

Policy Department C  
Citizens' Rights and Constitutional Affairs



**REVIEW OF SECURITY MEASURES IN THE 6th RESEARCH  
FRAMEWORK PROGRAMME AND THE PREPARATORY  
ACTION FOR SECURITY RESEARCH**

**CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS**





PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET  
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT  
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS  
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT  
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT  
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

**Directorate-General Internal Policies  
Policy Department C  
Citizens Rights and Constitutional Affairs**

## **REVIEW OF SECURITY MEASURES IN THE 6<sup>th</sup> RESEARCH FRAMEWORK PROGRAMME AND THE PREPARATORY ACTION FOR SECURITY RESEARCH**

### **BRIEFING NOTE**

#### Abstract:

Security research has constituted, over the past few years, a strong priority for Community policies in the field of scientific research, industry, and justice and home affairs. Community efforts in this domain have been channelled, over the period 2002-2006, through the 6<sup>th</sup> Framework programme (FP6) and the Preparatory action on security research (PASR). FP6 has sustained, within its various thematic priorities, a series of projects and programmes dealing with technological developments in the field of security. The PASR is a targeted initiative of the European Commission aiming at developing contacts and partnerships between the actors of the European security industry, the public actors, and research bodies. PASR activities, in this respect, have mainly focused on technological development and the networking of actors, in anticipation for the thematic programme on security now established under FP7. The analysis of the contents of research being conducted under the FP6 and PASR is very revealing in this respect: it highlights the fact that this research is mainly oriented towards technological development as such, and unquestioningly takes security as a norm and a fundamental value. In this regard, and despite the odd exception, European security research does not include in its scope the effects that increasingly sophisticated technologies of control and surveillance can have on individual freedom and rights, particularly with regard to privacy and the protection of personal data. It does not address the necessary limits to security. The point, then, is to envisage the modalities through which a reflection on the ethical, legal, political and social implications of security technologies can be strengthened and further integrated in European security research.

**PE 393.289**

This note was requested by The European Parliament's committee on Civil Liberties, Justice and Home Affairs.

This paper is published in the following languages: EN, FR.

Authors: **Didier Bigo and Julien Jeandesboz, Centre d'Etudes sur les Conflits, Paris**

Manuscript completed in May 2008

Copies can be obtained through:

M. Alessandro Davoli

Tel: +32 2 2832207

Fax: +32 2 2832365

E-mail: [alessandro.davoli@europarl.europa.eu](mailto:alessandro.davoli@europarl.europa.eu)

Informations on DG Ipol publications:

<http://www.ipolnet.ep.parl.union.eu/ipolnet/cms>

Brussels, European Parliament

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

## Briefing Note

### **Review of security measures in the 6<sup>th</sup> Research Framework Programme and the Preparatory Action for Security Research\***

**Didier Bigo and Julien Jeandesboz, Centre d'études sur les conflits, Paris**

European activities aiming at fostering research in the field of security have developed significantly over the past few years, in correlation with the development of the European Research Area. This development resonates with a twofold orientation; firstly, optimising the potential and competitiveness of European firms and industries in a globalised context and raising the level of investment in security research and development in the EU (in line with the objectives of the Lisbon strategy), and secondly, improving the security of the European Union (EU), its member states and citizens, via the development and implementation of new and common technological instruments. This trend in itself is not specifically European. In this regard, the increasing funding of research and development for security technologies by Community means echoes concerns about the stated fragmentation and overall weakness of European activities in this domain compared to the growing consolidation of a industrial base in the security sector in the United States. The specificity of EU activities in this area, however, stems from the efforts that have been devoted to the correlation of research and development in security technologies with a reflection on the impact of these technologies with regard the fundamental freedoms and rights of individuals. In this regard, there seems to be a degree of awareness among EU officials about the impact of security technologies on this domain of crucial importance for European values.

Both the 6<sup>th</sup> Framework Research Programme (FP6) and the Preparatory Action for Security Research (PASR), which constitute the main efforts dedicated by Community bodies to support and sustain security research and development over the period 2002-2006, have allowed for a certain degree of mixing of technological research with reflection on the ethical and legal implications of breakthroughs in security technologies. In some cases, ethical, legal and normative considerations are embedded in technology-oriented projects; in other fewer cases, such considerations have become the main objective of stand-alone projects. But, in order to frame correctly the relation between technology, security and European values of freedom and democracy, it is important to insist on the fact that enhanced security cannot be the ultimate goal of research: the actual contribution of such enhanced forms of control and surveillance to the security and safety of citizens needs to be adequately assessed, as does the potential dangers that such technologies might pose to democracy, equality and freedom. As we will see, too many projects funded under the FP6 and PASR are oriented only towards the development of new technologies of surveillance. These technologies are often assumed, without demonstration, to provide improved safety and security to the citizens and peoples living in a specific area by detecting risks and dangers. However, even when they perform this task of detection, such technologies can simultaneously increase the safety of some and the insecurity of others, as well as give rise to a feeling that freedom and social cohesion have been diminished. Very little has been done in the way of reflecting on these issues in FP6 and PASR activities, and, in this regard, there remains considerable room for improvement.

---

\* The authors would like to thank Sergio Carrera, Anaïs Faure Atger and Elspeth Guild for their inputs in the realisation of this note, as well as Estelle Durand and Richard M. Spooner for copy-editing on earlier drafts.

# 1. Background

## 1.1. General background

Research in the field of security has received EU funding from two main frameworks over the period 2002-2007: the 6<sup>th</sup> Framework Research Programme and the Preparatory Action on Security Research. Earlier Community initiatives regarding this domain had initially targeted the twofold issue of a European common defence procurement market and a European policy towards defence industries. From defence matters, however, the discussion has somewhat been displaced to matters of security and security research<sup>1</sup>.

Community efforts and proposals were initially manifested in a 1997 communication from the Commission, laying out an “Action plan for the defence-related industry”<sup>2</sup> which already envisaged that the 5<sup>th</sup> Framework Research Programme (FP5) could contribute to developing and strengthening European research and development initiatives in the area of defence: “Some of the technological areas covered (e.g. materials, Information and Communication Technologies – ICT) have a multiple use dimension: the development of these technologies can contribute to the improvement of the defence technological base and the competitiveness of this industry”<sup>3</sup>. The FP5 thus featured several projects dealing with defence-related matters, particularly in the field of aeronautics and ICT, but the Action Plan itself, including its research and development component, was largely under-exploited; in an April 2002 resolution the European Parliament “call[ed] upon the Commission to develop an updated action plan” that would in particular explore “the possibility of developing a defence equivalent of the Advisory Council for Aeronautics Research in Europe so that European research in the defence field can be better pooled and coordinated”<sup>4</sup>. The call was addressed by the European Commission in its March 2003 communication “Towards an EU Defence Equipment Policy”<sup>5</sup>, which expressed its willingness “to offer its expertise for an initiative to promote cooperation on advanced research in the field of “global security”, and announced its intention “to launch a preparatory project that it would implement with the Member States and industry to implement some specific aspects that would be particularly useful in implementing the Petersberg tasks. This preliminary operation lasting no longer than three years would constitute a pilot phase [...] for evaluating the conditions and arrangements

---

<sup>1</sup> The European Commission, through its DG Enterprise, has however recently published a “defence package” featuring the necessary elements for the setting-up of a common market for defense goods, namely a proposal for a directive on the simplification of transfers for defence-related goods and another on defence procurements. See: European Commission (2007) (COM 764 final). *A Strategy for a stronger and more competitive European defence industry*; European Commission, (2007) (COM 765 final). *Proposal for a directive of the European Parliament and of the Council on simplifying terms and conditions of transfer of defence-related products within the Community*; European Commission (2007) (COM 766 final). *Proposal for a directive of the European Parliament and of the Council on the coordination of procedures for the award of certain public work contracts, public supply contracts and public service contracts in the field of defence and security*.

<sup>2</sup> European Commission (1997) (COM 583 final). *Implementing European Union Strategy on Defence-Related Industries*.

<sup>3</sup> *Ibid*, p.19.

<sup>4</sup> European Parliament (2002) (TA 0172). *European defence-related industries: European Parliament resolution on European defence industries*.

<sup>5</sup> European Commission (2003) (COM 113 final). *European Defence – Industrial and Market Issues: Towards an EU Defence Equipment Policy*.

needed for effective cooperation between national research programmes in the field of global security. It will cover just a few carefully selected subjects of advanced technology together with specific accompanying measures”<sup>6</sup>. The proposal later concretised into the PASR.

## 1.2. FP6 and security research

The FP6 is the main Community contribution to the creation and support of the European Research Area over the period 2002-2006. It was formally initiated by Decision No 1513/2002/EC of the European Parliament and the Council<sup>7</sup>, which established the maximum amount of the overall Community contribution to 16 270 million euros. Within the FP6, security-related research is particularly considered under the following thematic priorities<sup>8</sup>:

- Information society technologies (particularly the “Towards a global dependability and security framework”);
- Aeronautics and space;
- Sustainable development, global change and ecosystems.

Research in security domains is also envisaged under the ‘Policy-oriented research’ heading, which takes into consideration projects that would focus on the study of Community policies.

## 1.3. The Preparatory action for security research

The PASR emerged alongside the FP6 as a targeted initiative dealing solely with security research, during the period 2004-2006. It was formally initiated by Commission Decision 2004/213/EC of 3 February 2004<sup>9</sup>. The decision followed from the call for action in the European Parliament resolution of 10 April 2002, as well as from the Presidency Conclusions of the March 2003 and June 2003 European Council meetings<sup>10</sup>, and the suggestion laid out by representatives from the aerospace industry in the so-called “Star 21” report<sup>11</sup>. The launching of the PASR was accompanied by the tabling of several documents:

- A communication from the European Commission accompanying the Commission decision establishing the PASR, and laying down indications on its implementation<sup>12</sup>.

---

<sup>6</sup> *Ibid*, p.16-17.

<sup>7</sup> *Decision No 1513/2002/EC of the European Parliament and of the Council of 27 June 2002 concerning the sixth framework programme of the European Community for research, technological development and demonstration activities, contributing to the creation of the European Research Area and to innovation (2002 to 2006.*

<sup>8</sup> See Annex I of Decision No 1513/2002/EC.

<sup>9</sup> European Commission (2004) (2004/213/EC). *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.*

<sup>10</sup> Council of the European Union (2003) (8410/03). *Brussels European Council 20 and 21 March 2003: Presidency conclusions*; Council of the European Union (2003) (11638/03). *Thessaloniki European Council 19 and 20 June 2003: Presidency conclusions.*

<sup>11</sup> European Advisory Group on Aerospace (2002). *STAR 21 – Strategic Aerospace Review for the 21<sup>st</sup> century: creating a coherent market and policy framework for a vital European industry.*

<sup>12</sup> European Commission (2004) (COM 72 final). *Commission communication on the implementation of the Preparatory Action on the enhancement of the European potential in the field of Security research: towards a programme to advance European security through Research and Technology.*

- The March 2004 report of the Group of Personalities in the field of Security Research, convened in October 2003 at the initiative of Commissioners Busquin (Research) and Liikanen (Enterprise and Information Society)<sup>13</sup>.
- A second communication from the European Commission, tabled in September 2004, which draws from the conclusions of the Group of Personalities in the field of Security Research and lays out a road map for the development, from 2007 onwards, of a European Security Research Programme (ESRP)<sup>14</sup>

The PASR, as highlighted in the communication accompanying the decision from the Commission, “is designed to assess the need for a further initiative that will complement and liaise with existing and future intergovernmental schemes” (the abovementioned ESRP) as well as “contribute to bridging the current gap between generic civil research (as supported by EC Framework programmes) and national and intergovernmental programmes oriented to defence procurement needs”<sup>15</sup>. The PASR was designed to fund a small number of focused projects which could be completed in the timeframe of the Action Plan, as well as initiatives designed to address the market conditions in the field of security, including for the purpose of networking actors from the private sector, the public sector, and research organisations.

## **2. Contents and analysis of security research conducted under the FP6 and PASR**

Security research conducted under the FP6 and PASR highlight an evolving landscape of security practices and uses of technology for security purposes. Over 170 projects (out of a total of 10 180) funded under the FP6 participate directly or indirectly from the priorities and perspectives of security research. Furthermore, 39 activities, including 9 support activities, have been funded under the PASR scheme. It would clearly be unpractical to survey all projects and activities in detail: in this respect, the note will focus on key initiatives, particularly among the bigger, Integrated Programmes (IP) and Networks of Excellence (NoE) funded under the FP6 and some of the PASR activities that highlight most strikingly the orientations and perspectives of contemporary EU-supported security research. It will also, when necessary, provide a view of some of the smaller-scale projects, in particular FP6 Specifically Targeted Research Projects (STREP). These initiatives are distributed by key domains of research:

- Biometrics and identification (2.1.)
- Detection and surveillance (2.2.)
- Exchange of information, risk analysis and risk anticipation (2.3.)
- Critical infrastructure protection, crisis management and public safety (2.4.)
- Freedom and privacy (2.5.)

The last section (2.6) will then provide an overview of the apparent priorities and orientations of EU funded security research. It

### **2.1. Biometrics and identification**

---

<sup>13</sup> Group of Personalities in the field of Security Research (2004). *Research for a Secure Europe*.

<sup>14</sup> European Commission (2004) (COM 590 final). *Security Research: the Next Steps*.

<sup>15</sup> *Commission communication on the implementation of the Preparatory Action on the enhancement of the European potential in the field of Security research: towards a programme to advance European security through Research and Technology*, op.cit., p.5.



- **FP6<sup>16</sup> IP:** Two FP6 Integrated Programmes focus on biometrics. The 3DFACE and BIOSEC programmes deal with the technological development of biometric identifiers: the first with a specific focus on three-dimensional identification of facial features, the second with an emphasis on multi-modal biometric identifiers (iris, fingerprint and voice identification). Privacy considerations, in particular users' ownership of biometric identifiers, are included in both.
- **PASR<sup>17</sup> activities:** Project BIOTESTING EUROPE also focuses on biometrics, but with the aim of establishing a European network for the testing and certification of biometric components.
- **Other projects:** FP6 activities in this domain are further flanked by two NoE – BIOSECURE and FIDIS – and three notable STREPs – BIO-RESIDENCE, DIGITAL PASSPORT and HUMABIO. BIOSECURE focuses on the use of biometrics to ascertain user identity in information sensitive applications (e.g. online commerce, online banking). FIDIS places the question of biometrics within the broader context of identity and identification in a 'European information society' (EIS), focusing in particular on the balance between security/trust and privacy in a context where digital identities are proliferating: the NoE provides in this sense a reflection on identity in an information society, with a focus on identity management systems, on citizens' trust in current identity and identification systems, on profiling taking into account the risks of automatic profiling, on various possibilities for privacy-preserving practices in information technology intensive identity and identification systems (e.g. study on 'privacy-preserving data-mining'). The STREPs mentioned above all focus on the improvement of biometric technologies: BIO-RESIDENCE aims at promoting the use of biometrics in the context of the development of automatic-access systems, where biometrics are used to ascertain the identity of the user; DIGITAL PASSPORT deals with the specific issue of travel documents and the question of border controls, with a view to developing a new generation of biometric passports that would allow for fast and fully-automated border passage; HUMABIO, finally, focuses on developing new biometric algorithms and sensor types, in order to develop a so-called 'Ambient Intelligence Space' for security-sensitive environments where regular or constant authentication of identity is required. Out of these three, BIO-RESIDENCE is the only project which takes privacy as one of its concerns.

## 2.2. Detection and surveillance

The focus on detection and surveillance – in respect of the development of improved, better communicating or integrated sensor systems, and ameliorated imaging techniques – constitutes a cross-cutting trend in FP6 projects as well as in PASR activities, and one of the broadest field of activity in current EU-sponsored security research:

- **FP6 IP:** 7 IPs funded under different action lines deal with this matter, with either direct or indirect implications for security research. Project LIMES focuses on the possibility of the use of satellite technology to provide information services, tools, and platforms to public authorities engaged in humanitarian operations and the

---

<sup>16</sup> For further indications on FP6 programmes, including summary fiches, please refer to the dedicated website of the Community research and development information service (CORDIS): <http://cordis.europa.eu/fp6/whatisfp6.htm>.

<sup>17</sup> All PASR activities are referenced on the website dedicated by DG Enterprise to security research. For the fiches of the various projects, see: [http://ec.europa.eu/enterprise/security/articles/article\\_2007-02-23\\_en.htm](http://ec.europa.eu/enterprise/security/articles/article_2007-02-23_en.htm).

surveillance of EU land and sea borders, including the surveillance of maritime traffic; LIMES is also claimed to contribute to confronting the proliferation of weapons of mass destruction, organised crime, terrorism and trafficking. The MARNIS and MERSEA projects share this orientation. MARNIS, building on developments in surveillance systems and Galileo applications, focuses on information sharing regarding maritime traffic, including the semi-automatic reporting of positions and destinations of vessels, the exchange of information between public authorities in charge of controlling maritime circulation, but also on the standardisation, harmonisation and circulation of information concerning weather to vessels cruising in European waters. MERSEA aims at developing the Ocean component of the satellite earth-observation project Global Monitoring for Environment and Security project (GMES)<sup>18</sup>, and particularly applications stemming from the observation of oceanic trends and developments: MERSEA adopts a broad focus, including the provision of services for the fishing industry, for the protection of the environment, for the safety and efficiency of maritime traffic, as well as for security agencies and purposes. GMES is also the focus of the SANY project, which focuses on the development of interoperability between various types of sensor systems, including applications for the fusion of data from different categories of sensorial sources, for purposes which include risk management and security. The E-SENSE project, in this respect, also proceeds from the idea of fusing information for differentiated sensor systems, with a focus on real-time provision and management of data. Finally, the TERA EYE and TERANOVA integrated projects deal with the development of new imaging technologies (Terahertz imaging).

- **PASR activities:** 12 PASR projects focus on detection and surveillance, making this area of activity the largest in the preparatory action. These projects are increasingly aimed at either the interoperability and interaction of detection and surveillance instruments, or at the development of new technologies. Within the first thread of research, strong focus is placed on space capacities such as satellites, in projects ASTRO+ (development and integration of Earth-observation capacities for ESDP and JHA activities) and GEOCREW (early detection of crises via satellite observation and development of an information sharing platform for integrating data from different sources). The integrated surveillance of crowded public spaces is also a strong element of this thread: project ISCAPS aims at the development of a system for real-time and automated surveillance in public places; project PROBANT focuses on the assessment and development for real-time monitoring of individuals inside buildings in crisis situations; TRIPS deals in particular with the protection and surveillance of subways and metropolitan railways; and project HAMLeT aims at supporting the development of a real-time indoor surveillance system, integrating data from differentiated sensorial apparatuses. Finally, activities within this thread also share a focus on border management: BS-UAV focuses on the potential use, technical and operational requirements and establishment of mission parameters for border surveillance by unmanned aerial vehicles (UAVs); SOBCAH deals with the development of threat scenarios for both land and sea borders, and the elaboration of matching security architectures,

---

<sup>18</sup> GMES is a joint venture of the European Commission (DG Enterprise) and the European Space Agency (ESA), initiated in 1998 and which participates in the Global Earth Observation System of Systems (GEOSS) international initiative of the Group on Earth Observation (GEO). For further details on GMES, please consult the dedicated website: [www.gmes.info](http://www.gmes.info).

with an emphasis on integrated and networked sensor systems; and STARBORSEC aims at supporting activities in the field of border surveillance technologies, with a focus on EU wide standardisation and interoperability of border surveillance systems. The second thread of research is dominated by projects dealing with the development of new means of detection, such as TERASEC (Terahertz imaging technologies), BODE (dry detection devices – *i.e.* lasers) and ISOTREX (portable devices for the detection of highly energised material via particle/vapour emissions).

- **Other projects:** A host of FP6 STREPs focus on issues of detection and surveillance. The most notable are:  $\mu$ DRONES, which concentrates on the development of a UAV system for surveillance in urban/crowded environments; DICIT, which focuses on the development of voice interfaces for remote controlling of TV systems, which is also acknowledged as a potential breakthrough in surveillance technologies (allowing the monitoring of conversations); DYVINE, which aims at elaborating wireless networks of visual sensors for installation on multiple supports (fixed or airborne); I-IMAS, which aims at developing new generation sensors for dual use (the foreseen domains being health and security). The GMOSS network of excellence, also funded under the FP6, focuses on the integration of European research with regard to earth observation instruments and tools, both on the generic level but also with a specific focus on security, particularly in the investigation of current and future threats and their link with earth monitoring.

### 2.3. Exchange of information, risk anticipation and risk analysis

Another grouping of projects in the FP6 and PASR focuses on technologies for exchanging information, either in a generic form or with security agencies as end-users. Work on exchange of information involves, in this context, research to make platforms more secure, as well as the enhancement of information exchange system in terms of inputs (the mixing of information from differentiated sources) and access (access via mobile devices for instance). Exchange of information, in this regard, is also frequently associated with the capacity to anticipate risks, and to run risk analysis based on available stocks of information.

- **FP6 IP:** Within the FP6, a wide range of programmes address the issue of exchange of information. Integrated programmes such as OPEN\_TC, SEINIT or SERENITY focus on the issue of secure networks (platforms for OPEN\_TC, Ambient Intelligence “ecosystems” for SERENITY), or interoperability between heterogeneous systems (SEINIT). Abovementioned programmes (e.g. E-SENSE, MARNIS, SANY) also fall in this category, to the extent that they deal with questions related to exchanges of information (integrating data for heterogeneous sources, interoperability of systems, “networks of networks”). There are no major FP6 IPs focusing on risk anticipation and risk analysis, but there are a series of autonomous programmes and projects, some run by the EU Joint Research Centre (JRC), some which do not fall within any of the FP6 categories (see below).
- **PASR activities:** Two PASR activities deal with exchanges of information from the perspective of improving security of communications via cryptographic systems (SUPHICE), and enhancing the robustness of information exchange platforms (ROBIN). WINTSEC focuses on developing wireless interoperability among the communications and information exchange systems of European security agencies and services. Beyond the technical development of information exchange systems, projects such as HITS-ISAC focus on the development of

cross-border exchanges of information and analyses, including work on the possibility of merging differentiated sources of data, in order to prevent, predict, and protect against, potential terrorist activities. Exchange of information, albeit on a different scale, is also the central interest of the EUROCCOP activity, which deals with the better connection of pedestrian police officers to information exchange structures, with the twofold objective of improving inputs in terms of information and operational intelligence, as well as conducting criminal investigations. VITA deals with the enhancement of knowledge about risks faced by critical infrastructure systems (see also below), while PATIN conducts the same kind of research for air transportation systems and infrastructure. A whole range of projects, however, also deal with the development of anticipative behavioural models for the purpose of detecting individuals susceptible to involvement in criminal or terrorist activities: one group's projects involves the tracking of individuals through their financial behaviour, such as GATE (which namely focuses on "advanced behavioural modelling" for anti-terrorism financing purposes, by moving beyond the analysis of transactions to include notions of demographics, lifestyle and culture) and I-TRACS (which focuses on the identification of individuals by the analysis of communication, financial and travel data).

- **Other projects:** Among JRC programmes are included reflections on the methodology of risk analysis ("Compatibility of technological risk assessment methodologies" project), and a range of risk analysis projects, dealing with cybersecurity ("Prospective Cybersecurity Activities"), anticipation of natural and industrial disasters ("Risk analysis including MAHB and NEDIES"), or the research on safeguard possibilities in the field of nuclear activities ("Safeguard R&D"). Other projects<sup>19</sup> include development of knowledge, risk assessments and analyses on organised crime (ASSESSING OC, EU-ICS, IKOC, MARC), as well as on migration (via the issue of environment and forced migration – project EACH-FOR).

#### 2.4. Critical infrastructure protection, crisis management and public safety

Critical infrastructure and public safety, including the development of methodologies and tools for crisis management, constitute another major part of FP6 and PASR funded security research. Most of the projects detailed below focus on protective/reactive steps, but in some cases, they also involve the building of threats scenarios and risk analyses.

- **FP6 IP:** There are two main programmes dealing with infrastructure protection in the FP6, both dealing with information and communications systems: DESEREC deals with both the conception of resilient systems and the designing of detection and counter-measure devices; IRRIS concentrates on the reduction of risks to information-based infrastructure systems. The OASIS programme aims at developing a generic system of crisis management, complete with databases, communications system, command and control software as well as decision support software. CHORIST deals with citizen awareness and rescue services communications in industrial or environmental disaster situations, with an eye at improving the communication of guidelines and directives to citizens and improving the coordination of rescue and civil protection agencies and services. Other examples include the SPADE programme, which aims at developing a

---

<sup>19</sup> The exact status of these projects (whether they are STREP, JRC projects or otherwise) is not specified in available documents.

platform for decision-making and operational support for air transportation facilities, including for safety and emergency situations. This broad perspective (in automobile transportation infrastructures) is also shared by the GST programme, which focuses on telematics for safety purposes in automobile traffic. Finally, as an example of more narrowly focused projects, the NANOSECURE programme aims at harnessing nanotechnologies for the purpose of detection and detoxification of harmful airborne substances.

- **PASR activities:** Several threads of research can be distinguished: general preparedness for infrastructure protection (VITA, which focuses on the development of threats scenarios and the evaluation of available tools; PATIN which deals with the same issue regarding air transportation infrastructure); focus on specific infrastructure and safety issues: PALMA which focuses on threats to aircrafts by ground-air individual defence systems (MANPAD<sup>20</sup>) attacks, BIO3R which concentrates on biological attacks including threats and response scenarios and awareness/prevention, AEROBACTICS which deals with microbial dispersion models in cases of biological attacks, and WATERSAFE which looks at detection and detoxification devices for the protection of water systems. Another thread of projects concentrates on the preparedness of public authorities and technological devices in a crisis management context: CRIMSON proposes the development of hardware and software in virtual simulations of crisis situations for training purposes; TIARA deals with the constitution of a European network for reaction in the case of radiological incidents; MARIUS, with the development of an integrated pre-operational command post, including a mobile information system, for crisis situations; in this vein, CITRINE proposes the development of crisis management tools based on a real-time information system, with multiple users (NGOs, health services), in a variety of crisis situations (ranging from humanitarian interventions to rescue operations).

## 2.5. Freedom and privacy

Research on freedom and privacy in the context of a changing landscape for security practices and technologies has been identified as an important concern in relevant European Commission documents as well as by the European Data Protection Supervisor, and has been undertaken in several FP6 and PASR activities, from two angles: a reflection on the ethical, legal, political and social implications of security technologies, and research on “privacy preserving” technologies.

- **FP6 IP:** In FP6, three major programmes have dealt with the issues of freedom and privacy in relation with developing security technologies. The first one is the CHALLENGE programme, which includes the issue of technologies from the angle of freedom and privacy in a wider reflection about the “changing landscape” of liberty and security in Europe. The second one, PRIME, concentrates specifically on information technologies and addresses “privacy-enhancing identity management”, combining both non-technological and technological possibilities offered to enhance the protection of personal data. The GUIDE programme also looks into these issues, from the perspective of access to e-Government services, by working on the twofold issue of trust (can electronic identities be trusted?) and privacy/data protection. Finally, alongside these integrated programmes, the already-mentioned FIDIS network of excellence explores, in the context of research on biometric identifiers, the possibility of

---

<sup>20</sup> “Man portable air defence systems”.

privacy-preserving or privacy-enhancing technologies with regard to databases and practices of profiling.

- **PASR activities:** Two key PASR-funded activities have dealt with the matter of freedom and privacy. ESSTRT, while focusing on potential threats, threat scenarios, and the necessary technological developments required to meet anticipated menacing trends (particularly terrorism, which constitutes the core concern of ESSTRT's final report), takes into account the implications in terms of freedom and privacy, highlighting that these questions have to be met while nonetheless developing those technologies which are presented as necessary for the preservation of security. Support activity PRISE, on the other hand, concentrates on the development of security policies in line with privacy requirements, exploring in particular the potential for privacy-preserving and privacy-enhancing technologies.

## 2.6. Analysis

This overview of security measures funded under the FP6 and PASR has provided a broad image of the security technology landscape that requires further discussion, in particular in the light of concerns for the impact of such security technologies on the fundamental freedoms and rights of individuals. As the elements provided above point out, EU-supported security research has strongly focused on meeting security challenges through technologies that allow for pro-activity, prevention, and generally speaking anticipation, including by means of individualisation of control and surveillance (typically, the PASR-funded GATE and I-TRACS projects). Projects aiming to increase interoperability between databases and the enhancement of information exchange systems multiply in this regard the possibility of personal data being used for purposes beyond the ones for which this data was initially connected.

The PASR provides an illuminating example of the overall trend in EU-funded security research. Out of the 39 activities supported under the PASR, only one (PRISE) takes as its major concern and explicit focus issues of freedom and rights, via the question of privacy and data-protection. Out of the 44,5 million euros of the actual Community contribution to the PASR, however, PRISE only accounts for slightly above 600.000 euros. The situation is similar in FP6 projects, with CHALLENGE being the main project dealing with the various legal, political and social effects of European security policies: this is a large integrated project with a Community contribution of 4,5 million euros, but it is nonetheless dwarfed by the number of projects and amount of EU funding put into stand-alone security technological development. As an illustration, the 7 integrated projects listed in the 'Detection and surveillance' section above (2.2) account for more than 62 million euros in Community contribution.

Of course, despite these obvious limitations, it remains important to stress that EU-funded research on security technologies has not entirely away from discussions on privacy, fundamental freedoms and rights. Several of the research projects and activities mentioned above, including the ones geared towards technical cooperation and technological development, take the issues of freedom, privacy and rights as part of their concerns. Two trends are discernible in this respect:

- Research on privacy preserving security technologies (e.g. FIDIS, GUIDE).
- Research on the ethical, legal, political and social implications of the utilisation of security technologies (e.g. CHALLENGE, PRISE).

These developments are important, and should be welcomed. Furthermore, the involvement of actors from the security industry in reflection on these issues stands out as a sound initiative. However, work on freedom, privacy, and rights should continue, particularly with regard to the conceptual position that underpins the aforementioned projects. In many cases, freedoms and rights are discussed as part of the notion that necessary measures to increase the security of the EU, its Member States, and its citizens should be balanced against the preservation of freedoms and rights. This is the image of a ‘balanced’ approach to security. In most cases, however, the ‘balance’ between security and freedom is understood in a context where security is the fundamental concern, and the respect of fundamental freedoms and rights is one of several criteria and standards to be met by developing technologies, which may be “sacrificed”. Typical in this respect is argument contained in the final report from the PASR-funded ESSTRT<sup>21</sup>: “Achieving 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. Some anti-terrorist measures in Europe have required citizens to sacrifice civil liberties – for example by diminishing privacy, restricting free speech and extending periods of detention without charge. [...] Technologies can help considerably in the fight against terrorism. [...] Legal and ethical considerations are, however, important. Some technologies arouse concerns about invasion of privacy; reliability – the risk that people could be wrongly identified as security threats; social exclusion; damage to humans and the environment; and difficulties of regulation”<sup>22</sup>.

A major question is whether security research should primarily be driven by concerns for more sophisticated technologies (which are presumed to be more efficient), or by political concerns for freedoms and rights, which include - but also go beyond - legal and ethical concerns. Containing the potentially harmful consequences of the growing use of increasingly sophisticated security technology via codes of conduct, best practices, and other systems of rules is certainly a possibility. However, it may be more effective to promote the freedoms and rights of individuals by further embedding ethical, legal, political, and social research into the EU-funded frameworks for governing security research and development.

### 3. Conclusions and recommendations

From this brief survey, it appears that a majority of FP6 and PASR activities are oblivious to the fact that security cannot be considered as a norm, as a *prima facie* value which has to be expanded. They do not analyse the necessary limits of security, and must be reminded that security can be considered as an exception - a legitimate derogation to the fundamental rights which are the core values of the EU under specific circumstances - but never as an overarching principle, equivalent to freedom and democracy. Security is there to protect freedom, and is subordinated to freedom (see the European Convention of Human Rights). Security and freedom cannot be analysed through the metaphor of the balance between two equivalent values. Security is the means to achieve freedom and democracy. If the main programmes of FP6 and now FP7 are oriented towards the promotion of technology and security by European companies competing in a global market, but miss the relations with the stated goals of the European Charter and European Convention of Human Rights, they may undermine the core values of the EU. The role of the European Parliament must be to

---

<sup>21</sup> ESSTRT stands for “European Security: High Level Study on Threats, Responses and Relevant Technologies”, a joint project of Thales Research and Technology (UK), the International Institute for Strategic Studies (UK) and the Crisis Management Initiative of Matti Ahtisaari.

<sup>22</sup> ESSTRT (2006) (Deliverable D6-1). *New European Approaches to Counter Terrorism*, p.20-21.

stand for these values, to insist on the inclusion, within EU security research, of programmes monitoring the other programmes in order to check their impact on freedom, individual rights, presumption of innocence, and programmes specifically addressing the relations between freedom, democracy and security at an interdisciplinary level. Closer association of fundamental rights and data protection agencies could also be considered<sup>23</sup>. It is crucial that the political and ethical questions of the relations between democracy, security and technology are not reduced to the inclusion of a professional code of ethics by the companies providing technologies, even if this is important. Ethics cannot be limited to this specific aspect. Politics, in the sense of analysis of legitimacy of the actions and consequences (intended or not) of these actions, cannot be marginalised by a discourse focusing only on technological efficiency.

The European Parliament must define those aspects crucial to the maintenance of a democratic society, and the limits of security, with the help of large-scale research programmes which combine the knowledge of different disciplines with the expertise of the EDPS and those different bodies associated with the Article 29 Data Protection Working Party. If it fails to do so, the judges of the European Court of Human Rights and the European Court of Justice will be the only guarantors against excess. The shortcomings of this as a solution are evident in Germany, where the level of disagreement between the German Ministry of the Interior (and some of its European counterparts at the origin of the Prum initiative) and the *Bundesverfassungsgericht* has now made it very difficult for them to work together, as they have very different visions of the rights of individuals and data-protection<sup>24</sup>. It is far better that the European Parliament plays its full role regarding the executive, whether it is the Commission, or Council Initiatives. It is the great lesson of Montesquieu that the logic of security, by giving more power to the executive, increases the temptation to use security as the ultimate value. In consequence, the legislative and judicial powers have to work jointly, not to paralyse, but to check what the executive (and the “ingenious industry », according to Tocqueville) is doing effectively for security and democracy when developing through its administration, a body of knowledge and technology it wants to accumulate.

Accordingly, we recommend that the European Parliament insists on its budgetary role, and calls on the Commission to establish within the upcoming new FP7 call a significant percentage - at least 10 to 15% of FP7's total budget - dedicated to programmes which focus primarily on freedom of circulation, data protection, limits of security, and the relationship between security, privacy and technologies. This could also be accompanied by a deeper enquiry into the projects that have been conducted under the FP6 and PASR.

---

<sup>23</sup> See for instance the recent policy paper of the European Data Protection Supervisor on this issue: European Data Protection Supervisor (2008). *The EDPS and EU Research and Technological Development*.

<sup>24</sup> In February-March 2008, the *Bundesverfassungsgericht* produced a series of decisions running against evolutions in the security laws of several Länder (Nordrhein-Westfalen in the first place, Hessen and Schleswig Holstein later on). These evolutions would have allowed for the setting-up of automated systems of personal data collection (data from private computers for the former, number plates for the latter). In the same movement, the Court suspended some provisions of the federal law implementing the European data retention directive. In its decisions, the Court particularly insisted on the importance of individuals to know about their personal data being collected, the authorities responsible for the collect, and the databases on which they are being stocked, as a fundamental principle of data protection.