

The EU and the European Security Industry

Questioning the ‘Public-Private Dialogue’

**Didier Bigo
& Julien Jeandesboz**

No. 5 / February 2010



Research for this Policy Brief was conducted in the context of INEX, a three-year project on converging and conflicting ethical values in the internal/external security continuum in Europe, funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme. The project is coordinated by PRIO, International Peace Research Institute in Oslo. For more information about the project, please visit: www.inexproject.eu



International Peace Research Institute, Oslo

THE EU AND THE EUROPEAN SECURITY INDUSTRY QUESTIONING THE ‘PUBLIC-PRIVATE DIALOGUE’

DIDIER BIGO & JULIEN JEANDESBOZ*

INEX POLICY BRIEF NO. 5/FEBRUARY 2010

Introduction

In September 2007, the European Commission published a Communication on “Public-Private Dialogue in Security Research and Innovation” (European Commission, 2007a). The outcome of a joint venture between DG Enterprise and Industry and DG Justice, Freedom and Security (DG JLS), it sought to specify the guidelines, objectives and modalities for the relations between public and private actors in EU-funded security research schemes, in the context of introducing a ‘Security’ theme within the Community’s 7th Framework Programme (FP7).

The tabling of this Communication, however, is misleading. Indeed, relations between the European institutions, particularly the European Commission, and major companies in the field of defence and security, have intensified significantly since the early 2000s. Starting with the establishment of the *Group of Personalities on Security Research* (GoP) in 2003 and the launch of the Preparatory Action on Security Research (PASR) in 2004, it seems that these relations have in fact already moved beyond a mere ‘dialogue’. Major defence and security companies have played a key role in the definition of the orientation and priorities of the EU’s research and development policy for security-related technical systems – and also turn out to be the major beneficiaries of this policy.

This observation leaves unanswered a series of questions concerning the ‘dialogue’ advocated by the European Commission. Firstly, between whom is this dialogue supposed to take place? Previous and current EU security research schemes have notoriously left little room for participants other than major industrial groups, on the one hand, and national and European security agencies and services, on the other. Secondly, what should be the purpose of such a dialogue? So far, the objectives of EU security research schemes remain vague and their priorities undefined. They include enhancing the protection of EU citizens in the face of “new threats”, the preservation of “European values” as well as sustaining the “European industrial base”. In the meantime, a serious assessment - which would go beyond a mere cataloguing - of the priorities that need to take precedence (including in financial terms), and of the ‘threats’ that are not a priority is still lacking. The analysis of insecurities, their diversity, their inevitability in an open world, is never properly carried out. In the process, the fact that insecurity also means opportunity and freedom, which would counterbalance the ideology of a security for all by showing it to be an untenable argument, is put aside. Technology is embraced as an unquestionable component of the EU’s security policies. It is presented as a solution not only for one given threat, but for many, if not all of them. This perspective sustains a tendency to adopt as the best technology the one that is purported to be the most multi-functional, capable of simultaneously confronting several threats – technical systems are ‘added’ onto one another, such as in the case of biometrics, computerised databases and speedy exchange of information when confronting the difficulties posed at the transnational level by any form of freedom of circulation (except, for a while at least, the circulation of capital). This lack of reflection upon

* Didier Bigo is President of the Centre d’Etudes sur les Conflits and Professor at the Institut d’Etudes Politiques de Paris. Julien Jeandesboz is associate researcher at the Centre d’Etudes sur les Conflits and Ph.D. candidate at the Institut d’Etudes Politiques de Paris.

the effects and implications of current and future technical systems, beyond discussions of their ‘capabilities’ or ‘efficiency’, is all the more problematic as civil liberties and privacy organisations, but also European and national agencies in charge of these questions have at best been marginalised as ‘end-users’, or worse, completely excluded from EU security research schemes.

The present briefing note provides a brief overview in section 1 of the relations between the EU and the defence and security industry. Section 2 proceeds to discuss the notion of ‘dialogue’ as promoted by the European Commission and a set of conclusions for future developments is outlined in a final section.

1. Relations between the EU and the European security industry: An overview

1.1 The emergence of EU security research

Relations between the EU and the European defence and security industry date back to the early 1990s, when the main industrial associations of European defence and aerospace industries opened offices in Brussels. For most of the decade, the main point of contention arose in the efforts of the European Commission to incorporate defence procurement markets into the framework of the Single Market, despite the opposition of member state governments.

European security research initially emerged as a policy issue out of the armament markets. In a 2003 Communication on “Towards an EU defence equipment policy”, the Commission changed its approach to the question by expanding the question of defence procurement to include the hazy notion of ‘global security’ (European Commission, 2003: 16). The reference was a clear attempt to join the bandwagon on the acceleration and transformation of European security policies following the attacks in the US on 11 September 2001. Within this perspective, the Commission offered in particular its ‘expertise for an initiative to promote cooperation on advanced research in the field of ‘global security’ (European Commission, 2003: 16). ‘Security research’ subsequently became the new label under which relations between the EU institutions and the European defence and security industries developed. While the Commission proceeded to establish a succession of high-level venues bringing together representatives from the public and private sector to discuss this matter (discussed below in section 1.2), defence and security industries re-engineered their pattern of engagement with the Brussels arenas, establishing two new professional associations in the process (see section 1.3). EU security research, on the other hand, materialised through two successive initiatives: the PASR and FP7-Security Theme (elaborated in section 1.4).

1.2 High-profile venues in the field of security research

In the period 2003-09, the European Commission established or supported three successive high-profile bodies on the issue of security research: the *Group of Personalities on Security Research* (GoP, 2003-04), the *European Security Research Advisory Board* (ESRAB, 2005-06) and the *European Security Research and Innovation Forum* (ESRIF, 2008-09). All three bodies brought together executives from major European defence and security companies (e.g. BAE Systems, Diehl, EADS, Ericsson, Thales, Sagem, Siemens), European officials from the Commission and the Council, representatives from a handful of established think tanks (e.g. the EU Institute for Security Studies, the Fondation pour la recherche stratégique, the Istituto Affari Internazionali), and a number of officials from national and European security agencies and services (both police and military).

Through their reports, the GoP and ESRAB have had a strong influence over the shaping of EU security-research schemes. The main proposal developed by the GoP report in this regard is the establishment of a European security research programme (ESRP) from 2007 onwards, relying

in part on the experience, which was ongoing at the time, of the PASR. ESRAB's final report takes on the same view, further singling out four main 'mission areas' of interest:

- Border security
- Protection against terrorism and organised crime
- Critical infrastructure protection
- Restoring security in case of crisis.

The proposals of the GoP and ESRAB were largely taken up by the Commission in the crafting of the FP7's Security Theme.

A third venue, the *European Security Research and Innovation Forum* (ESRIF), was established in September 2007. While the Commission was not its initiator, it nonetheless strongly supports its creation in the abovementioned Communication on "Public-Private Dialogue".¹ Chaired by the former EU Counter-Terrorism Coordinator Gijs de Vries, ESRIF is fairly similar to ESRAB in terms of constituency: a close-to-identical 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). ESRIF, incidentally, is also characterised by a stronger influence of member state governments and FP7 associated countries, which control the nominations to the forum. The objective of ESRIF, as stated by its chairman in the foreword to the forum's interim 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" (ESRIF, 2008: 5). ESRIF is then essentially a foresight exercise to establish a roadmap for European security research beyond the 2013 deadline of FP7.

1.3 Representation of the security industry in the European governmental arenas

In recent years, the presence of the defence and security industries in Brussels has evolved from their original footholds established in the early 1990s, both in terms of organisation and orientation. One important step was taken with the creation of ASD (Aerospace and Defence Industries Association of Europe). Another recent development has been the constitution of the European Organisation for Security (EOS). EOS was established in July 2007, both to "support a consistent and comprehensive implementation of security strategies at national, European and international level" and to "support the development of a European security market", by "developing a common understanding of security requirements" and "supporting the definition of sectoral solutions that are interoperable across applications and borders".² The membership of EOS is composed of major companies in the field of defence and security, of professional associations (most prominently, ASD) and to a lesser extent, of so-called 'research organisations' (e.g. TNO³), representatives of which staff the governing board of the organisation.

Both ASD and EOS have been established with a clear angle: engaging with the European institutions, to support 'European' technological products in the field of defence and security, and the market thereof. The constituencies and governing boards of ASD and EOS are largely

¹ ESRIF was announced at the second Security Research Conference in Berlin in March 2007.

² EOS website (www.eos-eu.com).

³ *Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek* (Netherlands Organization for Applied Scientific Research).

similar - if one excludes the fact that the basic membership of ASD is composed of national associations instead of individual companies, while EOS membership is more of a mixed crowd. The EOS website, however, places strong emphasis on the fact that the organisation “addresses different domains of Security”, including “Green and Blue Border Surveillance, Security and Safety”, “Critical Infrastructure Protection” and “Civil Protection” – which incidentally correspond to the mission domains singled out by ESRAB in its final report, and currently explored by ESRIF.

1.4 The security industry in European research schemes

EU-funded security research has evolved into an important financial and political stake since 2003. A first approach was initiated through the establishment the PASR (OJEU, 2004) which, over the period 2004-06, sponsored 39 actions and pilot projects in various domains of security research⁴ receiving a total Community contribution of €44.5 million. One-third of these projects were led by major defence and security companies (Thales, EADS, Finmeccanica, Sagem and their European association ASD), which overall participated in two-thirds of the PASR activities (Hayes, 2009: 12). Incidentally, most of these companies were also represented in the GoP and ESRAB.

Following the recommendations of the GoP, the Commission established a major security research component within the Community’s FP7. Dubbed ‘Security Theme’, it accounts for about 4% of the FP7’s Cooperation Programme (CP).⁵ This figure, however, is somewhat misleading insofar as one can find security-related projects in other segments of the Cooperation Programme, such as Information and Communication Technologies (28% CP) Transport (12%) or Space (4%). The funds earmarked for the five years of the Security Theme nonetheless represent 30 times the amounts allotted for the three-year PASR. The European Commission has document 45 projects funded under the Security Theme so far (as of May 2009). Out of these, the organisations which were initially represented in the GoP total 32 individual participations, and have taken the lead on 7 projects.⁶ While not as obvious as for the PASR, these figures are indicative of a pattern in which major defence and security companies are contributing to the shaping of EU security and research policies on the one hand, and becoming important beneficiaries of these policies on the other.

2. Analysis: Questions about the ‘Public-Private Dialogue’ in EU security research and its implications

The findings briefly presented so far raise important questions with regard the so-called ‘Public-Private Dialogue’ advocated by the European Commission in its eponymous 2007 Communication. The first question (2.1) that one feels compelled to ask in this respect is: dialogue between whom? Who are the ‘stakeholders’ that are actually (or supposed to be) involved? A second question (2.2) to be raised in this respect involves the objectives of such a ‘dialogue’, and the adequacy between existing patterns of relations and these objectives. Here, we find in particular the issue of competitiveness, but also to some extent of transparency in the attribution of EU research funding.

2.1 Dialogue between whom?

The Commission’s 2007 Communication stipulates that ‘[d]eveloping an effective security research policy [...] requires the implication of all relevant stakeholders’ (European

⁴ See Bigo & Jeandesboz, 2008, for an overview.

⁵ Representing some €1,350 million out of a total of €32,365 million (see European Commission, 2007b, p. 4).

⁶ Among them, Thales presents the most impressive record, participating in 10 projects and leading 3.

Commission, 2007a). The document, however, remains mostly unclear as to who these ‘stakeholders’ are supposed to be. It mentions several times the notion that these include the ‘supply and demand’ sides of security research and technologies. It also points out ESRIF as the adequate venue for the envisaged Public-Private Dialogue to take place, by bringing together “a balanced representation of all stakeholders [...] i.e. industry, research establishments, public and private end-users, civil society organisations, European institutions, in particular the European Parliament, and European organisations” (European Commission, 2007a: 10).

An overview of the current membership of ESRIF, however, offers a sobering perspective on the actual shape of the ‘dialogue’ that this forum would be spearheading. Out of the 64 formal members of ESRIF, 34 are public officials, a majority of whom come from European or national security agencies and services, 16 represent corporate entities (including familiar names such as EADS, Finmeccanica, Thales, Sagem), 9 come from the academic sector and 5 from either public or private think tank structures. Due to overlapping responsibilities, five ESRIF members can be construed as representing ‘civil society’ (Hayes, 2009: 23). The ESRIF plenary, however, does not feature any representative from civil liberties or privacy organisations, nor representatives from the European Parliament. The same holds true for the 660 ‘stakeholders’, participating in the 11 working groups set up by ESRIF. According to the figures obtained by Statewatch researchers from the Commission, 66% (433) originate from the defence and security industry (with ASD, EADS, Finmeccanica and Thales totalling 102 contributors by themselves), 30% (200) from the ‘demand side’ (national or European public sector), while only 9 participants can be accounted for as ‘civil society’ (1.4%), none of which is actually part of a civil liberties or privacy organisation (Hayes, 2009: 24).

The ‘dialogue’ foreseen by the European Commission and supposedly exemplified by ESRIF, is therefore currently a dialogue between the security and defence industry, particularly major transnational companies, and likely public sector customers. The absence of civil liberties and privacy organisations is probably the most striking aspect of ESRIF’s constituency. Another cause for concern is also the minority position occupied by representatives of academic bodies, which points to the confiscation of a whole facet of the European Research Area by private interests in accord with public authorities. This trend is all the more problematic as the objectives of a ‘dialogue’ in European security research remains unclear.

2.2 Dialogue for what?

The introduction of the Commission’s Public-Private Dialogue Communication specifies that “one of Europe’s main objectives is to preserve its values of open society and civil liberties while addressing the increased security threat. At the same time, Europe must secure its economy and its competitiveness...” (European Commission, 2007a: 2). The ‘dialogue’ envisaged by the communication is then geared towards a threefold objective: upholding values and fundamental liberties, guaranteeing security and preserving (and possibly enhancing) its competitiveness and economic growth.

These three priorities, to say the least, have been rather unequally pursued in the context of EU security research. In its report, the GoP already indicated that such research should be “capability-driven”, i.e. dealing with questions such as “[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?” (GoP, 2004: 16). The ESRAB report advocates “research activities that aim at identifying, preventing, deterring, preparing and protecting against unlawful or intentional malicious acts harming European societies; human beings; organisations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (also applicable after natural/industrial disasters)” (ESRAB, 2006: 18).

In the meantime, very little attention is dedicated to the question of fundamental freedoms and rights, and on the impact that new or improved technological ‘capabilities’ might have on those. When this is done, however, the dominant idea remains that freedom and security are equivalent values that should be ‘balanced’. The final report of the ESSTRT consortium,⁷ one of the projects funded by the European Commission under the PASR, is illuminating in this respect. It notes that “[a]chieving the right balance between civil rights and security is challenging. A broad democratic debate on threats and responses offers the best guarantee that tougher security measures and enhanced powers conferred upon intelligence services and police forces have public consent” (ESSTRT, 2006: 20). It further specifies that “[a]nother factor to be taken into consideration is the relative efficiency of technologies. For example, facial recognition systems at present are very unreliable. *The choice of technologies will become political and ethical if it is between efficient, but highly privacy-invasive systems and less efficient, but privacy-neutral solutions*” (ESSTRT, 2006: 21. *Emphasis added*). While democratic debates on European security policies and their implications for the fundamental rights and freedoms of individuals are certainly *necessary*, they are by no means *sufficient*, for some of the contemporary practices that are related to the technological management of insecurities fall beyond the scope of democratic investigation and scrutiny. Furthermore, the dominant viewpoint, as asserted in the ESSTRT report, frames the issue of privacy in terms of a choice between effective intrusiveness and non-intrusive inefficiency. **The underlying assumption is that intrusiveness is a requirement for efficiency, and that privacy undermines efficiency (and thus enhances potential insecurities).** Finally, the report favours the notion of ‘privacy-neutral’ prospects, over the possibility of ‘privacy-enhancing’ ones (which are however mentioned previously). Such a perspective by all means impoverishes the scope of discussions related to the ethical and political assumptions and the effects of security technologies.

Part of the problem, here, lies in the fact that most of the projects funded by EU security research schemes are technical – i.e. focusing on engineering issues and technological development/demonstration. For instance, out of the 39 activities funded under the PASR, only two (ESSTRT and PRISE) take into consideration the broader legal, political and social implications of the reliance on security technologies (Bigo & Jeandesboz, 2008: 10). Within the 45 documented projects of FP7-Security Theme, the INEX and DETECTER (*Detection Technologies, Terrorism, Ethics and Human Rights*) projects, and to a lesser extent the social science component of the GLOBE (*Global Border Environment*) project actually investigate the ethical, legal, political and social implications of the growing reliance on technical devices for security purposes.

The objective of ensuring the “competitiveness of European industry in the security research area” (European Commission, 2007a: 7-8) should also be assessed critically. EU security research tends to be dominated by larger companies capable of a broad scope of activities and investments (EADS, Thales and Sagem being the most recurrent), while small and medium companies (SMEs) are almost invisible – although at least one PASR activity (SecureSME, third call) deals with their involvement in EU research and development schemes. Furthermore, the involvement of major companies *both* in the policy process of establishing EU security research schemes and as applicants for funding through these schemes, appears highly problematic insofar as the fairness and transparency of the application process is concerned. Finally, this involvement appears to be self-sustaining. Most of the corporate participants in the GoP were involved in ESRAB, and in turn in ESRIF. Within the FP7-Security Theme, the CRESCENDO project (*Coordination action on Risks, Evolution of threats and context*

⁷ The ‘European Security: High Level Study on Threats, Responses and Relevant Technologies’ consortium was composed of Thales Research and Technology and Thales e-Security (UK), the International Institute for Strategic Studies (IISS, UK) and the Crisis Management Initiative (presided over by Matti Ahtisaari, Finland).

assessment by an enlarged network for an R&D roadmap) is the follow-up to two PASR activities (SeNTRE and STACCATO) and aims at furthering and expanding the public/private, expert/stakeholder network already established in previous schemes. These elements raise a number of issues – not the least being the actual desirability to foster or support ‘European champions’ in a domain that used to be the turf of ‘national champions’ in view of the EU’s competition policy, or of the objective of supporting a strong industrial basis in a way that would be detrimental to SMEs.

3. Recommendations

As we have seen, the lack of reflexivity and the path dependency that characterise established relations between the industry and member states’ ministries of defence, has been extended to the ministries of interior through the involvement of DG Enterprise. In the meantime, it has excluded or relegated to mere ‘addenda’ the bodies, groups and organisations working on such related questions as policing accountability, surveillance, civil liberties in relation to security and human rights. This orientation, which has been embraced since the very beginning, has forced these groupings to set up, often without financial backup of any kind, their own networks – which have been composed more of NGOs and academics than companies. In this respect, one can question the internal choice of the European Commission to put DG Enterprise in charge of the EU’s activities in the field of security research and development – a choice that has resulted in an unbalanced and narrowed down understanding of security issues in these research schemes. It is important to recall, in this perspective, that legal questions related to freedom and human rights are, and should be, key elements for any research on security technologies. At the moment, beyond the occasional exception, these issues have mostly been relegated to the devising of ‘codes of conduct’ for ethical research. The entanglement of internal and external security concerns implies new relations involving a growing number of actors. Any effort to achieve ‘global security’, or even an ‘area of security’ as in the case of the EU, through technology involves, beyond defence and border interdiction, issues related to intelligence, policing, border crossing, justice, data protection, citizenship, the rights of foreigners, ethics, and the questions of freedom of movement and presumption of innocence – particularly in a context where pre-crime strategies and prevention through sophisticated technologies are given priority.

It is therefore central to see that the EU Ombudsman and his network, the European Agency for Fundamental Rights, the European Data Protection Supervisor and the Art. 29 Group, as well as the LIBE and Human Rights Committees of the European Parliament are granted the possibility to offer significant research funding on the issues of security, privacy and freedom.

Secondly, these bodies should be entitled to examine and assess the findings of other research schemes financed by the EU to see if they are in compliance with their objectives. Finally, they should be involved extensively in the framing of calls for proposals.

Before a full reorganisation is launched (in preparation for the upcoming 8th Framework Programme), a transition initiative should be undertaken, to promote in particular a better awareness on the part of DG Enterprise of the broader implications of security research. This could alternatively take the form of a specific social science call on security, freedom, human rights and privacy, or of the creation of a network of experts chosen in equal parts by the main protagonists, whose mission would be to envisage alternative framings to these questions – emphasising, beyond the link between technology as an alleged ‘requirement’ for security, the entanglement of freedom and security as two sides of the same coin.

References

- Bigo, D. and J. Jeandesboz (2008), *Review of Security Measures in the 6th Framework Research Programme and the Preparatory Action For Security Research*, Briefing Note for the European Parliament, PE 393.289, Brussels (<http://www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=21149>).
- ESRAB (2006), *Meeting the Challenge: the European Security Research Agenda*, Office for Official publications of the European Communities, Luxembourg.
- ESRIF (2008), *European Security Research and Innovation in support of European security policies: intermediate report*, Office for Official publications of the European Communities, Luxembourg.
- ESSTRT Consortium (2006), *European Security: High Level Study on Threats, Responses and Relevant Technologies*, study financed by the European Commission under the Preparatory Action for Security Research (PASR) (<http://www.iiss.org/programmes/defence-analysis-programme/analysis-archive/european-security-high-level-study/>).
- European Commission (2003), *European defence – Industrial and Market Issues: Towards an EU Defence Equipment Policy*, Brussels, COM(2003) 113 final.
- European Commission (2007a), *Communication on Public-Private Dialogue in Security Research and Innovation*, Brussels, COM(2007) 511 final.
- European Commission (2007b), *FP7 – Tomorrow’s answers start today*, DG Research, Brussels (http://ec.europa.eu/research/fp7/pdf/fp7-factsheets_en.pdf).
- Hayes, B. (2009), *NeoConOption: The EU Security-Industrial Complex*, Transnational Institute, Amsterdam (<http://www.statewatch.org/analyses/neoconopticon-report.pdf>).
- GoP (2004), *Research for a Secure Europe: Report from the Group of Personalities in the field of Security Research*, Office for Official Publications of the European Communities, Luxembourg.
- (OJEU) 2004, *Commission Decision of 3 February 2004 on the Implementation of the Preparatory Action on the Enhancement of the European industrial potential in the field of security research*, L67, 18-22, Brussels, 5 March.