



**The European Security Research Programme: a  
challenge for existing police cooperation  
networks in the EU**

**Frank GREGORY**

Professor of European Security and Jean Monnet Chair in European  
Political Integration, School of Social Sciences, University of  
Southampton

**WORKING PAPER SERIES ON EU INTERNAL SECURITY  
GOVERNANCE**

***WORKING PAPER N° 3***

**THE SECURINT COLLECTION**

## Contents

1. Introduction
2. EU major event security policies
3. The football policing network<sup>1</sup>
4. Information/ Research Sharing networks relating to public order, terrorism and extremism<sup>2</sup>
5. The European Security Research Programme (ESRP): Commission as an 'autonomous actor'
6. The developing ESRP
7. The wider implications of Internal Security research/procurement and the links to defence equipment cooperation
8. Industrial pressures
9. Conclusions

## Abbreviations

**CEPS** – Centre for European Policy Studies

**ERA** – European Research Area

**ESRAB** European Security Research Advisory Board

**ESRP** – European Security Research Programme

**GoP** – Group of Personalities

**NFIP** – National Football Intelligence Points

**UNICRI** – United Nations Interregional Crime and Justice Research Institute

**PWGT** – Police Working Group on Terrorism

**CTELO** - Counter-Terrorism and Extremism Liaison Officers

---

<sup>1</sup> This section draws on a fieldwork interview with the UK Football Policing Unit, 12/10/06

<sup>2</sup> This section draws on fieldwork interviews with the UK National Public Order Intelligence Unit (31/10/06), the UK Police International Counter- Terrorism Unit (15/12/06) and a UK Counter-Terrorism & Extremism Liaison Officer (10/11/06)

## Summary

The European Security Research Programme (ESRP) takes the Europeanization of security into the new area of internal security scientific and technical cooperation. This raises important issues in the respect of public procurement that have parallels in the area of EU initiatives in defence procurement cooperation. A policy network analysis investigates research sharing in this new area for police major event security issue networks. The variable network structures are found to be a factor in determining their responses. This is especially so because police services, in general, have only recently needed to address policy issues related to new technologies and scientific advances. Consequently the expertise in police or internal security science and technology is more narrowly based in police services than in the military and rarely reflected, at present, in the main EU police cooperation networks. Three particular challenges need to be tackled, firstly, too many Commission initiatives and ESRP projects have networking aims and these need to be rationalized, secondly, the EU police and internal security public sector agencies need to be aware of and capable of managing the growing commercial pressures and, thirdly, the EU police services need to become, in UK Ministry of Defence terms, “smart” customers to achieve value for money for the citizens of the EU.

*This Working Paper only conveys solely the view of its author.*

## 1. Introduction

Referring to the Prüm Convention, an analysis of EU security information flows by CEPS (T. Balzacq, D. Bigo, S. Carrera & E. Guild, 2006, p.14) argues: “[...] the conventional wisdom in the security field [is] that ‘more is better’ and that an increase in the number of databases increases security. However, insecurity is not acute because law enforcement authorities do not share enough information, but rather because they share it badly and in a multiplicity of different fora.” This paper examines the “multiplicity of different fora” issue in the context of Peterson’s discussions of policy networks (2004, p.120) and his distinction between “[...] tightly integrated policy communities” and “[...] loosely affiliated issue networks [...]”. The paper follows the general methodology, as outlined in Peterson’s observation (2004, p.118-119) that “[...] most analyses of the EU which employ the policy network as a metaphor seek to test the basic proposition that the way in which networks are structured in any EU policy sector will determine, and thus help to explain and predict, policy outcomes.”

The first impetus for the paper comes from recent developments in the EU in the area of internal security research and technology where a combination of EU Council, Council of Ministers, Commission and industrial agenda priorities have led to the initiation of wide-ranging EU cooperation initiatives. In some respects, these initiatives are comparable to the longer established Commission pressures for defence equipment cooperation and show clearly the Commission’s “autonomous actor” capacity (Bache and George, 2006, p.266) through the use of the “actor” competences of three DGs: Research, Enterprise and Industry and Justice, Freedom and Security. These internal security initiatives are now known as the European Security Research Programme (ESRP). The initial stage in the development of ESRP was the February 2004 Commission Communication on “Preparatory Action on the enhancement of the European industrial

potential in the field of Security research” (PASR). The second stage was the March 2004 Report of the Commission initiated industry-dominated Group of Personalities (GoP) entitled “Research for a Secure Europe” which recommended the launching of an EU funded ESRP. The GoP also recommended the establishment of a European “Security Research Advisory Board”, (ESRAB). ESRAB produced a definitive report in September 2006 entitled “Meeting the Challenge”. ESRP is now fully established as a funding stream in Framework Programme 7 and the Commission has just published (September 2006) a linked initiative in its “Green Paper on detection and associated technologies in the work of law enforcement, customs and other security authorities.” So far these important attempts at EU internal security cooperation have received little general attention apart from Hayes’s pioneering monograph (2006).

The second impetus for this paper has come from the author’s participation in a ten-country EU project, known as EU-SEC, on “Coordinating National Research Programmes on Security during Major Events in Europe”, running from 2004-2008, an ERA Framework Programme 6 Project (FP6-02-ERA-1-CA-SSA – No. 011823).<sup>3</sup> This project led by Europol for the EU and UNICRI brought together country representatives from the Member States police forces and interior ministries. All of these participants were in some way connected to what, in Peterson’s terms, can be described as the issue networks linked to the EU major event security policy area, which dates from the Trevi era. The EU major event security policy spectrum covers sporting events, such as the World Cup and the Olympics, and political events such as EU Council Meetings, G8 meetings and state visits.

The EU-SEC project was based upon the assumptions that, firstly, there are or might be national research programmes on security during major events in Europe and,

---

<sup>3</sup> The author’s role in the EU-SEC Project was to research and draft the Report on the UK Team’s task, as set out in the Project specification, to carry out an “assessment of the obstacles that hinder the coordination of research programmes.”

secondly, that there would be a benefit from coordinating such research. The Project 'Abstract' referred to such coordinating activity as having a risk reduction objective. This objective was to be achieved by "[...] carrying out a networking activity among national research programmes in the field [...]". Participation in the EU-SEC project has contributed to a greater understanding of the two European police issue networks which are most closely involved in major event security: the football policing network and the public order, terrorism and extremism network.

It has also highlighted the fact that police liaison work was essentially about the exchange of either professional development related 'best practice' or more operationally related information or intelligence. Such liaison work did not, normally, encompass the new content of the more science and technology and equipment based ESRP. If these police issue networks are to cover such matters then it will raise questions about their competence in these new areas and how they will deal with the emerging industrial lobbies pressing for more spending on internal security research and procurement. Such commercial pressures have been described by Hayes (2006) as "arming big brother" and, from a US perspective, as "the security-industrial complex" (Prof. Peter Swire, Ohio State University in P. Harris, 2006).

This paper commences with an evaluation of the key features of the main EU policies on major event security and the implementation obligations expected of Member States. This is followed by a review of the football and public order policing networks. The conclusions from these two sections are then used to inform an examination of ESRP from the perspective of its potential impact upon these police issue networks. There then follows a consideration of possible transferable learning experiences from the EU defence equipment procurement cooperation initiatives and a highlighting of the new and

growing EU internal security interest groupings which are a mixture of European associations and lobbying consultancy bodies.

## **2. EU major event security policies**

The EU has a long history of regarding aspects of police cooperation and public order maintenance as a matter of common concern going back to the post-1975 TREVI system on co-operation which included a focus on football hooliganism intelligence and policing, (see Anderson et al, 1995, Crawford (ed.), 2002 and Occhipinti, 2003). Domestic or national policing responsibilities remain unchanged except in respect of obligations to co-operate, share “information” and expertise. However, the delivery of such responsibilities can be shaped by EU level policies, (Walker (ed.), 2004). In particular, in this context attention has been drawn to “[...] the Europeanization of security [...]”, (Bigo, 2000, p.68 and see also Monar, Rees and Mitsilegas, 2003).

Since the Amsterdam Treaty introduced the aim of making the EU an “area of freedom, security and justice”, there is the implication that wherever an individual is, in the EU, they should enjoy a common standard of security at a “major event”. This aim was specifically referred to by the EU Council, in May 2004, in the context of the Athens Olympics: “The EU’s objective is to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the field of police co-operation.” (EU Council, 2004)

Examples of policy development can be found in EU sources such as the Joint Action on co-operation on public order and security, ( 97/339/JHA May 1997) and the JHA Council Conclusions on security at meetings of the European Council and other public events, (10916/01JAI82 July 2001). Such policies are discussed in JHA Council expert

groups and within the Police Chiefs Task Force (PCTF) and these discussions have links to the Council General Secretariat Security Office which advises the Council of Ministers on security. The Security Office of the European Commission can also be involved 'where necessary.' (ENFOPOL 123, 2002) Working through a number of relevant EU documents helps to establish key principles and issues.

In the 'Security Handbook for the use of police authorities and services at international events such as meetings of the European Council', (ENFOPOL 123, 2002). Two public order principles are set out: (1) "The enforcement of law and order should be guided by the principles of proportionality and moderation preferring the less intrusive approach. Where possible, a deescalating *police* approach should be chosen." (2) "Dialogue and cooperation with demonstrators and activists should be actively pursued by the *police authorities*." The minimum implementing requirement is for each Member State to have a "national contact point" which is supposed to: collect, exchange and disseminate information and risk analyses.

The "Handbook for Member States Co-operation against terrorist acts at the Olympic Games and other comparable sporting events" demonstrates the dynamic nature of this EU policy area because the Handbook is seen as "an evolving instrument" which needs to be updated via future experiences and best practice. It specifically expects there to be inputs on: assessments of terrorist threats, suspect persons and threat levels, (ENFOPOL 14, 2004). A similar expectation is found in the EU Presidency note , "Proposals relating to the enhancement of measures to counter football related violence" (ENFOPOL 23, 2004) which contains suggestions as to improvements that could be made to the Football Handbook such as: improving the operational use of categories of estimated risk, better information on Member States travel restrictions rules, using the annual ad hoc report on football vandalism compiled by Belgium, the UK, The

Netherlands and Germany, mutual assessments of police effectiveness at major football events and developing a website because: “A single resource and reference centre for police working in this area could be very helpful.” The EU now seems to be moving towards simplifying major event security policy advice through the December 2006 EU Presidency Proposal for a single “Security handbook for the use of police authorities and services at international events” (ENFOPOL 190, 2006) for all events *except* football events which will remain covered by the 2006 EU football policing handbook.

In the early stages of the EU-SEC Project the Project partners became aware that there were definitional, content and outcomes issues to address. The ERA and ESRP documentation primarily seems to relate to scientific and technical research. The EU major event security documents do not refer to research rather they refer to ‘information’, ‘risk assessments’, ‘threat assessments’ and ‘best practice’. In strict ERA or ESRP terms these police issue networks might be expected to share research knowledge on, e.g., riot control equipment, CBRN detection equipment<sup>4</sup>, Closed Circuit Television (CCTV) systems, barrier technology and IT systems. This was certainly an assumption made by the initiators of the EU-SEC project with the implication that EU police issue networks would simply be able to add in this extra dimension to information sharing. However, it will be seen from the following issue network case studies that this was not the case. Moreover it will be suggested that the inherent differences between the two networks and the special characteristics of the ESRP are very relevant to any consideration of the feasibility of police cooperation task expansion to meet the demands of new EU policies.

It is necessary to recognize that, by comparison with the wider spread equipment procurement experience among the EU states’ military forces, the police services of the EU states have had a very limited contact with equipment procurement related science

---

<sup>4</sup> “CBRN detection equipment” is a commonly used term for equipment to detect chemical, biological, radiological ., or nuclear materials.

and technology research. Until about the 1980s police internal security equipment, broadly defined, was relatively “low-tech” and was evolving at a much slower pace than military science and technology. The application of IT technology to policing and the increasing sophistication of the response required in the areas of; forensics, e-crime, physical border controls and post 9/11 counter-terrorism (especially countering CBRN threats) means that now police services need much greater procurement expertise in order to both accurately define their operational requirements and to evaluate competing commercial solutions in terms of value for money. There is the additional complication for police services that their use of new technologies must be compatible with the legal framework in which they operate in terms of human rights legislation, data protection laws and rules of evidence.

### **3. The football policing network<sup>5</sup>**

This long-established, high-profile network derives its cohesion and commitment to sharing information and research from the following factors:- the popularity, national prestige and private sector investments (sponsorships etc) attached to football events; the need to ensure that a country is seen as having appropriate stadium standards and good behaviour by its football fans in order not to incur FIFA or UEFA bans; the common EU aim to prevent football hooliganism; the clear lead from the EU Council by its December 2001 Decision that all Member States must designate a single national point of contact (NFIPs) for football policing issues related to European or international games and that its expertise has a “transferability” value for other major public events through the dissemination of best practice. For example, the Italian police football intelligence officer was also involved in the security arrangements for the 2006 Winter Olympics in Turin.

---

<sup>5</sup> This section draws on a fieldwork interview with the UK Football Policing Unit, 12/10/06

This sector does not report any significant problems in sharing information or research other than the variable capabilities of the resources available for national contact points (Interview 12/10/06). For example, the UK “national point of contact”, the UK Football Policing Unit, is supported by 92 police football intelligence officers (“spotters”) located in the constituent forces of UK police system. There is one such officer for each major league football club. Some other EU states do not have such a large support network for their national point of contact. However, not surprisingly, there are particular and variable national constraints in the sharing of personal data under both data protection and human rights legislation. Additionally, information or research that might be derived in whole or in part from national intelligence sources, such as a UK JTAC Assessment (Joint Terrorism Analysis Centre) would only be shared in a suitably indirect manner and on a strictly ‘need to know’ basis.

This network has and continues, to commission academic research into areas such as football hooliganism, crowd behaviour control strategies and risk management. Moreover, countries hosting very high-profile football events make significant efforts to promote information-sharing. For example, in preparing for the 2006 World Cup, the German Federal Ministry of the Interior organised international conferences in Berlin in 2002 and 2003 (two conferences) to share experiences on major sporting and football events. Additionally, German fire department officials provided a detailed discussion of World Cup related CBRN measures, in conformity, with the Nationales Sicherheitskonzept to the professional journal ‘NBC International’ (Winfield, 2006 (a), pp.72-75).

The network is also developing the peer review process, as proposed in ENFOPOL 23 in 2004, and, in due course, the result of the peer reviews will also be disseminated. The website, mentioned in the Council’s ENFOPOL 23 document, has been constructed and

is available as the European National Football Information Point website, under password control for NFIPs and Europol, on the UK Centrex (police central training facility) website (ENFOPOL 158, 2006). This website contains not only police originated information for sharing but academic research papers as well.

This network benefits from the fact that the high political visibility of international football events linked to their relative frequency of occurrence has ensured that football policing cooperation issues are a standing agenda item for each EU Presidency based on a Report from the Police Cooperation Working Party (experts on major sporting events). The network also makes full use of the impetus that can be provided by an active “core group” of Member States that routinely facilitates activities through the close cooperation of the Presidency and adjacent near past and near future Presidency states.

However, the network has not, so far, considered event security “equipment” because provision of such items, on essentially private spaces, is more a matter for the clubs, series organizers, FIFA/UEFA requirements and the requirements of national Health and Safety legislation. Nonetheless because of its well developed close working relationships this network will consider the implications of the September 2006 Commission Green Paper, on detection technologies, because of its reference to the protection of mass events and possible EU security harmonization legislation.

#### **4. Information/ Research Sharing networks relating to public order, terrorism and extremism<sup>6</sup>**

Unlike the more bounded working environment of the EU football hooliganism intelligence network the non-football European major events public order intelligence network operates within a more diverse working environment. This can be summarized in

---

<sup>6</sup> This section draws on fieldwork interviews with the UK National Public Order Intelligence Unit (31/10/06), the UK Police International Counter- Terrorism Unit (15/12/06) and a UK Counter-Terrorism & Extremism Liaison Officer (10/11/06).

the following points: the location and frequency of events such as EU Council meetings, state and VIP visits, G8 Summits and Olympic Games are more varied than with major football events; the likely public order problems are essentially political in character and, apart from terrorist threats, grounded in the democratic right of public protest as opposed to the mindless violence of football hooligans; EU Member States have a variable experience with the diverse “protest groups” according, in part, to national circumstances; the “protest groups” cover a broad spectrum of single-issue and multi-issue concerns, for example, EU farmers’ groups protesting against an aspect of the Common Agricultural Policy (CAP) reform, animal rights groups, environmental protection action groups, anti-capitalist groups and right or left wing political extremist groups. The only common theme, from a public order policing perspective, is that of ‘extremism’ which implies a willingness to use violence against persons or property. Consequently, outside the football area, the police information/research sharing networks are more diverse in character.

Unlike the football intelligence network which has clear EU institutional linkages the public order network is based upon the wider membership Police Working Group on Terrorism (PWGT) which is an inter-agency network with governmental recognition. PWGT utilizes both its own secure communications network and links into a network of national liaison officers known as CTELOs (Counter-Terrorism and Extremism Liaison Officers). For example, the UK CTELO in France is attached to UCLAT in Paris and the French CTELO to the UK is located within the new Metropolitan Police Counter Terrorist Command (SO15).

Under the TEU, as amended by the Treaty of Amsterdam action against, terrorism is defined as one of the priority areas through which a high level of security is to be achieved for EU citizen(Article 29) in view of making the EU an “area of freedom,

security and justice” (Article 2). However, when the CTELO network is tracked back to ‘national contact points’ in the EU Member States, it is evident that the terrorism aspects are handled in a separate manner from other public order issues, (Gregory, 2003). For example, in the UK the National Coordinator for Domestic Extremism (NDCE) oversees the work of the National Public Order Intelligence Unit (NPOIU) but the NPOIU only feeds into the CTELO network on non-football and other major event security issues on issues related to extremists and extremist groups. Police information and intelligence related to terrorism flows from the UK to the European partners through the non-EU PWGT via the International Section of the Metropolitan Police Counter-Terrorism Command (SO15) and the Police International Counter-Terrorism Unit (PICTU). Even where the information flows on terrorism are exclusively to EU Member States such flows still go overwhelmingly by PWGT.

Well before 9/11 and even before the activation of Europol’s counter-terrorism mandate in 1999 there were occasional attempts at the Europeanization of counter-terrorism information flows. For example in 1996 a JHA Joint Action had required the creation and maintenance of a ‘Directory of Specialised Counter-terrorist Competencies, Skills and Expertise in the Member States’. However, that Joint Action has not really been fully and continuously implemented owing to the variability of responses from Member States.

Within this diverse and partly non-EU based issue network, the information flows do not usually contain the kind of data that is envisaged to be encompassed by the ESRP. Such exchanges do occasionally take place but either in an ad hoc manner or via inter-state structures such as the trilateral research links between the UK, The Netherlands and Germany on information exchange on surveillance technology and blast mitigation with the possibility of sharing of research tasks (UK PSTS, 2004) or via protective security

networks of security and intelligence agency officials such as those found in the UK's National Security Advisory Centre (NSAC) (Gregory, 2005). In fact the only long-established, publicly visible and, indeed, non-EU European issue network in the broad area of police-work sciences is the European Network of Forensic Science Institutes (ENFSI).

## **5. The European Security Research Programme (ESRP): Commission as an 'autonomous actor'**

This 2003 initiative used Commission powers, under Article 157 (2) EC, to prompt Member States to address the need for coordinated action on EU industrial competitiveness issues in the security area. Under these powers the Commission may "take any useful initiative to promote such coordination." (HC 42-xii, 2004, Paras 4-5)

There are three important aspects to this Commission initiative. Firstly, the Commission used, initially, a politically low-visibility policy development route by setting up a "Group of Personalities" (GoP) in October 2003 to draft proposals, (See Hayes, 2006, p.13f). Secondly, the GoP contained a significant industrial representation from *EADS, BAE Systems, Thales, Finmeccanica, Indra, Siemens and Diehl*. Moreover, although the Commissioners for DG Research and DG Information Society were members of the GoP, JHA Commissioner Vitorino was not a member of the GoP. Thirdly, as the UK House of Commons noted, the Commission was using powers under Treaty Title VI (Industry) which are distinct from Title XVIII (Research and Technological Development) powers which are the foundations for the EU's Framework Programme for research and technological development.

Consequently, at least in the UK, when the Commission published its "Communication on the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of security research, towards a programme to

advance European Security through Research and Technology” (COM(04) 72, 2004) some concerns were raised. The UK House of Commons European Scrutiny Committee noted that the Communication contained no definition of “security research”, queried the Treaty powers used and noted that there appeared to be no connection in the Preparatory Action proposed with the agreed JHA priorities. Furthermore, the Committee agreed with the FCO Minister’s view that the Commission should “[...] limit its work to civilian security research [as] defence- related security issues are within the competence of Member States” (HC52-xii, 2004,Para 5.19.) In a later Report the Commons’ European Scrutiny Committee referred to its concerns about whether the ESRP complied with the requirements of subsidiarity and proportionality. However, a Minister stated that the Government felt that the Commission was aware of these issues and that “[...] it would be possible to negotiate a satisfactory agreement on the security theme” (HC 34-v, 2005, Para 18.12.) The UK position was supported by France and Germany, and a Home Office chaired cross-Whitehall working group took some proposals to the Commission which formed part of the process of resolving the issues of concern, (HL182, 2006, App. D.)

The resolution of Member State concerns covered the following matters. Firstly, Commissioner Verheugen, in March 2006, stated that the ESRP “[...]has a very clear and exclusive focus on civil research [...]”, (Ibid.) Secondly, on research projects involving dual-use technology the Commission has “[...] introduced bilateral institutional links, notably with the European Defence Agency (EDA), to ensure that the current and future research projects are transparent, complementary and non-duplicative” (HL182, 2006, Para 66.) Thirdly, Member States are seeking to ensure that the EU governance method for the space and security elements of FP7 allow for greater Member State control than the Qualified Majority Voting procedures applicable to the rest of FP7, (HL182, 2006,

Para 66-68.) The Member States finally reached political agreement on FP7 in July 2006, (EU Council, Presse 215, July 2006).

There are two main challenges, arising from the ESRP initiative, facing the EU public sector internal security agencies, such as the police major event security issue networks, discussed earlier. Firstly, there is the need to identify the preliminary national stages that are necessary so that these networks can be enabled to access and share the relevant science and technology based data. From the research carried out for the EU-SEC project it seems probable that these established police issue networks are unlikely themselves to be the actual channel of communication for ESRP related data but they may be the route of access to other sources or more specialized national bodies, where those similar to the UK's Home Office Scientific Development Branch (HOSOB) actually exist as discrete entities (HOSDB, 2005). Secondly and drawing on the long and often bitter experiences in the European defence procurement cooperation area (Hood, 2004) is the challenge for public sector internal security agencies, like the police, to become, in UK MoD procurement strategy terms, *SMART customers* who can “[...] make the right decisions in acquiring [...] complex and advanced systems” (Jordan, 2003, p.133.) In amplification, this approach means, as described in UK defence procurement, developing acquisitions expertise that provides “[...] a better approach to managing our key suppliers, and whether they truly have the resources and competences to undertake projects in the timescale and at the cost they are claiming” (Walmsley, 2003, p.27).

## **6. The developing ESRP**

The first stage in the development of ESRP came in February 2004 with the Commission Communication on “Preparatory Action on the enhancement of the European industrial potential in the field of Security research (PASR)”, (COM (2004)72, 2004). At the launch in March 2004 Jacques Bus, Head of Unit at DG Information

Society for Security Research, said “The focus today is on building a community that will take us into the full-scale Security Research programme of the future” (European Commission, May 2004). The Commission proposed allocating 65m euros over the period 2004-06 to this aim with the future goal of developing a full Security research programme under FP7. Under these proposals certain activities have particular relevance for this article as they envisage the creation of yet more issue networks. For example, a summary presentation on PASR was produced in January 2006 and it included among “Supporting Activity Priorities” a facilitation proposal, (von Bose, 2006). The proposed mechanism is a “Coordination network between security technology stakeholders including research activities supported on national and/or regional level.” This can be linked to the potential contribution of the European Security: High Level Study on threats, Responses and Relevant Technologies (ESSTRT), one of the 12 proposals (out of 170+ bids) funded under PASR 2004. ESSTRT, is a general roadmap for security research which “[...] aims at benchmarking existing activities, analysing gaps and proposing solutions on the basis of detailed research, including proposals for EU co-operation” (MEM0/05/38, 2005). The ESSTRT Final Report of March 2006 contains the following proposed actions necessary to support the project’s “Principal Policy Recommendations” namely that Member States should ‘Devote more resources to *intelligence* capabilities and to *sharing* intelligence with key partners.’ (Supporting policy action 1), p.6), (ESSTRT, 2006, pp.6-9).

The second stage in the development of ESRP was the March 2004 Report of the GoP entitled “Research for a Secure Europe” which recommended the launching of an EU funded ESRP, (European Commission, March 2004). The GoP Report referred to the need for funding to boost EU internal security capability, closing the gap between civil and defence research and a need to focus on interoperability and connectivity as “key

elements". It also recommended the establishment of the European 'Security Research Advisory Board' (ESRAB) to draw up strategic guidelines to prepare the research agenda of an ESRP and to advise on the principles and mechanisms of ESRP implementation. ESRAB was established in February 2005 with a membership drawn from more appropriate public and private sectors than the GoP. For example, the UK was represented by officials from the Home Office and Department of Trade and Industry as well representatives from BAE Systems and THALES; Germany had representation from the Bundeskriminalamt and Fraunhofer- Gesellschaft and Italy was represented by the Centro Studi e Ricerca Intelligence e Security and Finmeccanica, (HL182,2005, Annex B.) The importance of ESRAB is that it provides an embryonic form of institutional structure in the internal security research field that could, potentially, begin to serve similar collective aims as the EDA in the defence field.

ESRAB produced a definitive report in September 2006 entitled "Meeting the Challenge", (European Commission, PASR Call, 2006). The Report contains an important general caveat for the Europeanization of security process, namely, that "Research is not an end in itself. [...] for technology to be effective it must be supported and synchronised with the requisite standards, legislation and societal acceptance" (European Commission, PASR Call, 2006, p.32). In terms of the development of an EU internal security research institutional structure ESRAB made some significant suggestions which, again, involve the issue network creation. ESRAB recommended the establishment, from 2007, of a broadly mandated European Security Board (ESB) with a network of national "points of contact" with both supported by a steering group to ensure coherence and an "executive secretariat" funded by the EU, (ESRAB Report, p.62). Discussions on the establishment of an ESB were still continuing, as of December 2006.

It was established from EU-SEC research that it is actually difficult to identify comprehensive national major event security research programmes because of the diverse character and variable frequency of these events and this means that there are very variable national and trans-national internal security research sharing networks.<sup>7</sup> The UK was rather unusual in having the wide-ranging “Police Science and Technology Strategy 2004-2005” [PSTS 04-09] which is described as “[...] a key vehicle for the delivery of the Government’s priorities presented in the National Policing Plan [NPP] [...]”. Another significant feature of the UK situation is the existence of the Home Office Scientific Development Branch (HOSDB) which described itself as “[...] probably unique; we know of no other organisation in the world that conducts such a wide range of work in ‘policing’ technology [...]” and HOSDB (2005, p.1) says it works “[...] closely with selected law enforcement organisations across the world to share the risks, costs and benefits of complex technologies.” HOSDB employs over 200 scientists and engineers and is currently running 23 technical programmes and over 150 projects. Thus whereas the UK participants in the two police issue networks, discussed in this analysis, could be enabled to assist in ESRP policy related research information flows through reference to PSTS and HOSDB, the EU-SEC research suggested that this type of enablement might be more problematic for other Member States.

## **7. The wider implications of Internal Security research/procurement and the links to defence equipment cooperation**

Although the history of collaborative defence procurement is littered with failed projects and accounts of the complexities of the specification agreement, financial arrangements and project management structures it has recorded some successes and the

---

<sup>7</sup> Fieldwork interview with HOSDB official 28/11/06

EU states are now seriously attempting to address the core problems (Hood, 2004). However, the comments made by Hayward in the late 1980s that: “European technological collaboration is unquestionably a highly political activity. This is inevitable in a field where key technologies are so closely linked to military and economic security and where at the same time important national interests of states must be accommodated [...]”, (Hayward, 1987, p.11) are still valid today. In October 2006 the Airbus’ industrial group, EADS, was warned by Lord Drayson, the UK Minister for Defence Procurement, that “As a key customer, we see it as important for EADS to move in a direction that is free from political interference” (The Times 5/10/06).

The commonly found problems within multinational defence procurement were: difficulties in agreeing the Operational Requirement (OR) despite facing a common threat; pressures from national defence industries to secure particular national commercial advantages; cost control problems resulting from attempts to meet sometimes competing preferences within the particular OR; project vulnerability to subsequent national political decisions that might either reduce the number of partner-countries or the scale of the production-run and insistence by partner-countries on a fair return on investment (*‘juste retour’*) on *each* project.

The European Commission has been trying to persuade Member States to address these problems for some time. Its latest attempt was represented by the 2004 Green Paper on Defence Procurement, (COM (2004)608). In that Green Paper the European Commission highlighted some general issues that have a transferability relevance to the European internal security area. The Commission raised concerns about: the reduced size of national markets for defence industry products leading to problems of off-setting high R&D costs because of reduced economies of scale options; fragmentation of R& D spending in Europe increases national costs and that these factors damage the

competitiveness of the European defence industry and its “[...] ability to meet the requirements of the ESDP’ (Ibid.).

In one respect European defence procurement has, at the present, an advantage over the embryonic attempts to promote European internal security equipment procurement collaboration through its longer established organisational structures. Since 1996 the Joint Organisation for Armaments Cooperation (OCCAR – given legal personality in 2000), open to all EU states (but currently only comprising the “big five” defence industry states; Germany, Belgium, France, Italy & UK) has been trying to replace “[...] the system of *juste retour* per programme by an “overall *juste retour*” covering several years and several programme[...]”(Ibid.).

More recently, in 2004, the EU set up the European Defence Agency (EDA) (Joint Action 2004/551/CFSP, 2004 and see Trybus, 2006)) to help Member States meet their capabilities goals under the ESDP. Among the ways EDA seeks to achieve its goals there is one which might be seen as comparable to the needs of the internal security area that is “Helping them [Member States] to identify common needs and promoting collaboration through common solutions” (EDA). The EDA is, in EU institutional terms, an Agency of the EU operating under the Authority of the Council of Ministers with the EU’s Secretary-General of the Council and High Representative for CFSP, Javier Solana, as its Head of Agency and Chair of the Steering Board of Defence Ministers. If a comparable structure was considered appropriate for the internal security/JHA area, such as the proposed European Security Board (ESB), then the EDA could serve as a model. In that case the comparable agency head might be Gijs de Vries because of his role as EU Counter Terrorism coordinator with the Steering Board being composed of the JHA Ministers.

British official comment on the establishment of the EDA draws attention to a number of cautionary points relating to Member State concerns that might well arise in the internal security area. The then UK Defence Secretary, Geoffrey Hoon, told the Commons “The EDA is designed in such a way that will not turn into a supranational body that dictates procurement decisions. [...] it cannot force the UK to compromise kit for our armed forces or to accept a “fortress Europe” (i.e. anti-American) defence industrial policy” (UK House of Commons European Standing Committee B June 2004, see also Symons, 2000, p.17). However, Mr. Hoon did emphasise that he felt that the EDA would “[...] improve the essential link between the job of defining capability and the concrete delivery of those capabilities.” Additionally he stressed, in supporting the creation of a new agency, that ‘Only a permanent staff dedicated to improving European defence capabilities and spreading best practice can take all the components of capability improvements to the next level’ (Commons European Standing Committee B June 2004).

It might be beneficial if a mutually reinforcing relationship can be developed between the emerging ESRP and the longer established EDA so that there can be enhanced opportunities for collaborative research and procurement at the interface between defence requirements and internal security research requirements. This is because there is already a potentially relevant new “Contract Notice- Request to Participate” from the EDA, dated September 26<sup>th</sup> 2006, that has possible internal security utility against CBRN terrorism. This EDA initiative reflects the identified need for “[...] the definition of an Integrated Biological Defence System Architecture [...]” and it is hoped that the contracted study will be able to “[...] propose a generic biological defence system architecture with the view of using this as a reference for future EU capability developments” (EDA, File Ref. 06-CAP-047, 26/9/06).

In general terms, an EU state seeking to procure a new item of security equipment (broadly defined to cover, for example, lethal and non-lethal weapons, IT, dogs, vehicles, CCTV technology, specialised vehicles, detection devices, communications equipment and barrier technology) has the following choices: off the shelf purchase from a national or external commercial source (COTS); procurement from an “in-house” facility such as a national ordnance factory; ‘in-house’ R&D followed by commercial supplier production; ‘in-house’ R&D followed by in-house production in situations where there is no private sector option or where small production runs and/or high technical risk make a commercial partnership unlikely and consideration of the desirability of a bilateral or multilateral project.

Unlike defence procurement internal security equipment procurement, in the pre 9/11, era was mostly relatively “low tech” and largely purchased to meet purely national needs. However, post 9/11, the internal security threat range has increased both in scale and consequence and hence greater technical sophistication is being required from counter-measures. Moreover, within the EU there is an aspiration, based upon the concept of “an area of freedom, security and justice” for Member States to offer greater equivalence in security protection measures. This is particularly evident in the Commission 2006’ Green Paper on detection and associated technologies in the work of law enforcement, customs and other security authorities’ (COM (2006) 474).

There are two developments in EDA practice that may have a form of transferability into the ESRP area with regard to more cooperative research sharing and possibly common procurement. Firstly, EDA Member States have agreed a voluntary Code of Conduct on Defence Procurement under which a participating Member State will, under certain conditions, “[...] open up to suppliers in each others’ territories all defence procurement opportunities of €1 million or more[...]”, (HL 125, p.9.) Secondly, EDA is

tasked with “[...] developing a single portal for announcement of all new contracting opportunities [...]” (Ibid.).

## **8. Industrial pressures**

One point that is strongly made in the more civil-liberties based approaches to this topic is the need to be aware of commercial pressures from the growing, post 9/11, homeland/internal security industry (Hayes, 2006). It has been estimated, by the US market research company Frost & Sullivan that by 2014 the European homeland security market (biometrics, screening, RFID, UAVs and CCTV) will have a value of nearly 874m euros (prnewsire.co.uk, 2006).

However, there is a potential obstacle to free-flowing research sharing and procurement collaboration in the division of national industrial strategic approaches between countries, such as France, which are stressing national industrial protection and the UK, which favours much more open EU-transatlantic security industrial co-operation. The French position, as stated in 2005, was that 11 sectors of its economy were of strategic importance and should be protected from foreign take-overs. Among these sectors the French government listed:- research into anti-terror measures including defence against chemical attack, bugging and surveillance equipment, dual-use technology with civilian and military applications and companies providing IT security services to a public operator(The Times, 9/10/06). Needless to say the EU Commission is challenging the French protectionist position.

In order to provide some comparative data on commercial pressures, this section will commence with an overview of the situation in the US. Paul Harris in ‘The Observer’ commented that “Five years after the World Trade Centre fell, a highly lucrative industry has been borne in America – homeland security. There has been a

goldrush as companies scoop up government contracts and peddle products they say are designed to make America safe” (The Observer, 10/9/06). The growth in companies offering homeland security products or lobbying for the sector in the US, based upon the Harris’ article, is set out below.

Year	Number of US companies offering Homeland Security products.	Registered Homeland Security Lobbying Firms.
1999	9	
2001		2
2003	3,512	
2005		543
2006	33,890	

Since 2000 the US Government has gives out homeland security contracts worth \$130bn [£70bn] and by 2015 it is estimated that federal homeland security spending in industry could reach \$170bn.

Whilst the EU area does not register this level of growth in homeland/internal security spend and its linked commercial pressures they do, nevertheless, exist and have been a formative factor in the creation of the ESRP (Hayes, 2006, pp.9-10). The ‘umbrella’ Brussels lobbying organisation for this area is the Aerospace and Defence Industrial Association of Europe (ASD). Moreover, the first Report of the EU Advisory Group on Aerospace ‘Strategic Aerospace Review for the 21<sup>st</sup> Century’ saw the ‘ultimate goal’ as the establishment of a ‘European armaments policy to provide structure for European defence and security equipment market [...]’, (Ibid.). Among other European lobbying groups there is a non-profit organisation, the European Homeland Security Association (EHSA), formed in 2004, which focuses on civil defence and protection. Interestingly though, EHSA has among its partner institutions not only those that might be expected such as GCSP in Geneva, INHES in Paris and SIPRI in Stockholm but also CSIS in Washington DC and IDSS in Singapore. Moreover EHSA’s sponsors include Thales and EADS.

Additionally, there are clear pressures from some security product ‘end-users’ for increased EU and Member States public funding of post 9/11 security requirements for the private sector. For example, the European air transport industry has noted that “[...] from 2001 to 2003 the US government paid over US \$ 3 billion to compensate their national aviation industry for the cost of anti-terrorist measures. European governments, on the other hand, have so far refused to bear the costs for such measures, which aim at the protection of society in genera” (EATI, Policy Paper, 2003).

A potentially complicating factor, for EU collaboration in this field, is that of the variable relationships between the EU Member States and the US, which has already been referred to in relation to the UK’s determination not to allow a security industrial policy to emerge by which a “fortress Europe” approach might make industrial links with the US problematic. The UK Government’s ‘Trade & Investment’ website advertised for corporate participation in a “UK Technologies for Security Mission to the USA” from 30 October to 3 November 2005 in Boston and Washington DC. This UK initiative made specific reference to the relevance of various US DHS – Home Office cooperation arrangements and thus highlighted the fact that UK-US cooperation in homeland security was well established and furnished with appropriate supporting structures. By contrast, France’s more European orientation is well expressed by Dr. Pascal Stephan of the French DGA who is quoted (Winfield, 2006 (b), p.16) as saying, with reference to the ESRAB IMPACT project (Innovative Measures for Protection Against CBRN Terrorism), that “What we [France] would like to get from Impact is the ability to promote contractors in Europe developing technology.”

## 9. Conclusions

This paper concludes that, notwithstanding the ESRP initiative, there is no clear need for more police information/research exchange issue networks. There is already a problem of network multiplication and overlap within the evolving ESRP frameworks. There may, however, be scope for some form of network rationalization or inter-connection especially as there is no discrete 'major event security' network as such. The established networks in football and public order do not report any major obstacles to information sharing in their fields of competence other than those expected under ECHR, Data Protection laws and national security constraints. However, they have not, to date, contemplated the issue of security equipment, broadly defined, research sharing.

It would appear therefore that the ESRP may need to engage more closely with the issue of coordinating/sharing networks related to the Member State level of research programmes on internal security. Firstly, as already noted these may simply not exist as discrete entities but rather only exist as dispersed activities across a range of both public and private sector bodies. Secondly, the typical police official involved in the current information/research sharing networks is unlikely to be in close contact with the development and formulation of the more scientific and technical areas of event security. Thirdly, because the counter-terrorism response now tends to dominate general and event security concerns regarding new technologies it is very likely that the national fora within which such research is developed will operate in very restrictive security classification mode. Therefore any consequent trans-national research sharing which does occur is likely to be restricted to those countries with which a state has particularly privileged bilateral relations or within some privileged multi-lateral framework like the EU G6 group.

The most recent example of this was in the Conclusions of the October EU G6 Meeting which “agreed to take the following specific actions to combat the [terrorist] threat: share ongoing research into explosives, in particular on liquid explosives and giving support for more EU funding and support work on traceability of explosives and an early warning system on diverted explosives” (G6 Conclusions, October 2006). These G6 countries’ action points have subsequently been offered some project funding support by DG Justice, Freedom and Security.

However, this does not mean that national police information/research sharing contact points would be unable to share anything of significance regarding security equipment, broadly defined through EU police cooperation networks. They could be enabled to construct responses in the following areas: identifying, for a detailed response, those parts of police agencies which are more closely involved; drawing attention to national public or private sector open sources on new equipment purchases or equipment “bench-marking”; drawing attention to relevant open source publications in national scientific and technical journals or similar sources. A common feature, though, of all of the above is that they would require some form of EU or national resource input to the police contact point so that the contact point could be briefed or know where to go for further advice.

## **Bibliography**

### **References – EU documents**

Joint Action on ‘Co-operation on public order and security’, 97/339/JHA, May 1997/96/610/JHA.

“Security Handbook for the use of police authorities and services at international events such as meetings of the European Council”, ENFOPOL 123, Council of the EU [12637/3/02], Brussels 12/11/02, REV 3 LIMITE, 2002.

“Handbook for Member States Co-operation against terrorist acts at the Olympic Games and other comparable sporting events”, ENFOPOL 14, Council of the EU [5744/1/04], REV 1 LIMITE, 2004.

“Proposals relating to the enhancement of measures to combat football related violence”, ENFOPOL 23, 2004.

EU Council, Police Cooperation Working Party (experts on major sporting events), “Outcome of Proceedings”, 22/9/06, 13118/06, ENFOPOL 158, Brussels, 3/10/06.

Presidency of the EU Council to the Police Cooperation Working Party, “Proposal for Security handbook for the use of police authorities and services at international events”, EU Council doc. 15226/1/06 REV 1, ENFOPOL 190, 22/11/06.

Commission Communication “Preparatory Action on the enhancement of the European industrial potential in the field of Security research”, COM (2004) 72 final, Brussels, 3/2/04.

European Commission (Research), “European industry leaders and EU policymakers call for budget boost for Security Research”,

<http://www.ec.europa.eu/research/press/2004/pr1503en.cfm>, accessed 2/10/06.

European Commission, “EU Security Research initiative grabs aeronautics sector’s attention”, 7/5/04,

[http://www.ec.europa.eu/research/aeronautics/info/news/article\\_950\\_en.html](http://www.ec.europa.eu/research/aeronautics/info/news/article_950_en.html), accessed 11/10/06.

European Commission, “EU Security Research initiative grabs aeronautics sector’s attention”, 7/5/04,

[http://www.ec.europa.eu/research/aeronautics/info/news/article\\_950\\_en.html](http://www.ec.europa.eu/research/aeronautics/info/news/article_950_en.html), accessed 11/10/06.

EU Press Releases, “Terrorist Attacks and Tsunami: EU Research to prepare for the unexpected”, MEMO/05/38, 7/2/05.

H. von Bose, DG ENTR-H4, “Preparatory Action for Security Research”, 17/1/06.

PASR 2006 Call, “ESRAB Report”, [‘Meeting the Challenge’]

[http://www.ec.europa.eu/enterprise/security/articles/article\\_06\\_09\\_25\\_tc\\_en.htm](http://www.ec.europa.eu/enterprise/security/articles/article_06_09_25_tc_en.htm),

accessed 6/10/06.

EU Council, Police Cooperation Working Party (experts on major sporting events),

“Outcome of Proceedings”, 22/9/06, 13118/06, ENFOPOL 158, Brussels, 3/10/06.

EU Commission, “Green Paper on detection and associated technologies in the work of

law enforcement, customs and other security authorities”, COM (2006) 474 final,

Brussels, 1/9/06.

EU Commission, “GREEN PAPER- Defence Procurement”, Brussels, 23.09.2004, COM

(2004) 608 final.

Joint Action 2004/551/CFSP to set up a European Defence Agency (EDA) adopted by

the Council on 12 July 2004, OJ L 245/17, 17/7/04.

EDA, “Why the European Defence Agency?”, <http://eda.europa.eu/>, accessed 3/10/06.

EDA, “Contract Notice – Request to Participate”, “Development of an Integrated

Biological Defence System Architecture (IBDSA)”, File Ref. 06-CAP-047, 26/9/06.

ESSTRT Deliverable D6-1, “New European Approaches to Counter Terrorism”, 21/3/06,

p.6 & 9.

Meeting of the interior ministers of France, Germany, Italy, Poland, Spain and the United Kingdom, “Conclusion”, Stratford-upon-Avon, 25 and 26 October 2006, <http://www.press.homeoffice.gov.uk/press-releases/g6-meeting-conclusions>, accessed 13/12/06.

### **References - UK Parliamentary Papers**

House of Commons, European Scrutiny Committee, 12<sup>th</sup> Report of Session 2003-04, HC 42-xii.

House of Commons, European Scrutiny Committee, 5<sup>th</sup> Report of Session 2005 -06, HC 34-v.

House of Commons, European Standing Committee B, “Establishing a European Defence Agency”, European Standing Committee B Debates, Session 2003-04, 22//6/04.

House of Lords, European Union Committee, 33<sup>rd</sup> Report of Session 2005-06, “Seventh Framework Programme for Research”, HL 182, June 2006.

### **References - Books & Articles**

Anderson, M., den Boer, M., Cullen, P., Gilmore, W., Raab, C. & Walker, N., (1995) *Policing in the European Union*, Oxford, Clarendon Press.

Bache, I. and George, S., (2006) *Politics in the European Union*, (2<sup>nd</sup>. Ed.), Oxford, OUP.

Balzacq, T., Bigo, D., Carrera, S. & Guild, E. (2006) “Security and the Two- Level Game: The Treaty of Prüm, the EU and the Management of Threats”, CEPS Working Doc. No. 234.

Bigo, D., (2000) “Liaison officers in Europe: new officers in the European security field” in Sheptycki, J. (ed.), *Issues in Transnational Policing*, London, Routledge.

Crawford, A. (ed.), (2002) *Crime and Insecurity: the Governance of Safety in Europe*, UK, Willan.

Gregory, F., (2003) 'The EU's role in the war on terror', *Jane's Intelligence Review*, Vol. 15 (01), pp.14-17.

Gregory, F., (2005) Intelligence-led Counter-terrorism: a brief analysis of the UK domestic intelligence system's response to 9/11 and the implications of the London bombings of July 7<sup>th</sup> 2005', ARI Paper 94/2005, Real Instituto Elcano de Estudios Internacionales y Estratégicos, Madrid, [<http://realinstitutoelcano.org/analisis/781.asp>].

Hayes, B. *Arming Big Brother- The EU's Security Research Programme*, Transnational Institute & Statewatch, Amsterdam , April 2006.

Hayward, K., (1987/8) “Airbus: twenty years of European collaboration”, *International Affairs*, 64(1).

Hebenton, B. & Thomas, T. (1995) *Policing Europe: Co-operation, Conflict and Control*, Basingstoke, Macmillans.

Hood, F., (2004) ‘European Defence Procurement; The Future?’, Report on Wilton Park Conference WP734, 2-4 Feb. 2004, Wilton Park/FCO.

Jordan, G., Sc. & Tech Director, UK MoD, (2003) “The Leverage of Research and Technology II”, *World Defence Systems*, Vol. 5 (1), Spring .

Occhipinti, J. (2003) *The politics of police cooperation: Towards a European FBI?*, USA Lynne Reinner.

Peterson, J., (2004) “Policy Networks”, in Wiener, A. and Diez, T. (eds.), *European Integration Theory*, Oxford, OUP.

Monar, J., Ree, W., & Mitsilegas, V., (2003) *The EU and Internal Security*, Palgrave Macmillan.

Symons, Baroness of Vernham Dean, Minister of State for Defence Procurement, “Creating a Competitive European Defence Industry – the Government View”, *RUSI Journal*, Vol. 145 (3), June 2000.

Trybus, T., (2006) “The new European Defence Agency: A contribution to a common European security and defence policy and a challenge to the Community *acquis*?”, *Common Market Law Review*, 43 (3).

Walker, N., (ed.), (2004) *Europe’s Area of Freedom, Security and Justice*, OUP.

Walmsley, R., Chief of Defence Procurement UK MoD, (2003) “Smart Acquisition; The Next Steps”, *RUSI Journal*, Vol. 148(2).

Winfield, G., (2006 (a)) “Population Explosion”, *NBC International*, Autumn.

Winfield, G., (2006 (b)), “Braced for IMPACT”, *CBRNe World*, Autumn 2006.

### **References - Other Sources**

Harris, P., ‘How US merchants of fear sparked a \$130bn bonanza’, *The Observer* 10/9/06, <http://www.observer.guardian.co.uk/world/story/0,,1868912,00.html>, accessed 16/9/06.

European Air Transport Industry Policy Paper, “Funding of Anti-Terrorist Security Measures”, 1/12/03.

prnewsire.co.uk, ‘Need for Enhanced Homeland Security to Promote Uptake of Security Technologies’, News Release, 10/1/06  
<http://www.prnewswire.co.uk/cgi/news/release?id=161547>, accessed 11/10/06.

Police Science and Technology Strategy 2004-2009, [PSTS 04-09]04

[http://www.homeoffice.gov.uk/documents/PoliceST-S2\\_part\\_11.pdf](http://www.homeoffice.gov.uk/documents/PoliceST-S2_part_11.pdf), accessed 10/10/06.

HOSDB, "HOSDB: An Introduction", HOSDB publication 10/05, 2005, p. 1..