUROSUR and Integrated Border Management, and in compliance with Member States sovereign prerogatives." Cf. http://cordis.europa.eu/projects/rcn/94732_fr.html

[34] Ben Hayes, Chris Jones, and Eric Toepfer (2014), *Eurodrones Inc.*, StateWatch Report, 30–32.

[35] XP-DITE (Accelerated Checkpoint Design Integration Test and Evaluation) aims to "to develop, demonstrate and validate a comprehensive, passenger centred approach to the design and evaluation of integrated security checkpoints (CPs) at airports. The approach encompasses a variety of different types of requirements, relating to security, airport operations and societal aspects. An ethical framework will be defined which enables designers and operators to proactively introduce ethical factors in the checkpoint. The project team will identify and develop requirements and criteria at integrated system level. A key element of the project is the development of a design tool that allows the design of innovative new CPs and modification of existing CPs to meet changing threats. A major challenge comprises a validated set of protocols and tools for evaluating and monitoring the performance of

Little attention has been paid, however, to ethical, political and juridical aspects of border control, except for the GLOBE[36] project which represents € 1 million, i.e. 0,0000004% of the credits disbursed solely under this theme.

the CP at the overall system rather than component level."Cf. http://cordis.europa.eu/projects/rcn/104801_fr.html

[36] GLOBE (European Global Border Environment) provides "a comprehensive framework in which an integrated global border management system must be developed. The project will take into account the current and future technological environment. Additionally, GLOBE s scope reaches even further by looking into other key aspects of border management beyond isolated technology, such as the legal and political environment, the social and economic impact of border problems and, more specifically, the impact on information management and integration." Cf; http://cordis.europa.eu/projects/rcn/88217_fr.html

4. FUTURE DEVELOPMENTS IN THE FIELD OF EU SECURITY RESEARCH

KEY FINDINGS

- An examination of the developments within the framework of Horizon 2020 (H2020) foresees that funded research will be mainly put at the service of industry rather than society.
- Only 8 topics deal with the ethical or societal aspects of security research in the 2014-2015 work programme of H2020. The absence of ethical reflection on the uses of technologies of digital surveillance, in particular the impact that these technologies can have on the rule of law, is particularly striking in the post-Snowden era.
- The analysis of the Commission's proposals for an EU security industrial policy further demonstrates that the question of fundamental freedoms and rights is reduced to a matter of commercial considerations and as a limit to the acquisition of otherwise high-performance products.

Examining future developments in the field of EU security research in the perspective of EU-supported public-private partnership requires an analysis of the articulation between research policy and industrial policy. At stake here is the relation between security research and development within the framework of Horizon 2020 (hereafter H2020) and the European Commission's proposals for a *Security Industrial Policy*.[37]

In this section, we argue in particular that the foreseen organisation of this relation results in research being put at the service of industry rather than society. This move is informed by the assumption that whatever is good for industry is necessarily good for society, particularly in times of economic crisis. The assumption that support to industry will lead to job-creation and growth across all sectors, including the security sector, overrules all other societal considerations, which are relegated to preoccupations with societal acceptance of security technologies.

4.1. Security research and public-private partnerships in H2020

H2020 focuses on three priorities: raising the level of excellence in European science, promoting industrial leadership, and addressing societal challenges. Security research in H2020 comes under this last priority, with the heading 'Secure Societies', for which a total amount of € 1.695 billion has been earmarked.

Priorities and funding for the 2014-2015 work programme of the 'Secure Societies' area are distributed as follows.[38]

[37] European Commission (2012). *Security Industrial Policy: Action Plan for an innovative and competitive Security Industry*. COM(2012) 417 final.
[38] All following data is taken from: European Commission (2013). *Horizon 2020 Work Programme 2014-2015 – 14. Secure Societies: Protecting freedom and security of Europe and its citizens*. Brussels, C(2013) 8631..

Figure 11: H2020 Secure Societies Call, 2014 Budget (million Euros)

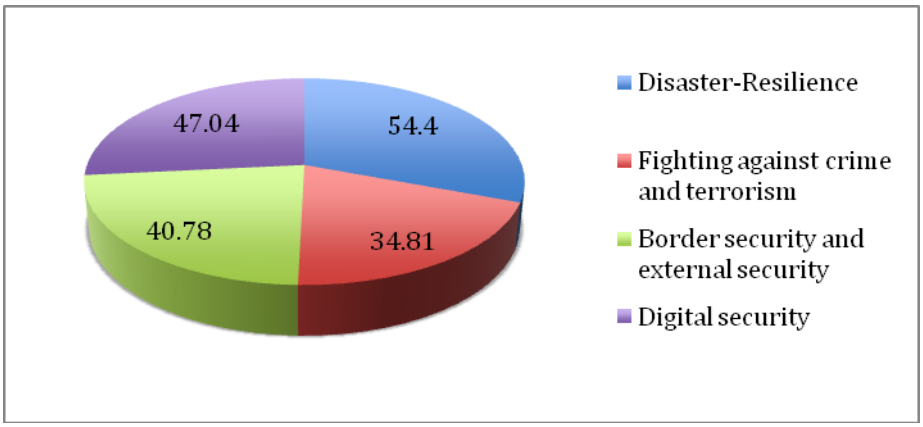
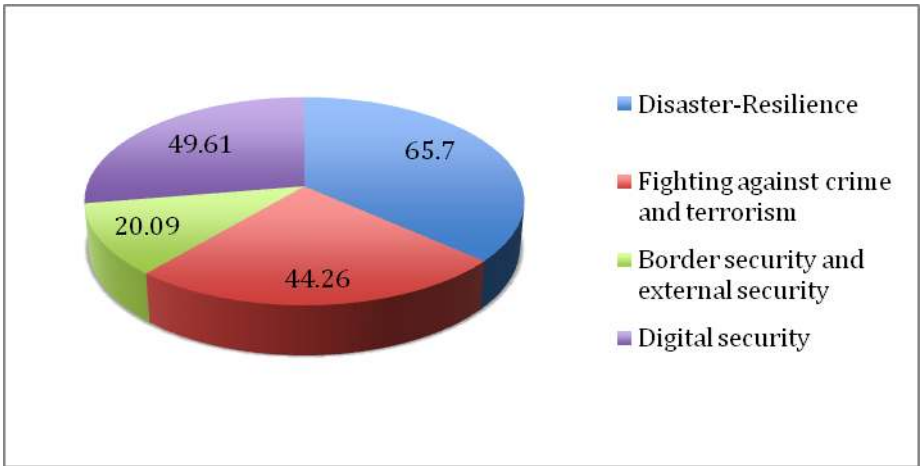


Figure 12: H2020 Secure Societies Call, 2015 Budget (indicative, million Euros)



Each call includes an ethical dimension, except for the call on digital security, where provisions are nonetheless made for research in the area of privacy. 8 topics deal with the ethical or societal aspects of security research in the 2014-2015 work programme of H2020: 3 out of 22 under the call "disaster-resilience", 4 out of 17 under the call "fighting against crime and terrorism" and 1 out of 13, under the call "border security and external security". On top of this rather limited quantity, it is also worth noticing that these topics tend to focus on enhancing the impact and effectiveness of security technology in terms of societal acceptance, sidestepping issues linked with their legitimacy. The absence of ethical reflection on the uses of technologies of digital surveillance, in particular the impact that these technologies can have on the rule of law is particularly striking in the post-Snowden era.

The building of public-private partnerships is a key component of H2020, which is not specific to the 'Secure societies' area. The justification put forward by the Commission is

that 'research and innovation are high risk activities and there is no guarantee of success', the aim of EU policy in this respect being to address 'general market failures'.[39]

4.2. Security research and the EU security industrial policy

The question of research and development in the field of security should be understood in light of the Commission's proposals for the further development of a *Security Industrial Policy*. In the following subsections, we outline the main characteristics of the envisaged policy on the basis of the Commission's 2012 action plan, before analysing their implications.

4.2.1 The Commission's proposals for an EU security industrial policy

The notion of an EU security industrial policy is intimately tied to the work of the high-level venues (GoP, ESRAB, ESRIF) discussed previously. The initial sketch was outlined in a 2009 Commission communication reacting to the final report of ESRIF.[40] The current framework under consideration is detailed in a 2012 action plan, supported by three studies conducted by ECORYS.[41] Comparing and contrasting the 2009 and 2012 communications is useful to understand what kind of lessons, if any, have been drawn from the FP7 Security Theme experience. Here we examine the key points of the 2009 communication, before moving to the analysis of the 2012 action plan (4.2.2. and 4.2.3.).

While framed as a 'reaction' to the ESRIF final report, the 2009 communication is mostly an endorsement of the latter. It summarises the key points of ESRIF's final output, and highlights some areas of particular interest, but does not discuss or debate the findings. The key points concern the '*societal dimension of security*', the improvement of the '*competitiveness of the European Security Industry*', and a research and development roadmap. Each of these points calls for a specific comment:

- The societal dimension consists of '*taking into account the respect for the rights and freedoms of individuals*' in order for security measures '*to gain societal acceptance*' – they should, in any case '*always [be] applied in accordance with the rule of law*'.[42] While the reference to the rule of law is most certainly welcome, **one may ask whether concerns with human rights and fundamental freedoms should primarily be endorsed in relation to the securing of societal acceptance**. The respect for fundamental rights and freedoms constitutes a non-negotiable tenet for a democratic European Union and Member States, rather than a means to an end.
- The question of competitiveness comprises two broad priorities: overcoming market fragmentation on the one hand, and strengthening the (security) industrial base on

[39] European Commission (2013). *Public-Private partnerships in Horizon 2020: a powerful tool to deliver on innovation and growth in Europe*. Brussels, COM(2013) 494 final, p.3.
[40] European Commission (2009). *A European Security Research and Innovation Agenda – Commission's initial position on ESRIF's key findings and recommendations*. COM(2009) 691 final.
[41] ECORYS (2012). *Study on Civil Military Synergies in the Field of Security Final Report*. Brussels: European Commission; ECORYS (2011). *Study on Pre-Commercial Procurement in the Field of Security Within the Framework Contract of Security Studies*. Brussels: European Commission; ECORYS (2011). *Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report*. Brussels: European Commission; ECORYS (2009), *Study on the Competitiveness of the EU Security Industry Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054 Final Report*. Brussels: European Commission.
[42] Ibid, p. 2.

the other. What remains unclear is, firstly, whether the 'security market' is an economic reality in the first place or a policy objective embraced by the Commission in conjunction with specific industrial players. While emphasising market fragmentation, the communication continues to refer to 'markets'. The same reasoning, secondly, can be applied to the 'security industry' and 'security industrial base'. In the definition it provides, the communication refers to '*traditional security industry (based around the supply of general security applications such as e.g. physical access control), security-orientated defence industry (based on the utilisation of defence technologies in security applications or [..] acquisition and conversion of civilian applications to security applications), as well as new entrants, i.e. mainly companies extending their existing (civilian) technologies to security applications, such as for instance IT companies*'.[43] **The result comes across as an ad hoc definition meant to fit the diverse constituency of ESRIF, rather than an evidence-based economic analysis**.

- The research and development roadmap, lastly, shifts the focus from research to innovation, whereby the key focus is extended from the development of technologies to 'the actual deployment of that technology'.[44] The central idea here is that an EU security industrial policy should engage with end-users so that they '*shape and respond to security innovation*' – in other words, to prepare customers to accept and adopt the technologies developed by industrial actors. An important notion outlined in this regard is the development of '*pre-commercial procurement of innovative solutions*', that is the securing of acquisition commitments from 'end-users' before a product is put on the market.[45] In sharp contrast with the idea of shaping a security market, then, **the underlying idea here seems to be the promotion of a non-market commercial relation between the 'security industry' and public sector customers**.

4.2.2 Making up a European security market or fostering industrial champions?

With regard to the 'European security market', the 2012 action plan does not vary much from the 2009 communication, in its objectives as well as in its limits. The 'key policy actions' it envisages here include 'overcoming market fragmentation' and 'reducing the gap from research to market'.[46] Two points can be made in analysing the document:

- **First**, **EU action seems to lack evidence-based strategies**.

A good example is the estimated value of the EU security market. The 2009 communication estimated the market value of the European security industry as ranging from €26 to €36 billion (2008 figures) and '*growing rapidly*'.[47] The 2012 action plan estimates this market value to be '*in the range of €26 billion to €36.5 billion*' for 2011.[48] The idea that the security industry is '*a sector with a significant potential for growth and employment*'[49] serves as a key justification for taking measures in this area. However, the reiteration of the same estimation in a three years interval casts doubt over the relevance of this

[43] Ibid, p. 4.
[44] Ibid, p. 6.
[45] Ibid, p. 9.
[46] European Commission, *Security Industrial Policy*, op.cit., p. 5.
[47] European Commission, *A European Security Research and Innovation Agenda*, op.cit., p. 4
[48] European Commission, *Security Industrial Policy*, op.cit., p. 3.
[49] Ibid, p. 2.

anticipation. At any rate, the growth potential of the security industry needs a clearer assessment.

A similar point can be made about the economic relevance of the 'European security market' and 'European security industry'. The communication notes that '*there is currently no clear definition of the security industry and a methodical classification of this industry is hindered*' in particular by the absence of relevant statistics: the industry '*is not covered as such by the main statistical nomenclature* [..] [and] *the production of security-related items is hidden under a wide range of headings*' which '*do not distinguish between security and non-security related activities*'. There is, finally, '*no statistical data source available at European level from the industry itself*'.[50] Despite the establishment since 2007 of a European Organisation for Security, which has played a significant role in the high-level venues discussed previously, it seems that concerned actors in the private sector themselves do not identify with the idea of a European security industry. One may ask, in this regard, whether the Commission's action plan is creating and addressing a straw man rather than dealing with a set of evidenced economic and industrial issues.

- **Second, it seems that the main aim of a European security industrial policy is to make up, rather than act upon, a European security market and industry.**

This endeavour is based, firstly, on an ad hoc definition of the 'security industry' that reflects broadly the scope of activities of the companies whose representatives have been involved in ESRIF, consisting of '*aviation security, maritime security, border security, critical infrastructure protection, counter-terrorism intelligence (including cyber security and communication), crisis management/civil protection, physical security protection and protective clothing*'.[51] These, however, are distinct areas of economic activities, and the extent to which they constitute a market would deserve a more thorough examination. In this sense, it is unclear whether the notion foregrounded by the Commission that EU action is required to overcome 'market fragmentation' is an actual cause for concern, or a way to legitimise its past and foreseen undertakings.

- **Third, and following this observation, the degree to which the EU's 'security industrial policy' would aim at supporting market mechanisms is unclear.**

It seems that the aim of the 2012 action plan is the fostering of industrial champions, through an economic model premised less on market mechanisms than on the promotion of privileged relations with institutional (public) customers, and on an export-driven strategy. In particular, the action plan aims to foster reliance on pre-commercial procurement (PCP) and the PCP instrument established under H2020. The action plan also deplores the 'lack of [..] a "EU brand"' similar to the 'US brand' enjoyed by American companies on the export market.[52] The aim of 'a true Internal Market for security technologies' would then be to provide 'a strong home base for the EU security industry with a view to gain market shares in emerging markets'.[53]

[50] Ibid, p. 3.
[51] Ibid, p. 4.
[52] Ibid, p. 2.
[53] Ibid, p. 3.

4.2.3 Research for closing market gaps and securing societal acquiescence

The role of EU-sponsored security research in the context of an EU security industrial policy is twofold.

In line with the 2009 communication, the 2012 action plan puts emphasis on '*reducing the gap from research to market*'. New Intellectual Property Rights (IPR) and the PCP instrument built in H2020 are meant to foster '*a more direct and faster exploitation of the results of EU security research by the national authorities*'.[54] Research, then, is envisaged firstly in terms of commercial outputs.

The second role of EU-sponsored security research in the perspective of an EU security industrial policy is a '*better integration of the societal dimension*'.[55] This includes considerations related to '*societal and fundamental rights*' (although one could question the meaning of 'societal rights' from a legal perspective) and the commitment that '*the Commission will involve society and make societal impact testing an obligatory part, where appropriate, of all its future security research projects*'.[56] The 2012 action plan here outlines more specifically the importance of privacy by design and privacy by default. Questions arise, however, when considering the purpose of a better-integrated societal dimension. The action plan notes here that '*the societal acceptance of new products and technologies is a general challenge across different industrial sectors*' and that not meeting this challenge might lead to '*negative consequences. For industry, it means the risks of investing in technologies, which are then not accepted by the public, leading to wasted investments. For the demand side, it means being forced to purchase a less controversial product, which however does not entirely fulfil the security requirements*'.[57] **The question of fundamental freedoms and rights, then, is reduced to a matter of commercial considerations and as a limit to the acquisition of otherwise high-performance products.** The societal dimension of security research is therefore meant to '*help in reducing the uncertainty of societal acceptance*'.[58] The degree to which this policy orientation is in line with the Treaties and the international commitments of the European Union and its Member States, including the European Convention on Human Rights, is unclear. Observance of fundamental freedoms and rights is not a means to an end, be it in a period of economic crisis, but an absolute pre-requisite.

[54] Ibid, p. 9.
[55] Ibid, p. 11.
[56] Idem.
[57] Ibid, p. 5.
[58] Ibid, p. 9.

5. CONCLUSION AND RECOMMENDATIONS

5.1. Conclusion: security, society and industry

Previous assessments have argued that security research has failed to address questions that are essential to security issues: what do we want to protect? How do security measures impact what we want to protect? The present study confirms that security research continues to overlook such questions under FP7-ST and will probably continue to do so under H2020.

- **The policy-making process on security research sidesteps a number of societal actors**. This is reflected both in the high-level Public-Partner Dialogue and in the second-track expert groups tasked with defining security research, where representatives of security industry and public security bodies are overwhelmingly present, at the expense of actors who may speak in the name of the citizens, including MEPs or non-governmental organisations. The unequal representation of industry, security agency and civil society in the policymaking process helps to understand why security research in the European Union is framed in a way that ignores the interests of the latter.
- This trend has only been reinforced by the worsening economic context that has impacted the implementation of FP7-ST and will continue to influence the implementation of H2020. Security research **puts research at the service of industry rather than society.** This move is grounded in the assumption that support to industry will lead to job-creation and growth across all sectors, including the security sector. This assumption overrules all other societal considerations, which are relegated to preoccupations with societal acceptance of security technologies.
- In this context, **the recent revelations regarding programmes of massive electronic surveillance**, which have multiplied in the aftermath of the Snowden case, **have simply not been taken into account in the programming of the H2020**. 'Business as usual' seems to be the default position of the European Commission in these matters.

We argue, instead, that the respect of the rights and freedoms of individuals facing the effects of EU security policies should, now more than ever, become central in security research. The following recommendations build on this conclusion.

5.2. Recommendations

Recommendation 1: The 'end-user' category needs to be clarified.

In particular, the distinction between public security agencies, bodies and services of the European Union and its Member States on the one hand and civil society organisations on the other should be asserted more strongly. This would prevent the monopolisation of the role of end-user by any of these two sub-categories. Additionally, both sub-categories must be associated on equal footing in the definition and/or implementation of security research activities.

Recommendation 2: A minimum threshold could be set in terms of budget allocated to universities and university partnerships.

The growing marginalization of Social Science and Humanities in research funded by the European Commission has drawn growing concerns from academic actors. In an open letter recently sent to Commissioner Geoghegan-Quinn, a group of scholars underline that the "Commission seems to regard SSH as a service function for other priorities, such as energy and transport, rather than as a means of addressing the acute social problems that Europe faces".[59] This remark converges with the findings of the present report. In order to address this issue, a minimum threshold could be set in terms of budget allocated to universities and university partnerships. Projects that do not meet this minimum threshold would then not be eligible for funding.

Recommendation 3: Relations between technology-driven research and the political, societal, ethical and juridical aspects of security should be clarified.

The emphasis has overwhelmingly been put on the former at the expense of the latter. Better integration of academic partners with backgrounds in social science should be promoted. The model of integration/coordination has failed at producing fruitful cross-fertilisation and should be replaced by a model of separation/cooperation, whereby provision would be made for independent research in the field of social science and security. A stronger cooperation framework should also be extended at the level of the programmes.

Recommendation 4: Further clarification about the role of third state partners in security research is required.

The fact that a sizeable amount of funding in the field of security research is allocated to institutions of third-states, such as Turkey and Israel, whose track record in terms of respect for human rights and international conventions is highly questionable, has raised considerable concern. In light of this finding, the European Parliament should tackle this issue. In particular, it would be worth asking for further clarification about the role of third state partners in security research, as well as the safeguards they provide to ensure the respect of the fundamental freedoms and rights of their populations.

Recommendation 5: Security funding must foreground fundamental and technical research to ensure that EU serves and protects its citizens

While the priorities of the EU include 'serving and protecting citizens', security research programmes have only partly addressed the concerns of EU citizens. In light of the Snowden revelations, it appears that if the European Union is to be recognised as a centre of technological innovation and economic growth that is also respectful of fundamental rights and privacy, security funding must foreground fundamental and technical research to ensure that:

- the right of individuals not to be illegitimately spied on is respected;
- the ownership of EU citizen over their personal data online in ascertained;
- European citizens are free from concern about pervasive technologies intruding in their private and professional life.

[59] See the open letter to Commissioner Georghean-Quinn at http://www.net4society.eu/public/473.php

Recommendation 6: More support should be provided for research in the field of free and open source software in the domain of security and privacy as topic for the next H2020 call.

While open source software offers several advantages over proprietary software such as (a) more security and privacy guarantees (b) significant savings in costs for systems security (c) an open access to technological innovation, it is unfortunately entirely absent from the H2020 call. Thus, research in the area of free and open source software should be encouraged and funded, for the following reasons:

- Open source software offers more guarantees for privacy and security than proprietary software in a broad range of domains. Encryption software packages such as GPG or TrueCrypt, anonymous browsing systems such as TOR are unanimously considered more reliable encryption systems than any commercial solution. The reasons behind this fact are simple: open source software can be and is regularly scrutinised by a broad community of software developers, who are able to detect backdoors and vulnerabilities.
- Open source software is most of the time free to use. Beyond encryption technologies, free software can replace most of proprietary software for governments and businesses, for diverse critical applications such as operating systems, traffic routing, email, file storage or instant messaging. Free software also covers the majority of office (word processor, etc.) needs and helps therefore cut significant expenses. In the aftermath of the Belgacom scandal[60], European institutions might want to turn to the free software community for their security needs.
- Finally, the open source and free software community has been at the very core of the development of the most important technological advancements of the past years in terms of digital technologies, resulting in important technological innovation.

[60] The NSA files released by Edward Snowden revealed that the European institutions were spied on by the GCHQ through an attack on the Belgian telecom operator Belgacom. See "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm" *Spiegel Online,* September 20, 2013

REFERENCES

Peter Burgess and Monica Hanssen (2008). Public-Private Dialogue in Security Research. Brussels: European Parliament, PE 393.286.

Rocco Bellanova and al. (2012). *Supporting Fundamental Rights, Privacy and Ethics in Surveillance Technologies - Smart Surveillance - State of the Art*. Oslo: PRIO.

Didier Bigo and al. (2008). *INEX - Security Technologies and Society. A State of the Art on Security, Technology, Borders and Mobility*, INEX. Paris: Centre d'étude sur les conflits.

Didier Bigo and Julien Jeandesboz (2008). *Review of security measures in the 6th Research Framework Programme and the Preparatory Action for Security Research*. Brussels: European Parliament, PE 393.289.

Didier Bigo and al. (2013). *Open Season for Data Fishing on the Web The Challenges of the US PRISM Programme for the EU*, CEPS Policy brief, Brussels: Centre for European Policy Studies.

ECORYS (2012). *Study on Civil Military Synergies in the Field of Security Final Report.* Brussels: European Commission.

ECORYS (2011). *Study on Pre-Commercial Procurement in the Field of Security Within the Framework Contract of Security Studies*. Brussels: European Commission.

ECORYS (2011). *Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report*. Brussels: European Commission.

ECORYS (2009). *Study on the Competitiveness of the EU Security Industry Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054 Final Report*. Brussels: European Commission.

European Commission (2006). Regulation No 1906/2006 of the European Parliament and of the Council of 18 December 2006 laying down the rules for participation of undertakings, research centres and universities in actions under the Seventh Framework Programme and for the dissemination of research results (2007-2013), Official journal of the European Union L 391/1, 30.12.2006.

European Commission (2006). *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.

European Commission (2007). *Commission Staff Working Document on Public-Private Dialogue in Security Research and Innovation*. SEC(2007) 1138.

European Commission (2009). *Mandate for the Security Advisory Group for the 7th Framework Programme*. Available from: http://ec.europa.eu/research/fp7/pdf/advisory-groups/security-mandate.pdf

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

European Commission (2010). *Report of the 2nd Meeting of the FP7 Security Advisory Group*. Available from: http://ec.europa.eu/research/fp7/pdf/old-advisory-groups/security-firstreport_en.pdf.

European Commission (2010). *FP7 Security Advisory Group Membership*, Available from http://ec.europa.eu/research/fp7/advisory_en.html.

European Commission (2012). *Security Industrial Policy: Action Plan for an innovative and competitive Security Industry*. COM(2012) 417 final.

European Commission (2012). *FP7 Security Advisory Group Annual Summary June 2011 - June 2012.* Available from: http://ec.europa.eu/enterprise/policies/security/files/secag-annual-summary-2011-2012-issue-1-0_en.pdf.

European Commission (2013). *Horizon 2020 Work Programme 2014-2015 – 14. Secure Societies: Protecting freedom and security of Europe and its citizens*. Brussels, C(2013) 8631.

European Commission (2013). *Public-Private partnerships in Horizon 2020: a powerful tool to deliver on innovation and growth in Europe*. Brussels, COM(2013) 494 final

European Parliament (2013). Regulation No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, Official Journal of the European Union L 347/104.

European Parliament (2014). European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). Brussels, P7_TA-PROV(2014)0230.

Ben Hayes (2009), *NeoConOpticon. The EU Security-Industrial Complex* (Transnational Institute / Statewatch, 2009)

Ben Hayes, Chris Jones and Eric Topfer (2014). *Eurodrones Inc.* (Amsterdam: Statewatch / TNI)

Ben Hayes (2013). "How the EU Subsidises Israel's Military-Industrial Complex", available from: http://www.opendemocracy.net/ben-hayes/how-eu-subsidises-israel%E2%80%99s-military-industrial-complex.

Julien Jeandesboz and Francesco Ragazzi (2010). Review of security measures in the Research Framework Programme. Brussels: European Parliament, PE 432.740.

Statewatch (2010). *Security Co-Operation between the EU and Israel*, available from: *http://www.statewatch.org/news/2010/nov/quaker-esrc-briefing.pdf*

EUROPEAN PARLIAMENT

CATALOGUE QA-01-14-399-EN-C

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: 978-92-823-5715-6
DOI: 10.2861/62647

Publications Office