EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Developing an EU Internal Security Strategy, fighting terrorism and organised crime

STUDY

EN

2011

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Developing an EU Internal Security Strategy, fighting terrorism and organised crime

STUDY

Abstract

The present study examines the steps taken since the entry into force of the Lisbon Treaty in the field of internal security and assesses commitments made in the areas of fundamental rights and civil liberties. The study examines the development of the EU Internal Security Strategy, with special attention paid to fighting terrorism and organised crime. It also investigates the activities of the main EU agencies involved in internal security policies. The study finally sketches out the key challenges lying ahead for EU internal security policies, with particular consideration paid to the role that the European Parliament will be called upon to play.

PE 462.423 EN

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

AUTHORS

Dr. Amandine Scherrer (Centre d'Etudes sur les Conflits, Paris)
Dr. Julien Jeandesboz (King's College, London)
Dr. Emmanuel-Pierre Guittet (University of Manchester, UK)

Under the coordination of the Centre d'Etudes sur les Conflits (C&C) and of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS)

RESPONSIBLE ADMINISTRATOR

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

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

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

Manuscript completed in November 2011

This document is available on the Internet at:
http://www.ipolnet.ep.parl.union.eu/ipolnet/cms/pid/1401
http://www.europarl.europa.eu/delegations/en/studies.html

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS 5

EXECUTIVE SUMMARY 8

INTRODUCTION 12

1. PRIORITIES OF EU INTERNAL SECURITY:BACKGROUND AND THE EUROPEAN SECURITY STRATEGY 16

1.1. Background 16

1.1.1. The analysis of the European fight against organised crime and terrorism: The state of the debate 17

1.1.2. The question of knowledge 21

1.1.3. The question of civil liberties 24

1.2. The European Internal Security Strategy 26

1.2.1. Strategy-making in the AFSJ: The Internal Security Strategy in context 27

1.2.2. The Internal Security Strategy and ISS in Action communication 30

1.2.3. Conclusion - The ISS and the post-Lisbon AFSJ strategic environment: The lack of articulation between security and freedom 33

2. ACTORS AND AGENCIES OF EU INTERNAL SECURITY: STATE OF PLAY AND CURRENT TRANSFORMATIONS 36

2.1. The Commission: the transformation of DG JLS 37

2.2. The Council: The establishment of COSI and changes to the working structures 38

2.2.1. COSI: Background 39

2.2.2. Ongoing debates and challenges 40

2.3. EUROPOL 46

2.3.1. Background on the agency 46

2.3.2. Ongoing debates and challenges 46

2.3.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS 47

2.4. FRONTEX 51

2.4.1. Background on the agency 51

2.4.2. Ongoing debates and challenges 53

2.4.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS 57

2.5. CEPOL 60

2.5.1. Background on the agency 60

2.5.2. Ongoing debates and challenges 62

2.5.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS 64

2.6. EUROJUST 66

2.6.1. Background on the agency 66

2.6.2. Ongoing debates and challenges 67
2.6.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS 69
2.7. The undefined role of the Counter Terrorism Coordinator, OLAF and SitCen 72
2.7.1. The EU Counter Terrorism Coordinator 72
2.7.2. The European Anti-Fraud Office (OLAF) 73
2.7.3. The EU Situation Centre (SitCen) 73
2.8. Current trends in agency and institutional cooperation in EU internal security policies 75
2.8.1. Cooperation between EU agencies, bodies and services in the field of internal security 75
2.8.2. The drive towards intelligence-led policies 80
2.8.3. The role of the freedom agencies of ISS 82
3. CHALLENGES OF EU INTERNAL SECURITY 87
3.1. The policy challenge 87
3.1.1. Towards an evidence-based EU policy 88
3.1.2. Effective consultation and involvement of the European Parliament and of bodies in charge of fundamental freedoms and rights 89
3.2. The technological challenge 91
3.2.1. The drive towards technology-intensive EU internal security policies 92
3.2.2. The question of data processing 98
3.2.3. The issue of oversight 105
3.3. The internal/external relations challenge 109
3.3.1. The external dimension of internal security policies in the post-Lisbon context 109
3.3.2. EU internal security activities in third countries: key areas of concern for the future 111
3.3.3. The implications of third country security policies for EU fundamental freedoms and rights 114
CONCLUSION 116
RECOMMENDATIONS 118
References 122
Annex 132

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
AWF	Analysis Work Files
CATS	Article 36 Committee
CMS	Case Management System
CEPOL	European Police College
CFR	Charter of Fundamental Rights
CIREFI	Centre for Information, Discussion and Exchange on the Crossing of Frontiers
CIRAM	Common Risk Integrated Model
COE	Council of Europe
COSI	Standing Committee on Operational Cooperation on Internal Security
COTER	Council working group on terrorism
CSDP	Common Security and Defence Policy
CTC	Counter Terrorism Coordinator
DCI	Development Cooperation Instrument
DPO	Data Protection Officer
EAWs	European Arrest Warrants
ECIM	European Criminal Intelligence Model
ECJ	European Court of Justice
EDF	European Development Fund
EDPS	European Data Protection Supervisor

EIS	EUROPOL Information system
ENISA	European Network and Security Agency
ENPI	European Neighbourhood Policy Instrument
EP	European Parliament
EULEX	European Union Rule of Law Mission in Kosovo
EUROSUR	European Border Surveillance System
FJST	FRONTEX Joint Support Teams
FRAN	FRONTEX Risk Analysis Network publication
HTCC	EUROPOL's High Tech Crime Centre
ILOs	Immigration Liaison Officers
ISS	Internal Security Strategy
JITs	Joint Investigation Teams
JROs	Joint Return Operations
JSB	Joint Supervisory Body
MASP	Multi-Annual Strategic Plan
MLA	Mutual Legal Assistance
MDG	Multidisciplinary Group on Organised Crime
MoU	Memorandum of Understanding
MS	Member States
OAPs	Operational Action Plans
OC	Organised Crime
OCTAs	Organised Crime Threat Assessment Reports
PAD	Policy Advisory Document
PNR	Passenger Name Record

PSC	Political and Security Committee
RABIT	Rapid border intervention teams
SCIFA	Standing Committee on Immigration, Frontiers and Asylum
SitCen	Situation Centre
SOCA	UK Serious and Organised Crime Agency
SOCTAs	Serious and Organised Crime Threat Assessment Reports
TCM	Terrorism convictions monitor
TEU	Treaty of the European Union
TFTP	Terrorist Finance Tracking Programme
TE-SATs	Terrorism Situation and Trend reports
TWG	Terrorism Working Group

EXECUTIVE SUMMARY

The present study examines the steps taken since the entry into force of the Lisbon Treaty (2009) in the field of internal security and assesses commitments made in the areas of fundamental rights and civil liberties. It surveys the drafting of the Internal Security Strategy (ISS) (1.2) and investigates the activities of the main European Union (EU) agencies, bodies and services involved in internal security policies (2). It finally sketches out the key challenges lying ahead for EU internal security policies, with particular consideration for the role that the European Parliament will be called to play (3).

The standing of fundamental rights, freedoms and justice, in view of the Lisbon Treaty and the development of the ISS is at the heart of the present analysis. With the abolition of the pillar system, issues of policing, counter-terrorism and judicial cooperation in criminal matters are now bound to the same common objectives and requirements as other EU policies. Alongside the changes to the EU's institutional structure, the Lisbon Treaty brings about two crucial modifications in this respect: it gives the Charter of Fundamental Rights legally binding status and introduces in the Treaty on European Union a general commitment to such principles as freedom, the rule of law and respect for human rights (Article 2 TEU). In the meantime, the inflection given to the Area of Freedom, Security and Justice (AFSJ) policies since the Laeken European Council (2001) and the Hague programme (2004) have seen a significant increase in security-related initiatives which have proved a challenge for legal guarantees of fundamental freedoms and rights and requirements of transparency and democratic accountability.

In this context, the study identifies key elements that require careful attention as regards fundamental freedoms, transparency and accountability.

- **The policy process**

The most important challenge for ensuring the proper functioning of the EU system of checks and balances, guaranteeing democratic accountability and enforcing compliance with the fundamental freedoms and rights obligations laid down in the Treaties, relates to the organisation of internal security policy. It is to devise a policy process that is inclusive of all stakeholders.

The work methodology adopted by the Standing Committee on Internal Security (COSI), which is called to play a central role in the ISS, and the subsequent establishment of an EU "policy cycle" for internal security (originally developed through the "Harmony" project) raises questions in this respect (2.2). The analysis of the managerial model that will be applied to EU security activities (based on the 'Harmony Project' proposals) highlights a lack of monitoring arrangement involving the European Parliament. Although the role of the EP is limited in decision-making on matters of operational cooperation due to the provisions contained in Article 87(3) TFEU, the envisaged policy cycle touches upon areas where the EP might have a say. The EU policy process in the field of internal security does not specify mechanisms through which, in accordance with Article 70 TFEU on impartial evaluation of EU policies, Article 71 TFEU on COSI and Article 6(2) of the COSI Decision, the European Parliament and national Parliaments are kept "informed", and how their comments can be taken on board (2.2.2.4).

Additionally, the working methodology adopted by COSI for internal security does not clearly lay down provisions for independent or external evaluations of the information and analyses leading to the development of internal security policies.

The question of the methodology developed by the "Harmony project" is even more

important when analyzing the threat assessments produced by EUROPOL that have become central for decision-making and are to become the basis for EU policy cycles in internal security (2.3). As such, it appears fundamental to make sure that the methodology used in such reporting exercise is made fully transparent, so it can be externally assessed just like any other knowledge process.

- **The inclusion of 'Freedom Agencies'**

The European security model advocated in the ISS supports an all-encompassing definition of internal security and a restrictive definition of the interactions between security, freedom and justice. Despite the commitments laid out in the Stockholm Programme in this respect, an illustration of that matter is the fact that bodies in charge of freedoms and rights are not systematically included in ISS activities. Does this imply that security is to be the driving priority of the AFSJ?

This is particularly clear in COSI's activities. There are grounds, detailed in the study, to include bodies such as the European Data Protection Supervisor (EDPS), the Article 29 Working Party or the Fundamental Rights Agency (FRA) in the planning of operational priorities undertaken by COSI (2.8.3). This is all the more possible as the FRA is now considered to be part of the JHA Agencies.

In this respect, it is worth noting that COSI's remit includes the evaluation of operational cooperation: the grounds on which the exclusion from such an evaluation of inputs of agencies in charge of fundamental rights remain unclear.

Of further concern are the consequences that such a situation might have after 2014 when the ECJ's mandate is fully extended to the AFSJ. Over the years, the EU's operational activities in the field of internal security have been met with considerable and extensive criticism from the point of view of fundamental freedoms and rights. The possibility of legal action over operational activities coordinated by the EU, and the related need to ensure that fundamental freedoms and rights are upheld in these activities constitute a solid basis for involving bodies such as the FRA, the EDPS or the Article 29 Committee in the evaluations conducted by COSI (3.2).

- **Roles, tasks and priorities of EU agencies in charge of security**

EUROPOL has benefited the most from the orientations encapsulated in the ISS (2.3). The agency has committed significant efforts to taking the lead in many areas the ISS covers, such as threat assessments and the exchange of information, including personal data. The second agency to benefit from the current state of play in EU internal security policies is FRONTEX (2.4). The agency should indeed see its mandate reinforced, with increased control over the initiating of joint operations and pilot projects. Much like EUROPOL, it appears to be gaining an increasingly central role in the collect and analysis of information regarding the external borders, in the field of risk analysis and threat assessment on the one hand, and with regard to access to electronic data, including the processing of personal data, on the other.

The two other main JHA agencies, CEPOL and EUROJUST (2.5. and 2.6) appear in a much weaker position. CEPOL has experienced difficulties following interrogations on its capacity to manage its financial resources according to the standards and regulations applying to EU bodies, but also from the lack of clarity as to its networked structure and the development of training activities by other EU agencies. EUROJUST is on the other hand experiencing other kind of difficulties, among which its quest for a clear positioning in the

EU security landscape. The report nevertheless reviews renewed possibilities for these agencies in an ISS context.

Furthermore, some EU agencies require clarification as to their role and tasks within the ISS (2.7). The future roles of the Counter Terrorism Coordinator (CTC), the positioning of the European Anti-Fraud Office (OLAF), as well as the involvement of the EU Situation Centre (SitCen) are not so clear in the context outlined by the ISS.

- **Data protection and the issue of oversight**

Data protection is a central issue for oversight in a context of technology intensive internal security policies relying on the processing of personal data (3.2).

The expansion of data processing has led to the development of a number of proposals for their regulation within the framework of internal security policies. An analysis of the Information Management Strategy (IMS), whose aim is to regulate data exchanges and processing, highlights several shortcomings: the strategy takes a strong stance in favour of data sharing and processing without clarifying which are the agencies, bodies, institutions or services that should be involved in ensuring that “information management” complies with all the requirements related to the right to data protection. Neither does it gives provisions on what should be the role of EU and national data protection authorities, of the European Parliament and of national Parliament, in the management of information exchanges. The European Commission Communication for a comprehensive approach on data protection in the European Union (adopted in November 2010) demonstrated the need for a single data protection framework, for increased oversight of law enforcement activities involving the processing of personal data, and to pay particular attention to specific forms of data processing.

The study reviews promising ways of efficiently addressing the issue of oversight with regard to data processing. The inclusion for instance of a statutory accountability principle in the revised EU data protection framework, supported by the Article 29 Committee, as well as appropriate and effective measures related to the legal obligations of the EU and its Member States with regard to fundamental rights and freedoms, including the right of data protection, could be a good starting point. On that matter, opinions expressed by the EDPS, the Article 29 Committee, or the FRA, demonstrates that EU safeguards are already in place and that their work should be more mobilised in EU internal security activities, in order to ascertain that requirements regarding impact assessment, for instance, are being observed in developing policies on internal security. These procedures include, for example, respect of the impact assessment guidelines designed by the European Commission and checks on how proposed measures comply with the Charter of Fundamental Rights according to the standards laid out by the European Commission and the Council Secretariat.

This aspect reinforces the need for more inclusion of freedom agencies in EU internal security policies. The involvement of EU “Freedoms Agencies” should not be seen as a concession offered to “civil liberties” supporters, but as an efficient way to comply with the rule of law and avoid controversies, as well as the possible consequences of court decisions.

- **Effective compliance of external activities**

Security cooperation with third countries raises a number of challenges and can be highly sensitive, as demonstrated by controversies around the EU-US TFTP and PNR agreements. The gist of the challenge regarding external relations is the possibility to ensure effective

compliance of external activities in the field of internal security with the principles governing the AFSJ as a whole, and particularly with Treaty-based obligations in the field of fundamental freedoms and rights (3.3).

There is clearly a need for monitoring the arrangements and agreements concluded by EU agencies and bodies with third countries. This would arguably reflect the fact that the Lisbon Treaty grants the EU a single legal personality and provides a single legal basis for the conclusion of international agreements (Article 217 TFEU). Article 218 TFEU further establishes a single procedure for this purpose, where the consent of Parliament is required for all fields where the ordinary legislative procedure applies, and in the fields where the special legislative procedure requires consent (Article 218(6)(a) TFEU). In other cases, the Parliament is to be consulted, although the Council does have the option of fixing a time limit for the issuance of an opinion (Article 218(6)(b) TFEU). This implies that in matters falling under Article 87(3) TFEU (operational cooperation in internal security matters), Parliament may only be consulted, but this consultation is mandatory.

Another issue for concern in recent years has been the direct involvement of the EU and its Member States in internal security operations in third countries. The best-known example of such a situation is the HERA series of operations coordinated by FRONTEX since 2006, which are based in the Canary Islands.

A third set of questions regarding the external dimension involves the impact of the security policies of EU partners on the guarantees regarding fundamental freedoms and rights afforded by the Union's legal framework. At stake here is in particular the unfolding of the relationship between the EU and the US in security matters. Of particular concern, in this regard, are the recent proposals of the European Commission towards the establishment of a European TFTP and European PNR. What are the implications of implementing policies which continue to raise so many questions among European citizens and governments?

While analysing these challenges, the study finally set out recommendations that are relevant for future EP actions in the field of the ISS. By reinforcing the powers of the European Parliament and despite the derogations to the ordinary legislative procedure in the field of police cooperation and operational activities, the Lisbon Treaty also puts additional requirements on the EP to engage actively with the monitoring of EU initiatives in the field of internal security. Monitoring and oversight involve three key areas that are addressed in the final recommendations: the development of an evidence-based EU policy, the enforcement of effective consultation at all stages of the European Parliament, and the promotion of a more open participation in internal security policies.

INTRODUCTION

The entry into force of the Lisbon Treaty on 1 December 2009 has consecrated the standing of the area of freedom, security and justice (AFSJ) as the European Union's (EU) second objective after the promotion of peace and the well-being of its citizens (Article 3(2) TEU). The Lisbon Treaty has simultaneously introduced a number of changes. It has most prominently abolished the pillar system originally introduced in the Maastricht Treaty. The AFSJ is now an area of shared competence between the EU and the Member States as laid out in Article 4(2) TFEU, where the 'ordinary legislative procedure' (Article 289 and 294 TFEU) applies. Article 10 of Protocol No. 36 annexed to the Lisbon Treaty nonetheless suspends the full application of this shared competence with regard to the powers of the Commission and the European Court of Justice (ECJ) in the field of police cooperation and judicial cooperation in criminal matters (former third-pillar matters), for a transitional period of five years after the entry into force of the treaty. Article 9 of the same Protocol additionally establishes that the acts adopted prior to the entry into force of the Lisbon Treaty will retain their legal effects until modified.[1] Finally, in specific domains related to the AFSJ, and particularly in the field of operational cooperation, 'special legislative procedures' still remain in place (Article 87(3) TFEU), whereby the Council may act unanimously while Parliament is only consulted.[2]

The changes brought about by the entry into force of the Lisbon Treaty open up a number of questions related to the development of EU activities in the field of internal security. While Lisbon formalises the demise of the third pillar, several exclusions from the ordinary legislative procedure involving fully the Commission, the Parliament and the ECJ, are maintained in this domain. Some are transitional, as in the case of Protocol No. 36. Some are permanent (short of a treaty revision), as in the case of operational cooperation envisaged in Article 87(3) TFEU. **A first hypothesis is that an explanation to these exclusions can be found in the contradictions between state sovereignty and European integration**. Article 4(2) TFEU, for example, commits the Union to respect "essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State". Security matters, defined as 'national security', are considered as part of the sovereign domain of competence of each Member State, and as such cannot be conducive to EU involvement, leading to the adoption of the aforementioned exclusions. Article 72 TFEU, in this regard, highlights that Title V TFEU "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security".

A second hypothesis, however, is that the tension between national sovereignty and European integration is only a small part of the explanation. **What is at stake in the field of internal security is less the 'defence' of the sovereignty of individual EU Member States in view of expanding EU competencies, than the preservation and possibly the diffusion of practices of policy-making initially established in the context of the Schengen cooperation and of the third pillar.**

[1] "[R]epealed, annulled or amended."

[2] The provision also concerns matters related to passports, identity cards and residence permits (Article 77(3) TFEU).

These practices include the predominance of intergovernmental modes of decision-making through the Council and its working structures, the favouring of discretion and secrecy in the conduct of security activities and the limited participation of other institutions and bodies. One can consider, in this respect, the abovementioned Article 72 TFEU in relation with Article 73 TFEU, which specifies that Title V "shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security". The point is less the tension between sovereignty and integration, than the preservation of the capacity for Member State governments to decide when and how forms of integration can proceed.

A number of scholarly contributions have shown that the development of the AFSJ has been heavily influenced by controversies and struggles stemming from the earlier initiatives adopted in the Schengen and third-pillar contexts. Disagreements persist, however, as to the interpretation of this influence. Some hold that Schengen in particular has been a laboratory for the development of communautarised policies in the field of justice and home affairs.[3] The entry into force of the Treaty of Amsterdam, which concomitantly incorporated the Schengen corpus into EU law and transferred issues of asylum, immigration and border control from the third to the first pillar, is said to illustrate this process. Others point to the fact that the incorporation of Schengen into EU law has, to some extent, 'Schengenised' the Community, by enabling ministries of the Interior and Justice as well as officials and experts from police and border guard services to intervene in a wider number of activities and policies undertaken through the European Union.[4] 'Third-pillar' concerns and practitioners have operated over the past decade at the junction between the first and second pillar as well, through the definition of the Union's visa policies, for instance, or of the so-called 'external dimension' of the AFSJ. The question is now whether the entry into force of the Lisbon Treaty and the collapse of the pillar system has altered this trend. **Are we seeing a streamlining of previous third-pillar practices into the general EU framework for decision- and policy-making? Are the developments taking place under the heading of internal security in fact hailing the persistence, and possibly the reinforcement, of these practices? To examine the development of an EU Internal Security Strategy (EU ISS), in this respect, requires surveying the state of play of relations between the agencies, bodies and services currently tasked with issues of internal security in the EU**. The adoption of the EU ISS under the auspices of the Spanish Presidency in February 2010 has to be put in perspective, for example, with the establishment of the Standing Committee on Internal Security (COSI), whose first meeting took place the following month.

Of central importance in this assessment is the standing of fundamental rights, freedoms and justice. With the abolition of the pillar system, issues of policing, counter-terrorism and judicial cooperation in criminal matters are now bound to the same common objectives and requirements as other EU policies. Alongside the changes to the EU's

[3] See inter alia P. Berthelet, (2011), *Le paysage européen de la sécurité intérieure*, Zurich: Peter Lang; W. de Lobkowicz, (2002), *L'Europe de la sécurité intérieure: une élaboration par étapes,* Paris: La Documentation Française; J. Monar (ed.) (2010), *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice,* Brussels: Peter Lang.

[4] See inter alia T. Balzacq and S. Carrera, (eds) (2005), *Security Versus Freedom? A Challenge for Europe's Future*, London: Ashgate; D. Bigo and A. Tsoukala, (eds) (2008), *Terror, Insecurity and Liberty: Illiberal practices of liberal regimes after 9/11*, London: Routledge; E. Guild and F. Geyer, (eds) (2008), *Security Versus Justice? Police and Judicial Cooperation in the European Union*, London: Ashgate; D. Bigo, S. Carrera, E. Guild and R.B.J. Walker (eds) (2010), *Europe's 21st Century Challenge: Delivering Liberty*, London: Ashgate.

institutional structure, the Lisbon Treaty brought about two crucial modifications in this respect: it gives the Charter of Fundamental Rights legally binding status and introduces in the Treaty on European Union a general commitment to such principles as freedom, the rule of law and respect for human rights (Article 2 TEU). In the meantime, the inflection given to AFSJ policies since the 2001 Laeken European Council and the December 2004 Hague Programme have seen a significant increase in security-related initiatives which have proved a challenge for legal guarantees of fundamental freedoms and rights and requirements of transparency and democratic accountability. This trend has been justified, most notoriously, through the argument that AFSJ policies needed to strike a 'balance' between security and freedom, whereby security was considered as an equivalently valuable right.[5] It has led to a number of well-publicised incidents between the Council, the European Commission, the Parliament and other bodies such as the European Data Protection Supervisor. The 2009 Stockholm Programme has recognised the problem by highlighting that "the challenge will be to ensure respect for fundamental rights and freedom and the integrity of the person while guaranteeing security in Europe. It is of paramount importance that law enforcement measures, on the one hand, and measures to safeguard individual rights, on the other, go hand in hand in the same direction and are mutually reinforced".[6] Likewise, the EU ISS claims to be inspired by the "values and principles established in the Treaties of the European Union and set out in the Charter of Fundamental Rights"[7] and highlights the need for "justice, freedom and security policies which are mutually reinforcing whilst respecting fundamental rights, international protection, the rule of law and privacy".

The present study examines the steps taken since the entry into force of Lisbon in the field of internal security to assess to what extent this commitment has been followed by action. It surveys the drafting of the Internal Security Strategy (section 1). It also investigates the activities of the main EU agencies involved in internal security policies (section 2). It finally sketches out the key challenges lying ahead for EU internal security policies, paying particular consideration to the role that the European Parliament and national Parliaments will be called upon to play (section 3).

This study is based on the collect and analysis of EU documentation dedicated to the fight against terrorism and organised crime as well as a follow up of all current initiatives affecting (officially or not) the EU internal security strategy. In particular, full attention has been given to the publications of the European Commission, the Council (with particular attention to COSI) and of the EU counter-terrorism coordinator on the priorities and guiding principles for the EU Internal Security Strategy, as well as the European Parliament's positions and resolutions on that matter. Collection of data has also concerned other actors: Council of Europe, European Court of Human Rights and European Court of Justice, European Data Protection Supervisor, and some key civil society representatives as well as NGOs active in the field of democratic scrutiny. In addition, semi-structured *in situ* interviews with key actors involved in the internal security field have enabled a qualitative analysis of their positions, experiences and opinions.

In order to provide additional information and evidence, this study relies on visual supports. Figure 5 available in the Annex presents the institutional and effective relations

[5] The European Internal Security Strategy, for example, considers security as a 'basic right'. See below, section 1.2.2.

[6] Council of the European Union (2010), The Stockholm Programme – An open and secure Europe serving the citizen, 5731/10, 3.3.2010.

[7] Council of the European Union (2010), Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 5842/2/10, 23.2.2010.

between EU agencies, bodies and services in charge of internal security in the pre-Lisbon context. Four timelines presenting the evolution of European internal security policies since the 1960s can additionally be accessed online (http://jiminy.medialab.sciences-po.fr/deviss/timeline/). Interested readers will find in the Annex a methodological note on how these timelines have been constructed and can be read.

1. PRIORITIES OF EU INTERNAL SECURITY:BACKGROUND AND THE EUROPEAN SECURITY STRATEGY

KEY FINDINGS

- An analysis of the logic that has prevailed in EU policies in response to Organised Crime and terrorism over the last two decades shows an increasing focus on intelligence-led, proactive and anticipative tools and strategies. Such logics have led to debates and controversies over the guarantee and protection of civil liberties and fundamental rights (e.g. on terrorist "watchlists").
- The current threat assessments produced by Europol raise a number of questions from a methodological point of view. The issue at stake is the development and promotion of an evidence-based policy in the areas of organised crime and terrorism. In these domains, debates over legal definitions and law enforcement capacities largely predominate. The survey of strategy-making activities in the AFSJ, brings to the fore the question of change in the development of the EU's policies in this area over the past twenty years.
- The European security model advocated in the ISS does not establish a hierarchy between the challenges it identifies, nor does it establish distinct priorities. At no point does the strategy define the scope and therefore limits of what constitutes an internal security issue.
- The ISS supports an all-encompassing definition of internal security and a restrictive definition of the interactions between security, freedom and justice, despite the commitments laid out in the Stockholm Programme in this respect, an illustration of that matter is that bodies in charge of freedoms and rights are not systematically included in ISS activities.
- The non-binding nature of the Charter of Fundamental Rights that has prevailed until the adoption of the Lisbon Treaty considerably limited the possibilities of establishing legal basis for fundamental rights and freedom scrutiny. The examination of the ISS and *ISS in Action* communication, however, seems to suggest that these legal changes have not significantly inflected the degree to which fundamental freedoms and rights are taken into account in strategy-making activities, and raise questions as to the transcription into policy of the collapse of the pillar system.

1.1. Background

The past decade has witnessed the adoption of a plethora of EU legislative measures and policy initiatives aimed at countering organised crime and terrorism as evidence by the numerous actions plans, directives and framework decisions.

In the field of organised crime (OC), various instruments and tools have been elaborated and implemented, targeting the various activities encapsulated in the terminology 'OC' such as drug trafficking or cybercrime, but also targeting the proceeds of crime through a whole set of anti-money laundering regulations. Indeed, the two EU action plans (1997 and 2000), the JHA Joint Action (1998), the Tampere Conclusions (1999), the Hague Programme (2004), the Council Framework Decision on the fight against organised crime,

which replaced the 1998 Joint Action (2008), as well as the three Directives on money laundering (1991, 2001 and 2005) have provided the EU with a rather impressive arsenal.

In the field of terrorism, the EU has similarly adopted a wide range of instruments, with an intensification of activities after the 9/11 attacks in the New York and Washington, D.C. in 2001, and the Madrid (11/3) and London (7/7) bombings in 2004 and 2005. The Framework Decision on combating terrorism (2002), the Hague Programme (2004), the establishment of the position of a Counter-Terrorism Coordinator (CTC) in 2004, the EU Counter-Terrorism Strategy (and action plan) launched in 2005, the EU Strategy for Combating Radicalisation and Recruitment (revised in November 2008), the inclusion of terrorist financing in the anti-money-laundering strategy in the third Directive (2005) and the Stockholm Programme (2010) are initiatives that have paved the EU framework of actions.

Embracing both the fights against terrorism and organised crime, the issue of police and judicial cooperation has been at the core of European activities in both fields. More or less informal working groups, experts meetings and various committees have been set up in support of the EU's quest to fight OC, prevent terrorism and promote better cooperation and information-sharing.

In the field of terrorism, these include the TREVI Group created in 1976,[8] the Police Working Group on Terrorism (PWGT) created in 1979, the Terrorism Working Group (TWG) launched in 1992, the Working Party on Terrorism (COTER) established in 1997, the Counter Terrorism Group (CTG) established in 2001 and the Working Party on the application of specific measures to combat terrorism (CP 931) established in 2001. The position of a Counter-Terrorism Coordinator created in 2004 was established with the aim of coordinating the EU action in the field.

Against OC, the Working Party on Cooperation in Criminal Matters established in 1992 has been followed by the Multidisciplinary Group on Organised Crime (created in 1997, now replaced by the Working Party on General Matters, including Evaluations).

Specific groups dedicated to judicial and police information exchange and cooperation have also been set up: the Article 36 Committee (CATS, created in 1997), the European Police Chiefs Task Force (EPCTF) established in 2000, the Law Enforcement Working Party (LEWP) established in 2010, and now the Standing Committee on Internal Security (COSI).

Article 71 TFEU refer to the setting up of a "standing committee" on "operational cooperation on internal security", which is to be "promoted and strengthened within the Union", with the possible involvement of Union bodies, offices and agencies. Such a committee, known as COSI, "shall facilitate coordination of the action of Member States' competent authorities". Article 71 TFEU also state that: "The European Parliament and national Parliaments shall be kept informed of the proceedings" of COSI. An assessment of COSI's activities since 2010, as well as an analysis of its relation with other European bodies active in the field, will be developed further and in details within this study.

1.1.1. The analysis of the European fight against organised crime and terrorism: The state of the debate

The adoption of a plethora of EU legislative measures and policy initiatives aimed at countering terrorism and organised crime, such as decisions, framework decisions, conventions and the increasing number of bodies and agencies dedicated to security have established EU internal security as one of the most dynamic domains of EU policy-making. The density and the variety of EU tools, instruments and actors nevertheless have the

[8] For more on TREVI, see T. Bunyan (1993), "Trevi, Europol and the European State", in T. Bunyan (ed.), *Statewatching the new Europe: A handbook on the European State*, Statewatch, London, 1993.

effect of obscuring our understanding of the issues at stake. The genesis and evolution of the EU fight against OC and terrorism, if well documented, reveal various debates in the academic community. Among these debates, the following are worth underlining in order to shed a more critical light on the study of the EU ISS:

- The problematic definitions of OC and terrorism,
- The logic and trends of the fight against OC and terrorism,
- The focus on law enforcement capacities,
- The question of precise and effective knowledge on OC and terrorism and
- The cost of the fight against OC and terrorism in terms of civil liberties.

1.1.1.1. The problematic legal definitions of OC and terrorism

If the use of the terminology of 'OC' has now become commonplace in EU documentation dealing with JHA matters, it is worth recalling that debates arise when it comes to its legal definition.

As underlined by EU specialists in the field of judicial cooperation, thorny issues in JHA matters involve the legal definition of organised criminal groups as well as the fact that organised crime is treated differently by the criminal law system of each Member State.[9] The latest attempt to provide a definition of organised crime, to be found in the 2008 Council Framework Decision on the fight against organised crime, does not show any progress on that matter. Instead, **terms of definition remain very broad and highly flexible, and do not provide any legal certainty**. Furthermore, the absence of a clear definition creates a potentially very extensive scope of criminalisation of organised crime across the EU. The need for a clearer definition has been reiterated in the LIBE report on organised crime in the European Union.[10]

The legal basis of what constitute 'terrorist activities' in EU legislation encounters similar difficulties. The 2002 and amended version of 2008 Framework decision on Combating Terrorism aimed at providing a comprehensive definition of terrorism and provided a list of terrorist activities.[11] Numerous heated debates have taken place both in the academic community and within the civil society on such a list, which includes for instance the "public provocation to commit a terrorist offence". **Concerns in relation to the exercise of democratic rights**, such as the freedom of expression, have been raised.[12] Similarly, the original proposal from the European Commission to embrace trade union and protests as possible scope of EU anti-terrorism activities has led to a wide range of criticisms, related to the exercise of democratic rights.[13] Such concerns have led to very detailed

[9] V. Mitsilegas (2011), "The Council Framework Decision on the Fight against Organised Crime: What can be Done to Strengthen EU Legislation in the Field?", PE 453.195, European Parliament, Brussels; A. Scherrer, A. Mégie and V. Mitsilegas (2009), "The EU role in fighting transnational organised crime", PE 410.678, European Parliament, Brussels; V. Mitsilegas (2009), *EU Criminal Law*, Oxford: Hart Publishing, 2009; V. Mitsilegas (2001), "Defining Organised Crime in the European Union: The Limits of European Criminal Law in an Area of Freedom, Security and Justice", *European Law Review*, Vol. 26, pp. 565-581.

[10] S. Alfano (2011), "Report on organised crime in the European Union", PE454.687v04-00, European Parliament, Brussels.

[11] E. Dumitriu (2004), "The E.U.'s Definition of Terrorism: The Council Framework Decision on Combating Terrorism", *German Law Journal*, Volume 5, No. 5.

[12] S. Allegre (2008), "Human Rights concerns relevant to legislation on provocation or incitement to terrorism and related offences", European Parliament, Brussels, PE 393.283. See also the International Commission of Jurists (2008), "Briefing Paper: Amendment to the Framework Decision on Combating Terrorism – Provocation to Commit a Terrorist Offence" (www.un.org/en/sc/ctc/specialmeetings/2011/docs/icj/icj-2008-fd2007-650.pdf)

[13] See Statewatch Observatory dedicated to the EU anti-terrorism plans: justice and home affairs proposals, Statewatch, London (www.statewatch.org/observatory2d.htm).

publications that reiterate that the rule of law, as well as the freedom of thought and expression should never be sacrificed in the struggle against terrorism.[14]

In addition to these legal uncertainties and consequences, several scholars have questioned the trends followed in European and international regimes and argue that the European agenda is guided by unclear logic and understanding.

1.1.1.2. The logic and trends of the fight against OC and terrorism

From a careful analysis of the different steps taken at the European level against OC and terrorism, several gaps and inconsistencies have been underlined. Scholars have usefully pointed out that, for instance, **the EU has largely focused on some areas of OC and terrorism, while leaving aside other issues**. The fight against drug trafficking, money laundering, terrorist financing and prevention of radicalisation has led to an impressive set of decisions and regulations. However, important issues such as corruption, environmental crimes or corporate crime have been given fewer priorities. The EU is indeed quite shy in the area of corruption for instance. The adoption of the network contact point against corruption, as well as efforts made by the European Commission to understand the links between organised crime and corruption (as demonstrated in the Commission Staff Working Document of February 2008 on "An examination of the links between organised crime and corruption"), certainly constitute a step further in the EU strategy against corruption. However, while the EU has been extremely active in the adoption of anti-corruption standards with regard to the candidate countries wishing to become EU members, and with regard to the development of international anti-corruption standards, *internal* EU legislative action against corruption has not been as intense[15]. An efficient framing of a comprehensive anti-corruption policy by the EU institutions has been called on many occasion, and notably in the recently adopted LIBE report on organised crime in the European Union.[16]

As detailed below with regard to the EU ISS, the lack of consistency in the priorities set up in the EU fight against OC and terrorism is clearly demonstrated in the EU ISS. The ISS appears to be all-encompassing, and if the issues of economic crime or corruption are mentioned, they are cited together with sexual exploitation of minors and child pornography, money-laundering, terrorist recruiting, etc. **without clarification on the priorities given**, nor on the level of effort that will be displayed for each of the listed crimes.

1.1.1.3. The focus on law enforcement capacities

The focus on law enforcement capacities is another field of debate among criminologists, and **OC and terrorism are seen as areas in which law enforcement rather than prevention largely dominate**. According to a wide range of researchers, a strictly judicial and police perspective might not provide the best answer to cure criminality worldwide. Some insist notably the need to focus on alternative conceptions of security which emphasise the underlying conditions that produce crime in the first place.[17] According to them, the prevention and reduction of crime do not exclusively involve intervening on the risk factors before crime happens, but also addressing the social and economic roots that produce crimes, such as working and living conditions, social marginalisation and political frustrations.[18] Many emphasize the possibilities of developing

[14] See notably research published by the Council of Europe (2004) *"Apologie du Terrorisme" and "Incitement to terrorism"*. The reports highlight the different approaches to the phenomenon of public expression of praise, justification and other forms of support for terrorism and terrorists referred to as "apologie du terrorisme" and "incitement to terrorism".

[15] A. Scherrer, A. Mégie and V. Mitsilegas (2009), op. cit.

[16] S. Alfano (2011), *Report on organised crime in the European Union*, op. cit.

[17] A. Edwards and P. Gill (eds) (2003), *Transnational Organised Crime. Perspectives on global security*, London: Routledge.

[18] Council of Europe (2005), "Security and social cohesion: Deconstructing fear (of others) by going beyond stereotypes", Strasbourg: Council of Europe Publishing; K. Beckett and S. Herbert (2011),

more effective crime reduction strategies through structural social adjustments that differ from practical responses of the police.[19] Such arguments acquire a peculiar echo when analysing the EU's efforts in the field of crime prevention.

A thorough analysis of the EU documentation in the field of OC and terrorism indeed shows that when the issue of prevention appears, it is usually addressed from a law enforcement perspective. For instance, the prevention of OC is seen through the lenses of money laundering and terrorist financing and as a quest for a deterrence effect. Among the strands emphasised in the 2005 EU counter-terrorism strategy (prevent – protect – rescue – pursue) - the 'prevent' one singles out the issue of radicalisation.

In these examples, no provisions are given that address the roots of political violence or criminal conduct. In the EU policy process, it seems that alternative ways of thinking about crime prevention and crime reduction strategies that are not necessarily linked to law enforcement capacities are marginalised.

Inspirations could be taken, for instance, from work undertaken in other institutions, such as the Council of Europe (COE), which has addressed the causes of terrorism and launched various interesting initiatives. For instance, the COE has explored ways to reduce the tensions in today's society[20] by promoting inter-cultural and inter-religious dialogue[21] and carrying out activities in the fields of education, youth and the media, ensuring the protection of minorities, fighting intolerance, racism and social exclusion.

The limited scope of such discussions in the EU and the key role of the agencies composed of professionals recruited from coercive agencies to the detriment of a broader participation, as well as the extent to which the policy process at the European level is open and transparent will receive full attention in sections 2 and 3.

1.1.1.4. OC and terrorism: What sources for what knowledge?

According to experts and researchers, the main methodological problem when studying organised crime and terrorism is the question of sources and knowledge. **Great stress has been put notably on the difficulties to estimate underground activities, but also on the all-powerful role played by the police in the field**.[22] Many scholars have insisted on the fact that the available knowledge is often originating from sources that are not publicly available and statistics that cannot be checked because of a lack of transparency and classified sources.[23] This problematic reliance on police assertions is

---

Banished. The New Social Control in Urban America, Oxford: Oxford University Press; L. Wacquant (2007), *Urban Outcasts: A Comparative Sociology of Advanced Marginality*, Cambridge: Polity Press.

[19] G. Hughes and A. Edwards (eds) (2002), *Crime Control and Community: The new politics of public safety,* Cullompton: Willan Publishing; A. Crawford (ed.) (2009), *Crime Prevention Policies in Comparative Perspective*, Cullompton: Willan Publishing; M. Levi and M. Maguire (2004), "Reducing and Preventing Organised Crime: An Evidence-Based Critique", *Crime, Law and Social Change*, 41, pp. 397-469; M. Maguire (2004), "The Crime Reduction Programme: Reflections on the Vision and the Reality", *Criminal Justice*, 4, 3, pp. 213-238.

[20] See Conclusions of the Council of Europe conference on Why terrorism? Addressing the Conditions Conducive to the Spread of Terrorism, Strasbourg, 2007 (www.coe.int/t/dlapil/codexter/conf_whyTerrorism_en.asp).

[21] See Council of Europe's White Paper on Intercultural Dialogue, 2008 (www.coe.int/t/dg4/intercultural/Source/Pub_White_Paper/White%20Paper_final_revised_EN.pdf).

[22] M. Beare and R.T. Naylor (1999), *Major Issues Relating to Organized Crime: within the Context of Economic Relationships*, Toronto: Nathanson Centre, Law Commission of Canada; J.P. Brodeur and B. Dupont (2004), "Introductory essay: The role of knowledge and networks in policing", in T. Williamson (ed.), *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*, Chichester: John Wiley & Sons Ltd, pp. 9-33; G. Favarel-Garrigues (2001), « Concurrence et confusion des discours sur le crime organisé en Russie », *Cultures & Conflits*, 42, pp. 9-46.

[23] M. Beare (ed.) (2003), *Critical Reflections on Transnational Organized Crime, Money Laundering, and Corruption*, Toronto: Toronto University Press; J.P. Brodeur (2002), "Crime organisé", in L.

seen as a major obstacle to an independent assessment of OC and terrorism in Europe and elsewhere.[24] Furthermore, the apparent technicity that surrounds the tools developed at the EU level against terrorism and OC blurs the issues at stake and few would question and challenge the very foundations of knowledge on OC and terrorism. Thus, the knowledge challenge is central in the field of OC and terrorism, and this point will be addressed in detail below.

1.1.1.5. The cost of the fight against OC and terrorism in terms of civil liberties

The extensive use of intelligence capacities, the use of extradition and mutual legal assistance, the will to deprive criminal groups of the means by which they commit their crimes and to disrupt the technological support and opportunities offered by constant progress in telecommunication have constituted the main activities of the European mobilisation in the field of OC and terrorism. Such operational and legislative choices have led to methods and practices that are sometimes **inconsistent with the protection of civil liberties and individual privacy**. In that regard, it has been convincingly demonstrated that the fight against OC, reinforced by the current fight against terrorism, has allowed most governments to give legitimacy to some procedures that have previously encountered many obstacles, specifically when it comes to the respect of fundamental rights.[25] The reports of the UN Special Rapporteur Martin Sheinin on human rights and counter-terrorism have for instance well documented issues such as the definition of terrorism, the right to fair trial in terrorism cases, the impact of counter-terrorism measures on economic, social and cultural rights, the right to privacy in the age of counter-terrorism, the role of intelligence agencies and their oversight in counter-terrorism.[26] Similar official committees investigated illegal practices and the non-respect of European human rights standards, such as the Council of Europe Committee on extraordinary rendition chaired by Dick Marty (2005), or the EP Fava Committee on the role of the EU member states in the operation of CIA secret prisons (2006). The repeated attacks on fundamental rights in the post-11 September context have been the subject of numerous critiques, many of which have brought to light the following paradox: the growth of illiberal practices in liberal regimes.[27] This dark side of the fight against OC and terrorism is addressed in more detail below.

In order to provide a well-informed background to the study of the EU ISS, and in accordance with the LIBE concerns and the role of the European Parliament in security matters, both the knowledge challenge and the civil liberties challenge are detailed below.

1.1.2. The question of knowledge

As pointed out above, one of the major obstacles to assess OC and terrorism concerns the lack of information and the difficulty to obtain reliable data and statistics. EUROPOL's efforts to portray OC and terrorism in the EU in their reports provide an interesting example of such difficulties. The careful analysis of these reports does raise concerns that echo the need for reliable knowledge-based approaches to OC and terrorism.

Muchielli and P. Robert (eds), *Crime et sécurité. L'Etat des savoirs*, Paris: La Découverte, pp. 242-251.

[24] P. Van Duyne and T. Vander Beken (2009), "The incantations of the EU organised crime policy making", *Crime, Law and Social Change*, 51, 2, pp. 261-281; C. Fijnaut et al. (1998), *Organized Crime in the Netherlands*, The Hague: Kluwer.

[25] See Bonelli L. and al. (2008), *Au nom du 11 Septembre. Les démocraties à l'épreuve de l'antiterrorisme*, Paris: La Découverte; Neal, A. (2009), *Exceptionalism and the Politics of Counter-terrorism: Liberty, Security and the War on Terror*, London:Routledge.

[26] See website of the Office of the High Commissioner for Human Rights (www.ohchr.org/EN/Issues/Terrorism/Pages/SRTerrorismIndex.aspx).

[27] D. Bigo and A. Tsoukala (eds) (2008), *Terror, Insecurity and Liberty. Illiberal practices in liberal regimes after 9/11*, London: Routledge.

1.1.2.1. OCTA Report

The main concern found after a thorough analysis of EUROPOL 2009 and 2011 Organised Crime Threat Assessment (OCTA) reports relate to the methodology used.

The methodology of OCTAs is not very clear and explained in very broad terms. According to the reports, the OCTA is based on a multi-source approach, including law enforcement and non-law enforcement contributions (OCTA, 2009). The 2011 report does not provide further details:

> The EU Organised Crime Threat Assessment is the product of systematic analysis of law enforcement information on criminal activities and groups affecting the EU. It has been produced by strategic analysts in Europol's Analysis and Knowledge Unit (O2), drawing on extensive contributions from the organisation's analysis work files (AWFs), SCAN Team and external partners (Acknowledgments, p. 2).

In response to requests for more information on the methodology used to produce OCTA reports, the following reply was given:

> Multiple sources have been used for the development of the OCTA: Member States and third countries, International organisations, analytical work files, open sources.

This reply raised several further questions on this matter: Which third countries contribute to OCTAs? How to assess the reliability of their answers to the questionnaires? What kind of open sources are used? How to assess their reliability? The reply was as follows:

> Based on intelligence requirements, three questionnaires were submitted, on organised crime groups and clusters (using 11 indicators[28] and 70 questions), criminal activities[29] (using 14 indicators[30] and 54 questions), money laundering (7 indicators[31] and 27 questions).

This reply, in turn, raised additional questions: What are the intelligence requirements? Were the questionnaires the same for all the stakeholders? If not, on what basis the synthesis of data has been elaborated?

Our demand to access the questionnaires has been refused. However, we were told they have been approved by Member States through their representatives to the OCTA Working Group and then validated by Europol's Management Board. For 2011 OCTA, a sub-group was created within the OCTA WG to revise the questionnaires following Member States' needs and constraints.

In the absence of a methodological note accompanying each report, it is difficult to assess the robustness of the OCTA reports. Explanations on how the data were gathered (with an exhaustive list of participants), more details on what sources used (with a complete bibliography, notably for open sources), and an explanatory note on what choices, have been made to synthesise such data are essential in order to back up OCTAs' findings. These methodological precisions might help to further assess some problematic assertions contained in the reports, as detailed below.

---

[28] Clusters, Criminal Activities, International Dimension, Durability, Structure, Use of legitimate Business Structures, Influence, Violence, Countermeasures, Use of Specialists and Co-operation, Key Trends.

[29] Drugs trafficking, Fraud (including VAT fraud, smuggling of cigarettes and alcohol, and fraud in public tendering, Euro counterfeiting), Commodity counterfeiting and intellectual property theft, Trafficking in and exploitation of human beings, Facilitation of illegal immigration, Weapons trafficking, Environmental crime and any other crime types that are of specific interest to a single country.

[30] Overview, Number and Size, Co-operation between OCGs, Suspect Characteristics, Modi Operandi, Use of Specialist Expertise, Trafficking Routes, Use of legitimate Business Structures, Use of Corruptive Influence, Use of Violence, Facilitating Factors, Changing Trends, Pull Factors, LE Response

[31] Modi Operandi, Geographical Distribution, Use of Specialists, Use of legitimate Business Structures, Exploited Vulnerabilities, Most Used Sectors, Law Enforcement Policies.

Another issue arising when studying OCTAs is **the vagueness of the concepts used**. The use of the terminology of 'criminal hubs' in the 2009 report constitutes a good example. According to the report:

> A 'criminal hub' is a conceptual entity that is generated by a combination of factors such as proximity to major destination markets, geographic location, infrastructure, types of OC groups and migration processes concerning key criminals or OC groups in general. A criminal hub receives flows from a number of sources and spreads their effects in the EU thereby forging criminal markets and creating opportunities for the growth of OC groups that are able to profit from these dynamics (OCTA, 2009, p. 29).

But how to determine "major destination markets"? How are defined the types of OC groups in this context? What are the "migration processes" in this context? What are the 'flows' made of? The maps that accompany the depiction of these 'criminal hubs' does not provide any explanation on the methodology used to produce them. The extensive use of nationality/ethnicity-based features such as "West African", "Albanian speaking", "and Lithuanian groups" is another object of concern, as no explanation is given on how and why such groups have been singled out.

Furthermore, the **near absence of statistics is highly problematic**. Drug trafficking, fraud and smuggling are the exclusive categories sustained with data. In addition, the sections dedicated in the 2011 report on criminal activities such as weapons trafficking, property crimes or environmental crimes are far less detailed than drugs, illegal migration, etc. Does that mean that such activities are not of significant importance in the EU? The lack of methodological explanation certainly gives this impression.

1.1.2.2. Terrorism Situation and Trend (T-SATs) reports

Such annual EU reports are elaborated by analysts and experts at EUROPOL. Drawing on information provided and verified by EU Member States' competent law enforcement authorities. The reports compile data on failed, obstructed or successfully executed attacks as well as arrests pertaining to suspects of terrorism over the past year. According to TE-SAT 2010, eight Member States reported a total of 209 failed, foiled or successfully perpetrated attacks and the UK reported 40 during the same period of time (see Annex 2, p. 36). Only three 'Islamist' attacks have been reported (two in Denmark and one in Sweden), while France reported 84 'separatist' attacks, Spain 74 and Austria 1 (160 separatist incidents reported on the overall for 2010). The next largest category of attacks is under the heading of 'left-wing' with 20 failed, foiled or completed attacks in Greece, 16 in Spain, 7 in Italy, 1 in Czech Republic and 1 in Austria (45 incidents on the overall). Over the last year 2010, 14 Member States reported 566 arrests and the UK reported 45 charges (see Annex 3, p. 37). In 2010, 288 individuals have been tried for terrorism charges in ten Member States and 19 individuals in the UK (see Annex 4, p. 38).

As stated in the introduction and methodological parts of TE-SAT, the main unit of trend analysis provided in the report is the number of arrests and incidents perpetrated by terrorist groups. While the annual report certainly offers some valuable information, facts and figures, several comments should be highlighted, firstly on the quality of the data provided, and secondly, on the trends analysis themselves:

1. **Threat perceptions remain largely national in character and vary considerably**. Data provided by the EU Member States' competent law enforcement authorities depend largely on national history, views and classification of terrorist threats. Thus, EU terrorist threats portrayed in Europol's reports are partly biased. The fact that less than 50% of the Member States' law enforcement authorities have contributed to the 2010 TE-SAT suggests that **not all Member States feel equally concerned by terrorism**.
2. While the report is based on the compilation of failed, foiled and completed attacks per Member State and per affiliation, **the distinction between the number of failed, foiled and completed attack remains unclear**.

3. A completed or successfully executed attack may have different implications depending on the fatalities, casualties and social cohesion; the report does not provide such information.
4. The unfortunate recent attack in Oslo certainly demonstrates that **the magnitude of a brutal attack does not necessarily depend on the degree of organisation** of a terrorist group and can be carried out by a single individual. As such, the classical focus on stereotype terrorist groups whether they are 'Islamist', 'separatist' or 'left-wing', is problematic.
5. As stated clearly in TE-SAT 2010, data collected do not count various other criminal offences committed in support of terrorist activities. However, this information could give interesting details in order to provide a full picture of criminal activities alleged to sustain terrorist acts.
6. To count the number of individuals prosecuted on the charge of terrorist is not sufficient information per se; differences between judicial systems in the Member States are blurred and the **report does not reflect domestic specificities** regarding terrorism laws, nor does it offer a more precise view on the degree of involvement of the convicted individuals.
7. In comparison to the information provided in previous TE-SAT 2008 and 2009, there is an apparent decrease in the number of EU terrorist incidents in 2010. Over the previous years, it appears also that **few Member States are concerned by terrorist acts and they are primarily concerned with traditional local/national terrorism**, whether it is qualified as 'separatist' or 'left-wing'. Thus, the first key judgement of the report stating that "[T]he threat of attacks by Islamist terrorists in the EU remains high and diverse" is not convincing.

Threat assessment reports such as OCTAs and T-SATs have become central in policy decision-making (see below on Harmony Project). As such, it appears fundamental to **make sure that the methodology used in such exercises is made fully transparent, so it can be externally assessed just like any other knowledge process.** The knowledge challenge is all the more important given that policy decisions and budgets are decided upon these EUROPOL reports. According to the Communication from the Commission to the EP and the Council on "The EU Counter-Terrorism Policy: main achievements and future challenges" (2010),[32] over the period 2007-2013, a total amount of €745 million has been made available to support policies to counter terrorism and organised crime.

1.1.3. The question of civil liberties

The civil liberties challenge is of significant importance for the LIBE Committee and will be detailed throughout the present analysis. Taking stock of the numerous specific and significant studies undertaken in this field in the last decade, the following remarks can be brought forward:

1. As mentioned above, the **vagueness of the terminologies** of OC and terrorism, as well as their loose legal definition leads to legal uncertainties, problematic judicial aspects and over-criminalisation.
2. Furthermore, the **anticipative logic** gives priority to data collection, data exchanges and data analysis, which are highly sensitive activities in terms of civil liberties.

Terrorism and OC are indeed ambiguous terminologies with legal consequences. As carefully analysed by EU legal experts, the 2008 Framework Decision on OC attempted to reconcile two seemingly different objectives: to introduce a specific offence of participation in a criminal organisation, which is distinct from other association/membership offences in domestic criminal justice systems; and at the same

[32] Brussels, COM(2010)386 final.

time not to be too rigid and narrow in its definition of organised crime, by taking into account the view that criminal organisations do not always operate under a hierarchical structure, but may also operate in networks.[33] The result of this effort is a seemingly contradictory definition of a criminal organisation which has the potential to lead to over criminalisation, as the elements of a criminal organisation are defined very broadly and with flexible, ambiguous criteria. In this case, great discretion, with limited guidance, is left to the national legislator and judge to implement and interpret these provisions.

Furthermore, controversies around the terrorist 'watch lists'[34] provide a good example of the problematic evolution of the EU counter-terrorism strategy. **This evolution is not only questionable from a legal perspective, eventually disrupts the EU functioning as well and creates tensions between the European Court of Justice, the European Council and MS law enforcement services**. The two following cases illustrate these tensions:

1. In 2008, the European Court of Justice annulled an EU Council regulation and rejected European governments' implementation of the UN terrorist watch list, on the ground that it breaches fundamental rights.[35]
2. The jurisprudence of the European Court of Human Rights related to terrorism[36] illustrates striking differences between the EU and its MS. In 2010, the European Court of Human Rights officially ruled police 'stop and search' powers, under UK Terrorism laws, illegal for the second time, rejecting a government appeal. The Court referred to stop and search powers as not in "accordance with the law", and a violation of Article 8 of The European Convention on Human Rights – the right to respect for private and family life.

In the counter-terrorism field, numerous other examples of departures from the rules of law have been well documented.[37] Changes in the EU legislation and the hardening of legislation in EU MS have produced many studies and critical assessments of the EU strategy in the field. Many researchers consider that claimed threats need to be discussed in terms of the proportionality of the response and legal norms about the presumption of innocence. The importance of safeguarding fundamental values has been constantly underlined and addressed by various NGOs, academics, international bodies such as the Council of Europe[38], but also on numerous occasions by the European Parliament. Sophia Int'Veld usefully recalls in her report for the LIBE Committee that "counter-terrorism policies should meet the standards set with regard to necessity, effectiveness, proportionality, civil liberties, the rule of law and democratic scrutiny and accountability that the Union has committed itself to uphold and develop, and that assessing whether

[33] See A. Scherrer, A. Mégie and V. Mitsilegas (2009), op. cit.

[34] See Statewatch Report (www.statewatch.org/terrorlists/terrorlists.html).

[35] It indeed annulled the European Council Regulation which followed a UN Sanctions Committee decision by freezing the assets of Yassin Abdullah Kadi, from Saudi Arabia, and the Al Barakaat International Foundation of Sweden, part of the 'Hawala' banking system. See Guild, E. (2010), "*EU Counter-terrorism Action: A fault line between law and politics?"*, CEPS, Brussels.

[36] See the website of the UN Office on Drugs and Crime (www. /tldb/en/case-law-of-the-european-court-of-human-rights-related-to-terrorism.html).

[37] See the research undertaken within the CHALLENGE Project (Changing Landscape of European Liberty and Security), funded by the Sixth Framework Research Programme of DG Research (European Commission) (www.libertysecurity.org/). See also E.P. Guittet (2008), "Miscarriages of Justice and Exceptional Procedures in the War against Terrorism", Brussels: CEPS; E. Guild (2010) *EU Counter-Terrorism Action: A fault line between law and politics*?, op. cit.; A. *Neal, Exceptionalism and the Politics of Counter-terrorism: Liberty, Security and the War on Terror*, op. cit.

[38] See the related publications of the Council of Europe (2007) *The fight against terrorism - Council of Europe standards* (4th edition); (2005) *Human rights and the fight against terrorism –The Council of Europe Guidelines*.

these standards are met must be an integral part of an evaluation of all EU counter-terrorism efforts".[39]

Such legal uncertainties are enhanced by **difficulties caused by the extensive use of data and the promotion of an intelligence-led logic**. The 'data challenge' encompasses the collection of evidence and its admissibility, the use of financial information for the purpose of identifying and then neutralising the proceeds of crime, the use of intelligence data to anticipate terrorist attacks and the principle of exchange and availability. The questions of data availability and interoperability of databases have become central in the EU strategy against OC and terrorism. As underlined elsewhere, these two aspects of judicial and police cooperation are highly problematic, at different levels:[40] in addition to difficulties on the operational aspect (the supplementary work that will be needed, the heaviness of the management of data coming into the system and the time spent to deal with the other agencies' demands), and to the question of the role and mandate of EU agencies in the databases, the debate focuses particularly on reasons linked to the very legitimacy of the principle of availability and on its effects on civil liberties. Those debates insist specifically on the qualitative difference between data shared by intelligence services and repressive authorities (police, customs, judicial bodies), for which eligibility in front of a court is not the same, and for which credibility and veracity depend on the conditions in which the information was obtained. In order to function, the principle of availability supposes that there is an agreement on the categories of authorities that will have access to these data. As acknowledged by the LIBE Committee on several occasions, the need for safeguards for the protection of personal data becomes of critical importance.

1.2. The European Internal Security Strategy

The entry into force of the Lisbon Treaty and the adoption of the Stockholm Programme has spurred the adoption of a number of strategy documents on the further development of the AFSJ. The Internal Security Strategy is therefore one of several documents laying down orientations for the AFSJ. A first question, in this regard, concerns the objectives of a strategy. **What should a strategy do?** Is a strategy limited to the enumeration of key priorities and goals? Should it be a management-oriented document, providing empirical evidence of a need for action and establishing milestones and benchmarks for future assessments and evaluations? Is the adoption of a strategy a symbolic move, which serves mainly to promote the visibility of its drafters and ascertain their legitimacy to act in a given domain? **How strategic**, in other words, **is the EU's Internal Security Strategy?** Of interest, here, is the examination of how the EU ISS relates to other strategy documents dealing with internal security as well as with the AFSJ at large. How do the elements featured in the internal security strategy relate to the broader 'Lisbon cluster' of strategy documents? In particular, how is the articulation between security and freedom organised across this cluster? As recalled in the introduction to this study, the Stockholm Programme establishes that ensuring simultaneously the respect for fundamental rights and freedoms and guaranteeing security is the key challenge for the AFSJ, which must be addressed "in a comprehensive manner", with "[f]urther efforts needed in order to improve coherence between policy areas" (p. 7). We examine in turn:

- The general post-Lisbon strategic environment for the AFSJ (1.2.1.);
- The specific priorities listed in the Internal Security Strategy and the *ISS in Action* communication from the Commission (1.2.2.); and
- The relationship between the ISS and *ISS in Action* priorities and the other strategic documents constituting the AFSJ's post-Lisbon environment (1.2.3.).

[39] S. Int'Veld (2011), "Report on the EU Counter-Terrorism Policy: Main achievements and future challenges", Brussels: European Parliament, PE 460.953v02-00.

[40] D. Bigo et al. (2008), *The Field of the EU Internal Security Agencies*, Paris: l'Harmattan.

1.2.1. Strategy-making in the AFSJ: The Internal Security Strategy in context

1.2.1.1. Overview of EU strategy-making activities in the AFSJ

The devising of strategy documents laying down priorities for the AFSJ has proceeded at a sustained pace since the entry into force of the Amsterdam Treaty, starting with the Vienna Action Plan adopted by the European Council in December 1998 and the Tampere 'milestones' adopted in December 1999. Alongside the three multi-annual programmes of Tampere (1999), the Hague (2004) and now Stockholm (2009), strategy documents for the AFSJ have included:

1. **Managerial strategy documents**: General strategy documents in the AFSJ have been accompanied by a number of implementing documents preoccupied with the management of actions undertaken through the EU. Managerial strategy documents related to the Hague Programme include, for example, the Commission's "Ten priorities for the next five years Communication" and the joint Commission-Council "Action Plan implementing the Hague Programme" published in 2005, as well as the 2006 Commission Communication "Implementing the Hague Programme: the way forward" adopted together with the Commission's report on the programme's first year.[41]
2. **Issue-specific and topical strategy documents**: These are documents that focus either on a specific issue area or are adopted in relation to a specific event. The two categories, however, very often overlap. The adoption of a strategy document regarding a given issue area has often been used as a symbolic measure to demonstrate that specific incidents have been taken into account by the EU.
3. **Strategies relating to external relations and common foreign and security policy**: Some of these documents, such as the Commission's "Strategy for to the external dimension of the area of freedom, security and justice" and the Council's "Strategy for the external dimension of JHA" both adopted in 2005, follow from activities in JHA matters or espouse a JHA viewpoint. Others hail from altogether different policy areas. The best example here is the 2003:"European Security Strategy" (ESS) and 2008 Report on the implementation of the European Security Strategy, which have been drafted by the High Representative for the CFSP and his team, and include security considerations related to the AFSJ and its external dimension despite being instruments of the former second pillar.[42]

1.2.1.2. EU strategy-making activities and the question of change

This brief overview calls for three comments. Firstly, **the distinction between the different categories of strategy documents is unclear**. The Tampere, The Hague and Stockholm multi-annual programmes are a good example, since they are simultaneously priority-setting documents and managerial tools for programming AFSJ-related activities. This observation leads to a second comment, namely that the adoption of strategy documents regarding the AFSJ has been driven by **three interrelated patterns**:

1. A **planning-driven pattern**, which follows from agreed upon processes of review and strategic planning. Examples of this pattern mainly concern the multi-annual

[41] See respectively European Commission (2005), "The Hague Programme: 10 priorities for the next five years", COM(2005) 184 final, 10.5.2005; Council of the European Union (2005), "Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union", 9778/2/05, 10.6.2005; European Commission (2006), "Implementing the Hague Programme: The way forward", COM(2006) 331 final, 28.6.2006.

[42] See European Commission (2005), "A strategy on the external dimension of the area of freedom, security and justice", COM(2005) 491 final, 12.10.2005; Council of the European Union (2005), "A Strategy for the External Dimension of JHA: Global Freedom, Security and Justice", 14366/05, 11.11.2005; Council of the European Union (2003), "European Security Strategy", 8.12.2003; Council of the European Union (2008), "Report on the Implementation of the European Security Strategy – Providing Security in a Changing World", 17104/08, 10.12.2008.

planning of activities in the AFSJ and the succession of five-year work programmes starting with the Tampere milestones, followed by the Hague Programme and now continued with the Stockholm Programme. The process, of course, is not as streamlined as it may seem. Alongside managerial concerns with the organisation of EU activities regarding the AFSJ, competition between actors and concerns with symbolic gestures following developments considered as major events have been a consistent driving force behind the adoption of strategy documents.

2. A **competition-driven pattern:** The adoption of strategic documents has also been driven by the tensions between the different agencies, bodies and services involved in AFSJ policies. In the case of the AFSJ's 'external dimension', for one, the Commission and Council's strategic documents of 2005 were adopted almost simultaneously, with some key differences: while the Commission's contribution aimed, at least in principle, to develop simultaneously the freedom, security and justice dimensions in the EU's relations with third countries, the Council's approach has been centred more squarely on counter-terrorism, organised crime, trafficking and migration.[43] Strategy documents, in this case, are adopted not only to establish priorities, but also to promote conflicting agendas. Competition, furthermore, is not only an inter-institutional pattern but also involves intra-institutional controversies.

3. An **event-driven pattern**: The adoption of strategy documents has in some cases been justified as a reaction to specific developments framed as 'key events', even though they have taken place quite some time after such developments. This is the case, for example, of the EU counter-terrorism strategy adopted in December 2005 to "take into the next phase the agenda of work set out at the March 2004 European Council in the wake of the Madrid bombings" (Council document 14469/4/05, p. 6). This does not entail, however, that such documents foresee significant policy inflections. Among the key priorities singled out under the 'Protect' heading of the EU counter-terrorism strategy, for instance, are the introduction of biometrics in EU passports (already decided a year before with the adoption of Council Regulation (EC) 2252/2004 of 13 December 2004) or the establishment of the Visa Information System (VIS) and Schengen Information II (SIS II). The possibility of using the VIS for counter-terrorism purposes had been at the time under consideration since the earliest discussions on the issue in November-December 2001.[44] The SIS-II, on the other hand, could hardly be considered as a novel measure at the time, since its development had been considered since December 1996 within the Schengen Executive Committee.[45]

The survey of strategy-making activities in the AFSJ, in view of these patterns, **brings to the fore the question of possibilities for change in the trajectory espoused by the**

[43] For a general assessment on these issues in the studies submitted to the AFET and LIBE committees of the European Parliament, see S. Alegre, D. Bigo and J. Jeandesboz (2009), "External Dimension of the Area of Freedom, Security and Justice", PE 410.688, European Parliament, Brussels. For region-specific analyses, see inter alia T. Balzacq (2008), "Implications of European Neighbourhood Policy in the Context of Border Controls", PE 393.284, European Parliament, Brussels; K. Hailbronner (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to the United States of America", PE 348.589, European Parliament, Brussels; S. Lavenex and N. Wichmann (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to the Countries covered by the European Neighbourhood Policy (ENP)", PE 348.596? European Parliament, Brussels; p; Luif and H. Riegler (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to the Western Balkan Countries", PE 348.588, European Parliament, Brussels; M. Menkiszak, M. Jaroszewicz and M. Falkowski (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to Russia", PE 348.594, European Parliament, Brussels.

[44] See E. Brouwer (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System,* Leiden: Martinus Nijhoff, pp. 127-132.

[45] Ibid., pp. 71-116.

development of the EU's policies in this area over the past 20 years. This is all the more important as these activities have sustained the reinforcement of the security logic in AFSJ policies. This has not been done, however, by systematically opposing security, freedom and justice, but also by including security priorities under the headings of freedom and justice. The case that has attracted the most comment over the past few years, in this regard, has been the Hague Programme.[46] The programme's first and longest section on 'Strengthening Freedom' incorporates a number of measures on the contested issue of 'offshore processing' of asylum claims, on readmission policy, on border control with reference to the establishment of Frontex, on biometrics and the establishment of SIS II and VIS, and so forth. These measures, placed under the "Freedom" heading of the programme, all target third-country nationals. As some scholars have suggested here, freedom in the Hague Programme is envisaged as "the creation of a 'safe area without intruders'. Freedom is a tool for maximising security".[47] This logic is hardly specific to the Hague Programme: it can be found in the 1988 Palma document, informed the development of the Schengen cooperation, and has since been transposed and arguably 'recycled' in most strategy documents on the AFSJ.

1.2.1.3. The 'Lisbon cluster' of AFSJ strategies

The run-up to and the aftermath of the entry into force of the Lisbon Treaty, with the additional influence of the adoption of the Stockholm Programme, have also been a period of strategic activism. The 'Lisbon cluster' of AFSJ strategies includes:

1. **The Stockholm Programme and the related Commission Action Plan** on *Delivering an area of freedom, security and justice*: these contain the major updates regarding the implications of the entry into force of Lisbon for the AFSJ.
2. **Fundamental rights strategy documents**: these comprise the Commission's 2010 *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union,* as well as its 2010 *Comprehensive approach on personal data protection in the European Union*.
3. **Internal Security Strategy documents**: these comprise the ISS and the 2010 Commission's *ISS in Action* communication, as well as the more specific *Information Management Strategy for EU internal security*.

The question, of course, is whether these documents reflect a change from the trends identified in previous strategy documents. The emphasis placed on fundamental rights and freedoms in the latest strategy documents, as well as a number of organisational developments prior to the adoption of the Stockholm Programme (chiefly the break-up of DG JLS into DG Home and DG Justice), suggest that we might be seeing an inflection whereby security and freedom are being pursued simultaneously, rather than having the security logic 'colonise' the priorities related to freedom. Assessments of the Stockholm Programme, however, suggest that the focus adopted in the Hague Programme remains, albeit in a more attenuated form. The emphasis on a "Europe of rights" and a "citizens' Europe", which are the main headlines of the programme, focus on the freedoms and rights of persons holding the nationality of an EU Member State, whereas legal instruments, including the Charter of Fundamental Rights (CFR) and the European Convention of Human Rights (ECHR), as well as the case law of both the Luxembourg and Strasbourg courts acknowledge these freedoms and rights as held by all individuals,

[46] See e.g. S. Peers (2004), "Annotations on 'The Hague Programme' final version", London: Statewatch; T. Balzacq and S. Carrera (2005), "The Hague Programme: The Long Road to Freedom, Security and Justice", in T. Balzacq and S. Carrera (eds), *Security Versus Freedom? A Challenge for Europe's Future,* London: Ashgate, pp. 1-32.

[47] D. Bigo (2005), "Liberty, whose liberty? The Hague Programme and the Conception of Freedom", in T. Balzacq and S. Carrera (eds), *Security Versus Freedom? A Challenge for Europe's Future,* London: Ashgate, p. 36.

regardless of their nationality.[48] It is certainly with these issues in mind, and with the question of change at the forefront, that the EU Internal Security Strategy should be assessed.

1.2.2. The Internal Security Strategy and ISS in Action communication

In view of the elements provided on the practice of strategy-making in the AFSJ, the main questions raised by the EU Internal Security Strategy and the Commission's corresponding *ISS in Action* communication are the following. Firstly, does the EU ISS reflect what public policy analysis scholars term a 'path dependency' on security issues? In other words, **does it simply constitute a follow-up and recycling of past orientations, or does it alter the 'path' of EU activities in the field of internal security? Is it a strategy document as such, or a symbolic gesture, which seeks primarily to publicise the steps to be taken by the Council, and particularly its Standing Committee on Internal Security, in the future?**

1.2.2.1. The drafting of the EU Internal Security Strategy

The principle of an Internal Security Strategy, firstly, has been evoked for some time in EU AFSJ documents. The issue was first considered following the introduction by the European Convention in the Constitutional Treaty of the setting-up of a Committee on Internal Security (Article III-261). References to an Internal Security Strategy surfaced after the French and Dutch referenda rejecting the Constitutional Treaty, in Council discussions on the "Architecture of Internal Security" (Council document 7039/2/06) as well as in the process of reviewing the 2004 Hague Programme. In its 2006 communication on *Implementing the Hague Programme*, the Commission calls for the adoption of such a document in light of the developing EU and Member State initiatives in the field of counter-terrorism and critical infrastructure protection (p. 9). In the same period, the notion appears in discussions within the Council's working groups in the field of justice and home affairs following the publication of the first OCTA report and in the perspective of enhanced operational cooperation in this area. It was pursued in particular by the Finnish presidency, notably in its report on the review of the Hague Programme (Council document 15844/06).

The discussion on an Internal Security Strategy was relaunched in the Council in 2008. The French Presidency raised the question among delegations in the context of discussions on the structuring of operational cooperation in internal security matters (Council document 12390/08). The Stockholm Programme formalised the debate by calling upon the Council and Commission to devise an internal security strategy based on the following (pp. 60-61):

- Clarifying the organisation of tasks: between the EU and the Member States, but also between Member States (principle of solidarity), between EU agencies (emphasis on cooperation) and between the EU and regional initiatives/cooperation;
- Defining a general approach, which is to be horizontal and cross-cutting different issue areas, preventive and reflecting a proactive and intelligence-led logic;
- Respecting fundamental rights, international protection and the rule of law; and
- Promoting the importance of the EU's protection role towards citizens.

The Spanish Presidency earmarked the ISS as a key priority both in the JHA Council (Council document 5462/10) and in the meeting with the LIBE Committee in January 2010 (Council document 6048/10). A full draft was circulated to the delegations at the beginning of February 2010 (Council document 5842/10) and the final text was adopted

[48] See S. Carrera and E. Guild (2009), "Towards the Next Phase of the EU's Area of Freedom, Security and Justice: The European Commission's Proposals for the Stockholm Programme", Policy Brief No. 196, CEPS, Brussels.

by the JHA Council on 25 February (Council document 6870/10).

1.2.2.2. Priorities and principles in the EU Internal Security Strategy

The final ISS document is articulated as follows: it defines the key developments that are considered to constitute the main threats to the Union, outlines the main components of a European security model and establishes strategic guidelines for action. Keeping in mind that the ISS is a general document of an arguably symbolic, more than practical, dimension, these three points call for a number of comments.

The definition of key security challenges, firstly, is almost all-encompassing. **The ISS does not provide a hierarchy between the challenges it identifies, nor does it establish distinct priorities**. To a large extent, it reiterates the priorities featured in earlier strategy documents. Terrorism and "serious and organised crime", "in any form" for the former and "in its various forms" for the latter, are the first items on the list. Terrorism seems to include actions of significant impact ("devastating consequences"), but also recruitment which is assimilated with radicalisation and propaganda. Serious and organised crime includes various forms of trafficking (drugs, arms, and humans), smuggling of persons and economic crime, sexual exploitation of minors and child pornography, money-laundering and document fraud, as well as corruption. The lack of hierarchy between challenges and priorities appears most strongly when the ISS presents "violence itself" as a threat, and correlates internal security and civil protection by including natural and man-made disasters in the list of challenges. **At no point does the strategy define the scope and therefore limits of what constitutes an internal security issue.**

The components of the European security model outlined by the ISS reflect the same logic. The basic principles of the model are all-encompassing and include:

- Mutually reinforcing justice, freedom and security policies, respecting fundamental rights, international protection, the rule of law and privacy;
- Protection of all citizens, especially the most vulnerable and with particular attention to victims of crime;
- Transparency and accountability;
- Dialogue;
- Integration, social inclusion and the fight against discrimination; and
- Solidarity and mutual trust between Member States.

A number of questions can be raised as to the interaction between these principles. The first principle of mutually reinforcing AFSJ policies respecting fundamental rights, international protection, the rule of law and privacy reiterates the priorities of the Stockholm Programme. The European security model advocated by the ISS, however, twists this commitment in a significant way. Two examples are particularly striking. The strategy asserts, firstly, that "security is in itself a basic right" (p. 9), but does not clarify the implications of this assertion. What is meant by security in this context? This specification can be understood in two ways:

1. **Security is confused with safety**: Safety, in the constitutional tradition of a number of Member States, is taken to imply the freedom of the individual from harm, including from possible abuses of power from public authorities (for example in the context of national security policies). This is, generally speaking, the *Habeas Corpus* tradition, whereby freedom encompasses security.
2. **Security is equated with survival**: There can be no freedom if one is at risk of being killed. In this perspective, fundamental rights and freedoms can only be considered after security is ensured. Security becomes the principle, and freedom the exception. Security, here, is first and foremost the right to survival of an individual or a collective, which implies that a double hierarchy can be established:

between the most valued form of survival (e.g. an individual can perish in the name of collective survival), and between rights, with security at the top of the list. Security, in other words, encompasses freedom.

These two interpretations simplify a broader and more intricate ethical, legal and political discussion but they do show the need for more precision as to what is meant by defining security as a 'basic right' and by considering this prescription as the building block of a European internal security model. They raise an important question concerning a seemingly taken-for-granted point in AFSJ-related documents: Should security be considered as a right, or simply as a policy goal? By arguing for the former, the EU Internal Security Strategy follows in the steps of previous AFSJ strategy documents such as the Hague Programme. The ISS, secondly, defines transparency and accountability as important principles to enable security policies "to be easily understood by citizens, and take account of their concerns and opinions". Transparency and accountability here appear to involve the importance of reaching out 'pedagogically' to EU citizens. The two notions, however, have broader implications, including the oversight and scrutiny of security policies by parliamentary and judicial authorities, the obligation to demonstrate the impact and effectiveness of measures taken in the name of security, and the right of all citizens to access information about security policies among others.

The strategic guidelines laid out by the ISS, finally, raise similar issues. They feature a mix of general considerations and issue-specific discussions (judicial cooperation in criminal matters, integrated border management, innovation and training, external dimension of internal security). **The central articulation of the guidelines is between the emphasis on a proactive, intelligence-led approach, and the development of a comprehensive model for information exchange and operational cooperation**. The ISS formalises in this respect the main orientation of EU JHA policies since the adoption and entry into force of the Amsterdam Treaty. We will come back to this point below (2.2.3.) but it raises the question of whether the framing of internal security has actually evolved despite Lisbon's 'collapsing' of the pillar structure.

Just as with the other items featured in the ISS, several questions can be raised with regard to the strategic guidelines. A key point concerns the issue of prevention. A proactive and intelligence-based approach entails "a stronger focus on the prevention of criminal acts and terrorist attacks before they take place […] as well as procuring the evidence required for prosecution" (p. 11). While complementary at first inspection, the question of priorities is unavoidable here. Prevention can be based on information, while prosecution requires evidence collected according to specific procedures. Prosecution involves the articulation with justice, while prevention isolates internal security from issues pertaining to the other policies of the AFSJ. A further interrogation in this regard concerns the guidelines regarding the "effective democratic and judicial supervision of security activities". The inclusion of these considerations is undeniably an acknowledgement of the changes brought about by the Lisbon Treaty. In the meantime, no specific guideline to speak of is included in the ISS regarding the "effective consultation at all stages" of the European Parliament. Furthermore, while agencies such as EUROPOL and FRONTEX are mentioned at several points throughout the ISS, the section does not make any reference to the European Data Protection Supervisor (EDPS) (despite mentioning data protection and privacy issues in the section dedicated to the information exchange model) or the European Agency for Fundamental Rights (FRA).

1.2.2.3. The "ISS in Action" Communication from the European Commission

The November 2010 Communication of the Commission on the "ISS in Action" presents similar shortcomings. It defines five strategic objectives which overlap without matching entirely the key challenges and priority issues singled out by the ISS: countering serious and organised crime, counter-terrorism, countering cybercrime, border management, and resilience to crises and disasters (whether natural or man-made). A general interrogation, however, resides in the evidence that can justify the necessity and proportionality of the measures envisaged. The EU is "facing serious security threats that are growing in scale

and sophistication", argues the communication in its opening statement, but the remainder of the document offers very little in terms of a hierarchy of priorities and justifications for the course of action proposed. In the case of "serious and organised crime", for example, the communication resorts to the same enumeration as the ISS, but one is tempted to ask whether drugs, arms and human trafficking can be met with the same measures as burglaries or car thefts. Accordingly, the communication does not offer any definition of the scope and limits of internal security. One outcome of this approach **seems to be the 'recycling' of earlier policy initiatives under different headings,** a trend that was discussed earlier in relation to the EU's counter-terrorism strategy. The first concrete action envisaged regarding serious and organised crime, for instance, is a proposal for the establishment of an EU Passenger Name Record (PNR) system. This is expected to enable the identification and dismantling of criminal networks and, argues the Commission, to "prevent and prosecute terrorist offences and serious crimes" (p. 5). The discussion on the EU PNR, however, is hardly new. Furthermore, it was initially framed as a counter-terrorism measure, not as a measure against organised crime. **The combination between the lack of evidence, supporting the necessity of envisaged measures, and the tendency to 'recycle' past initiatives under a new heading raises, paradoxically, the question of the adequacy of the strategic priorities for EU internal security, and underlines the problems stemming from the multiple definitions of internal security, its scope and limits as a policy area.**

Another interrogation, in this respect, involves the articulation between internal security and the other policy areas of the AFSJ. The communication frames EU internal security policies as being based on common values and refers both to the EU Charter of Fundamental Rights and to the Commission's strategy for its implementation. It departs in this respect from the Internal Security Strategy itself, which is limited to generic references to fundamental rights and freedoms. However, despite the Commission's commitment, in its Action Plan on implementing the Stockholm Programme, to a 'zero tolerance policy' regarding violations of the Charter of Fundamental Rights, the *ISS in Action* does not seem to regard the transposition of this policy in the field of internal security as a strategic objective. This observation raises an issue of consistency in the priorities pursued by the Commission, and on the actual communication between the Commission's directorates general.

A driving question in the present analysis of the EU's Internal Security Strategy has been whether it constituted an inflection from past trends in the AFSJ. The elements provided above suggest that both the EU ISS and the Commission's *ISS in Action* communication reflect a tendency to reiterate past orientations and to reframe past initiatives. In this regard, the Internal Security Strategy appears more as a symbolic move, to be understood in the context of the entry into force of the Lisbon Treaty where some actors have felt the need to reinstate their prerogatives and influence over internal security matters. The apparently piecemeal and patchy set of priorities and guidelines formulated in the EU ISS has more to do with a lack of agreement over the upcoming orientations of the AFSJ, both between the institutions and within. Controversies over security priorities lead to the adoption of not a minimum common denominator but a maximal heterogeneous common one, which in this case is composed of the perspectives that have been adopted in the past. While legally written out of the treaties, then, the outlook embraced since Maastricht and embodied in the setting-up of the third pillar appears to remain predominant in the practices of strategy- and policy-making linked to the issue of internal security in the EU. **This should not be taken as a form of reluctance effect change, but rather as an incapacity to alter courses of action previously agreed upon, based on the difficulty to find an agreement on new orientations.**

1.2.3. Conclusion - The ISS and the post-Lisbon AFSJ strategic environment: The lack of articulation between security and freedom

The observations presented so far suggest that a key issue with regard to the strategic objectives and guidelines on EU internal security in the post-Lisbon context is the articulation between security, freedom and justice. This is hardly a novel issue, but it does

raise a number of questions.

Until the entry into force of the Lisbon Treaty, the pillar structure of the EU was held responsible for the noticeable discrepancies between the different components of the AFSJ. The existence of the third pillar was used as a justification for the isolation of internal security policies from parliamentary and judicial checks and balances. Arguments following from this logic included the non-binding nature of the Charter of Fundamental Rights, which was supposed to deprive fundamental rights and freedom scrutiny of a legal basis. This has not, however, prevented the ECJ from adopting rulings on Third Pillar matters, establishing its competence and analysing the legal effects of Third Pillar acts. In important cases such as *Pupino*, *Segi* or *Advoocaten voor de Wereld*, the ECJ established that general principles of Community law, and particularly Article 6(2) TEU which makes explicit reference to the protection of human rights, applied to Third Pillar acts.[49] In the case of counter-terrorist policies, for example, the Court of First Instance in Luxembourg ruled in a landmark decision of 12 December 2006 that the inscription by the Council of an organisation on the EU's 'terror list' violated the right to a fair hearing and to effective judicial protection, among others.[50]

The examination of the ISS and *ISS in Action* communication, however, seems to suggest that these legal challenges have not significantly inflected the degree to which fundamental freedoms and rights are taken into account in internal security activities, and that the collapse of the third pillar has not been transcribed into policy. Such a development cannot be expected to happen overnight, clearly, and this is why the Lisbon Treaty establishes a transition period for adaptation until 2014. The problem here is that the abovementioned strategies are forward-looking documents which purport to define future, medium- to long-term priorities. No concrete steps are envisaged to enforce the disappearance of the pillars and the requirements stemming from the fact that the EU consists of an area of freedom and justice as well as of security. **It seems, rather, that the European security model advocated in the ISS and the *ISS in Action* communication supports an all-encompassing definition of internal security and a restrictive definition of the articulation between security, freedom and justice, where security stands as the main priority.** This echoes largely similar findings underlined in recent reports on the EU ISS.[51]

The persistence in all but name of the third pillar can be illustrated in various ways. The trend has been sustained, for example, by the rush to adopt key initiatives before the entry into force of the Lisbon Treaty. A case in point, here, is the EUROPOL decision. The lack of articulation between strategic documents adopted after Lisbon is another instance. The EDPS made this point in a recent opinion on the *ISS in Action* communication, issuing a call for "a comprehensive and integrated approach at EU level […] In more general terms, this approach of '*linking the strategies*' if taken on board in the future actions would show that there is a vision at EU level when it comes to *EU strategies* and, that these strategies, and the recently adopted Communications which elaborate on them, are closely interlinked" (p. 5). The next chapter will show how the trend is also sustained in practice, through the activities of the different actors involved in EU internal security.

To wrap up the examination of EU strategy-making activities in internal security following the entry into force of the Lisbon Treaty, it is important to point out that the

[49] See for an overview S. Peers (2007), "Salvation out of the Church: Judicial Protection in the Third Pillar after the *Pupino* and *Segi* judgements", *Common Market Law Review*, Vol. 44, pp. 883-929.

[50] CFI, T-228/02, *Organisation des Modjhahedin du people d'Iran v. Council of the European Union*, 12.12.2006. On fundamental rights implications of the EU's counter-terrorism strategy, see F. Geyer (2007), "Fruit of the Poisonous Tree: Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy", Working Document No. 263, CEPS, Brussels.

[51] M. Busuioc and D. Curtin (2011), "The EU Internal Security Strategy, the EU Policy Cycle and the Role of (AFSJ) Agencies. Promise, Perils and Pre-requisites", PE 453.185, European Parliament, Brussels ; E. Guild and S. Carrera (2011), "Towards an Internal (In)security Strategy for the EU?", CEPS, Brussels.

considerations proposed above involve more than technical issues of consistence and coherence among policy initiatives. They touch upon the overall functioning of the EU institutional system, firstly. The perpetuation of third pillar practices prevents the establishment of the full scope of checks and balances available in other policy domains. The absence of specific provisions regarding the involvement of the European Parliament in internal security policy-making is the most striking feature of this trend. It also raises questions as to the possibilities available to review and possibly limit or reframe EU activities in this area, if the only available criterion of assessment is of a wide and all-encompassing notion of internal security.

2. ACTORS AND AGENCIES OF EU INTERNAL SECURITY: STATE OF PLAY AND CURRENT TRANSFORMATIONS

KEY FINDINGS

- The extent to which the ISS promotes a policy process ensuring the proper functioning of the EU system of checks and balances and guaranteeing democratic accountability is not self-evident. The analysis of the work methodology adopted by COSI highlights a lack of monitoring arrangement involving the European Parliament. Additionally, COSI's methodology does not clearly lay down provisions for independent or external evaluations of the information and analyses leading to the development of internal security policies.
- Moreover, and despite the commitments laid out in the Stockholm Programme in this respect, bodies in charge of freedoms and rights (such as the FRA, the EDPS, the Article 29 Working Party) are not systematically included in internal security activities, in particular in COSI's activities.
- The review of the current players in the field of security indeed highlights that EUROPOL and FRONTEX have benefited the most from the orientations encapsulated in the ISS. These two agencies appear to be gaining an increasingly central role in the collection, analysis and processing of information, and in the field of risk analysis and threat assessment.
- The two other main JHA agencies, CEPOL and EUROJUST appear in a much weaker position. Furthermore, some EU agencies (such as the CTC, OLAF, and SitCen) are not so clear in the context outlined by the ISS.
- There are grounds to promote further the inclusion of bodies such as the FRA, the EDPS, the Article 29 Working Party or the European Ombudsman. Along 'traditional' bodies in the European internal security landscape, EU freedoms agencies now also have a voice in the issues associated with the ISS.

This chapter investigates the current state of play and transformation of the EU internal security landscape and the relations between its actors, namely the EU agencies, bodies and services in charge of internal security. **What has been the impact of the entry into force of the Lisbon Treaty and the adoption of the EU Internal Security Strategy?** To provide an order of comparison, Figure 5 in the Annex outlines the EU internal security landscape before the entry into force of the Lisbon Treaty.

The question of whether the relations between, and the activities of other agencies, bodies and services in the field of EU internal security have been influenced by the entry into force of Lisbon and the adoption of the EU ISS is central. If the examination of recent strategy-making activities related to the AFSJ suggests that the collapse of the pillar system has not been fully reflected, is it possible to reach similar conclusions when looking at the state of play in the current EU internal security landscape? In this respect, it is important to embed the analysis of the working structures, agencies, bodies and services dealing with EU internal security within an examination of the overall inter-institutional context in which they operate. The current emphasis on coordination and cooperation as the key driving concepts of EU internal security policies limits the degree to which centralisation at EU level can occur. By looking at the relations between agencies,

bodies and services, however, it would seem possible to identify the various poles around which these networks of relations are organised, and to identify the most predominant.

The following pages survey the transformations that occurred in the European Commission and the Council (with a focus on the Standing Committee on Internal Security – COSI). It then reviews the main EU agencies involved in the EU's internal security policies, starting with the two agencies that appear to have benefited the most from the ISS, EUROPOL and FRONTEX. CEPOL and EUROJUST are then examined, as well as the other bodies in the field that have been less addressed in the ISS, such as the Counter-terrorism Coordinator, OLAF and SitCen. The section finally gives an account and an assessment of the working between these agencies, bodies and services.

2.1. The Commission: the transformation of DG JLS

The transformations experienced by the European Commission services in charge of the AFSJ, which saw the splitting of the former Directorate-General for Justice, Freedom and Security (DG JLS) into DG Home and DG Justice with effect from 1 July 2010, raises in this regard the question of change among the other agencies, bodies and services involved in the AFSJ. **The reshaping of the Directorate General for Justice, Freedom and Security is a direct outcome of the Lisbon Treaty and can be seen as a positive sign in the evolution of the European internal security landscape**. It is true that the division does not result in great changes of personnel and therefore could be seen as just an internal reshuffle. As matter of fact, the previous DG JLS staff has been split almost equally between the two new entities. They still share central services including human resources, IT, budget and auditing controls (principle of a shared resources Directorate).

However, the splitting of DG JLS, together with the creation of two separate commissioner portfolios, purportedly reflects an effort on the European Commission's side to take into account the new legal and institutional environment deriving from the entry into force of the Lisbon Treaty and the accrued visibility of issues of fundamental freedoms and rights following the transformation of the Charter of Fundamental Rights into a legally binding text. The division of DG JLS also reflects the division of work in the central administrations of most EU Member States, where responsibility for internal affairs and justice is commonly split between different ministries as a consequence of the well-established principle of separation of powers. From now on, DG Justice is in charge of civil and criminal justice, data protection, fundamental rights and citizenship and, since January 2011, equality, while DG Home is responsible for other major policy areas, such as terrorism, organised crime, cybercrime, immigration, asylum policy and border security.

This division into two separate portfolios is the result of long and strong discussions inside and outside DG JLS on how the work undertaken might have been too much focused on security and immigration at the expense of justice. One major element in these debates has been that the structure of the directorate was maybe not conducive to handling justice issues appropriately and in the way that they are dealt with by most member states governments. It was felt there was a need for a split of the DG and of the tasks falling within its remit in order to avoid any potential conflicts of interest between justice and security issues. The key argument developed has been that separation of powers should be a European standard in order to improve the checks and balance of any policy and to prevent any potential serious jeopardising of fundamental rights. On the other side of the debate, any split of the directorate was seen as a problematic move because there was a need to keep security, justice and migration under the same roof in order to increase the efficiency in the responses to these challenges.

This tension has long-standing roots. It reflects the inter-institutional disagreements that followed from the introduction of the split between the First and Third Pillar in the Treaty

of Maastricht and the tensions and compromises that informed the establishment of Title IV EC in the Treaty of Amsterdam. It also reflects the difficult history of DG JHA, later DG JLS, which was established after the appointment of the college of Commissioners presided by Romano Prodi, by bringing together officials from the JHA 'task force' originally created in 1993 within the Commission Secretariat and officials who had previously been working on freedom of movement issues within the services dedicated to the internal market. The idea of a division of the DG has grown steadily since then, while the area of freedom, security and justice became increasingly central in the work of the European Commission and while the directorate grew from one of the smallest to one of the most important. The notion of maintaining the services in charge of justice, freedom and security within the same DG was reinforced following the adoption of the Hague Programme. As the newly appointed Commissioner for Justice, Freedom and Security Franco Frattini commented shortly after, "The principles of Freedom and Security are inextricably linked. The symmetry among these concepts is in fact the very basis of the creation of an Area of Justice, Freedom and Security".[52]

The perspective of the adoption of the Stockholm Programme and of the entry into force of Lisbon, together with the apparent emphasis that these two developments placed on the need to strengthen the rights and freedoms of European citizens,[53] contributed to reshaping this view. In her opening remarks during her hearing in front of the European Parliament's LIBE Committee, Viviane Reding argued for instance: "I believe that during the past decade Europe's policies have too often focused only on security and neglected Justice"[54].

What are the effects of the division? It might be too soon to reflect on the achievements and shortcomings of the freshly split DGs. First of all and on the recommendation of Commission President Jose Manuel Barroso, the division of DG JLS has been accompanied by several rotations of senior staff (under the principle of mobility for senior managers) and contributed to an important modification of the portfolios within the College of commissioners. The two new DGs, however, were kept on the same premises. In a number of cases, such as the treatment of Roma people, data protection or the use of the European Arrest Warrant, the creation of two separate portfolios and two distinct directorate generals has enabled a more pluralistic debate on matters related to internal security. The practical and logistical evolution of the split of the DG, as well as practices of cooperation between the two commissioners certainly deserve full scrutiny in the coming months and years. Such shifts in the Commission's ways of working are nonetheless already symbolically significant. While it is important to highlight the continuities before and after the splitting of the DG JLS on AFSJ policies, **this reallocation in terms of symbolic power relations gives some effective grounds to the claims that fundamental rights are a central preoccupation of the Lisbon Treaty**.

2.2. The Council: The establishment of COSI and changes to the working structures

The main transformation experienced within the Council in the field of internal security, following the entry into force of the Lisbon Treaty, has been the establishment of the Standing Committee on Operational Cooperation on Internal Security (COSI). The

[52] Franco Frattini, Intervention at a conference on The Hague Programme: A Partnership for the European Renewal in the Field of Freedom, Security and Justice, organised by the Centre for European Policy Studies, Brussels, 14 July 2005.

[53] See the Commission's communication of June 2009, "Communication on an area of freedom, security and justice serving the citizens", COM (2009)262 final, Brussels, 10 June 2009.

[54] Viviane Reding, "Opening remarks at the European Parliament Hearing in the Committee on Civil Liberties, Justice and Home Affairs (LIBE)", European Parliament Hearing, 11 January 2010.

following sections provide elements of background to understand the creation of COSI, survey the changes introduced in the Council working structures as a result, and examine some of the transformations associated with the proceedings of this new Committee, with particular attention to the so-called EU 'policy cycle' in internal security (Harmony project).

2.2.1. COSI: Background

2.2.1.1. Article III-261 of the Constitutional Treaty

The concept of COSI was formally introduced in 2004 in the Treaty establishing a Constitution for Europe. Article III-261 establishes that "a standing committee shall be set up within the Council in order to ensure that operational cooperation on internal security is promoted and strengthened within the Union" with the possible involvement of Union bodies, offices and agencies, and keeping the European Parliament and national Parliaments informed of the proceedings. It "shall facilitate coordination of the action of Member States' competent authorities", without prejudice to the dispositions contained in Article III-344 on the remit of COREPER.

2.2.1.2. The Lisbon Treaty and Council Decision 2010/131/EU

The Lisbon Treaty introduced a number of changes in the provisions concerning justice and home affairs and the organisation of policy- and decision-making in this domain. Article 71 TFEU (ex Article 36 TEU) establishes the Standing Committee on Internal Security on the model of Article III-261 of the Constitutional Treaty. The replacement of Article 36 TEU by Article 71 TFEU deprives the former *Comité de l'Article Trente-Six* (Article 36 Committee, CATS) of a Treaty legal basis. It is flanked by Article 72, which specifies that the dispositions contained in Title V TFEU "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security" and Article 73 TFEU which establishes that Member States remain solely competent for matters of national security.

On 25 February 2010, the Council adopted Decision 2010/131/EU on setting up the Standing Committee on operational cooperation in internal security. The remit of COSI is:

- To "facilitate and ensure effective operational cooperation and coordination under Title V of Part Three of the Treaty, including in areas covered by police and customs cooperation and by authorities responsible for the control and protection of external borders" (Article 3(1)). COSI's remit also comprises judicial cooperation in criminal matters when relevant for operational cooperation;
- To "evaluate the general direction and efficiency of operational cooperation" (Article 3(2)); and
- To assist the Council with regard to the provisions of Article 222 TFEU (the 'solidarity clause').

Two areas are excluded from COSI's remit: the Committee is not competent for conducting operations (Article 4(1)) and it is not to participate in the preparation of legislative acts (Article 4(2)). Council Decision 2010/131/EU further confers upon COSI the responsibility to "help ensure consistency" in the activities of EUROJUST, EUROPOL, FRONTEX and "other relevant bodies" which may be invited to attend the Committee's meetings "as observers" (Article 5). Finally, Article 6(2) establishes that the Council "shall keep informed the European Parliament and the national Parliaments of the proceedings of the Standing Committee".

2.2.2. Ongoing debates and challenges

2.2.2.1. Changes to the Council working structures in the area of internal security after Lisbon

The establishment of COSI and the replacement of Article 36 TEU by Article 71 TFEU have led to a number of changes in the Council's working structures in the area of internal security. The replacement of Article 36 deprives the Council of the centrepiece in its decision-making procedure since the entry into force of the Amsterdam Treaty, the Article 36 Committee. The most notable changes in the Council working structures are as follows (see also **Table 1 and 2 in the Annex**):

- **COSI takes over the operational side of the matters previously discussed in CATS and the Standing Committee on Immigration, Frontiers and Asylum (SCIFA):**
  - Regarding CATS: COREPER decided in November 2009 that the Committee would continue its meetings until 1 January 2012, at which point its utility would be evaluated. In the meantime CATS is to concentrate on strategic-level matters where COSI is not able to contribute and on legislative work (Document 16070/09).
  - Regarding SCIFA: SCIFA was initially established in March 1999 (Document 6166/99) for a five-year transitional period. It was extended by COREPER in March 2004 for a further two years (Document 7440/04) and in March 2006 until a general review of the Council's JHA structures is undertaken (Document 7606/06). In November 2009, COREPER decided that SCIFA would continue its meetings until 1 January 2012.
- A number of changes have also been undertaken at working party level:
  - **Discontinuation of CIREFI**, reflecting the progressive takeover of this working party's tasks by FRONTEX. SCIFA will remain in charge of several aspects of CIREFI's remit, including the management of the network of Immigration Liaison Officers (ILOs).
  - **Creation of a single structure in charge of Schengen matters**: The Working Party for Schengen matters replaces the working parties previously in charge of SIS (SIRENE and SIS-TECH working parties), of Schengen evaluation and the Schengen *acquis*.
  - **Creation of a single structure for police cooperation matters**: The working parties on police cooperation and on EUROPOL are merged within the new Law Enforcement Working Party.
  - **Discontinuation of the Multidisciplinary Group on Organised Crime (MDG)**: The MDG has been relabelled Working Party on General Matters and takes over the tasks of the Working Party on Collective Evaluation.
  - **Formalisation of *ad hoc* structures**: This concerns the JAI-RELEX group, the Ad hoc working party on fundamental rights and citizens' rights, and the Ad hoc group on information exchange.

Thus three-fold handling of policy-making in the field of internal security appears to be aimed at simplification, efficiency and accountability. However, while some measures appear to bring about a clarification and streamlining of the Council's working structures in the field of internal security, **a number of issues have been left pending**, particularly with regard to CATS and SCIFA. CATS, firstly, has lost the legal basis that gave it both its name and remit. The division of work between SCIFA and COSI, however, is unclear insofar as SCIFA remains in charge of some operational aspects, such as matters concerning the networks of immigration liaison officers that it took over from the now-defunct CIREFI. The criteria that will inform COREPER's evaluation regarding the future of these two committees remains at this stage undefined. **Would a phasing out of**

CATS and SCIFA entail the *de facto* expansion of COSI's mandate beyond its current operational remit and into more strategic matters, including legislative work? Is the distinction between operational matters, on the one hand, and legislative matters, on the other, so clean cut as to provide appropriate guidelines for the work of COSI? The question is all the more stringent as there seems to be little agreement among Member State governments on the issue, with some, for example the United Kingdom, clearly expressing their interest in promoting 'lean' working structures in the Council (which would entail the discontinuation of CATS and SCIFA and the expansion of COSI's mandate), while others remain attached to the continuation of these two groups. Furthermore, as detailed below, the role, mandate and working methods of COSI needs clarification.

2.2.2.2. A committee in search of a constituency and priorities

COSI has been active for a year and a half, but its constituency remains unclear. The initial rationale was that COSI should be a meeting place for senior law enforcement officials from the Member States. To that effect, COREPER foresaw the introduction of a statement on the composition of the Committee in the minutes of the Council meeting adopting the COSI Decision, establishing that its membership would be 'capitals-based', with Brussels-based support provided through the COSI support group (Document 5949/10). Member State representatives have not embraced this orientation in a uniform fashion. In its initial meetings, COSI did bring together a number of senior law-enforcement and Ministry of Interior representatives from some Member States, including director-level officials of security agencies (e.g. the UK's Serious Organised Crime Agency - SOCA) and ministerial cabinet staff and advisors. Other delegations remained content with sending Brussels-based personnel. The situation has created tensions among Member State delegations, which has seen some (e.g. France) limiting the seniority of their representatives in the Committee. This observation should support a nuanced evaluation of COSI's claimed undertakings and achievements.

Furthermore, a brief analysis of the workflow of COSI since its inception highlights the fact that the new Committee's priorities remain broad and unclearly organised at this stage.

The first meeting of COSI took place in March 2010. A preliminary assessment of priorities was drafted jointly by the Spanish, Belgian and Hungarian Trio of Presidencies and tabled in May 2010. The so-called M.A.D.R.I.D. report (Main Assessment and Description Report for Internal Debate) is however a broad document, identifying every issue from organised crime to failed states to civil protection as a possible concern for COSI.

The Committee's first work programme was structured by the Belgian Presidency, drafted together with the upcoming Hungarian Presidency, and adopted at COSI's fourth meeting in September 2010 (Council document 13871/10 for outcome of proceedings, 13084/10 for the work programme). The initial 12-month work programme (summarised and contrasted with the current 18-month work programme in **Table 3 in the Annex**) can be distributed between the following categories:

- Organisational questions: These include the EU policy cycle (Harmony Project, see below), the Internal Security Strategy, the coordination mechanism for joint operations, the financing of operational cooperation (Internal Security Fund), the coordination of work between EU JHA agencies, and the interactions between internal and external security.
- Topical matters: These include organised crime, drugs and arms trafficking, measures against the PKK organisation, the control of external borders and migration control as well as the discussion of the solidarity clause incorporated in the Lisbon Treaty.

Based on the new 18-month work programme of COSI, organisational issues are likely to remain a core set of issues for the Committee, particularly the follow-up to the 'EU policy cycle' in the internal security project, operation co-ordination and co-ordination between

EU agencies. The topical matters considered so far are mostly the continuation of previously adopted initiatives. With regard to external border control and migration control, for instance, the main focus of COSI's work has been the "29 measures for reinforcing the protection of the external borders and combating illegal immigration", which were adopted in the JHA Council's February 2010 Conclusions (Council document 113065/10) as a follow-up to measures such as the European Pact on Immigration and Asylum and the Global Approach to Migration.

It is by all means too early to propose an assessment of COSI's priorities. One element that stands out, however, is that the Committee's establishment **is in the process of redefining the organisation of the circulation and assessment of information about EU operational activities in the field of internal security**. A pattern seems to be emerging, for instance, whereby the EU JHA agencies are reporting systematically to COSI regarding their operational activities. A recent example of this is the joint report circulated by EUROJUST and EUROPOL to the Committee, where the two agencies seek to demonstrate the success of their cooperation and the 'added value' that it can bring to operational activities in the field of EU internal security (Council document 9387/1/11). The process is two-sided. On the one hand, COSI's work on the EU 'policy cycle' in internal security has placed it in charge of a number of programmatic activities such as devising Operational Action Plans (OAPs, see next point). On the other, EU JHA agencies seek to promote their own image and way of working as an important contribution to internal security policies. Hence in the aforementioned report, the agencies invite COSI "to recommend that this kind of cooperation is included in the Operational Action Plan for each of the EU priorities in the fight against organised crime" (9387/1/11, p. 2). More broadly, cooperation between EU JHA agencies has been a focus of COSI activities since its inception, following the request made to the former by the Swedish Presidency at the end of 2009 to strengthen their joint activities. COSI is therefore currently the main recipient of the reports concerning this cooperation and of the recently drafted 'scorecard' which evaluates the process (see Council document 5675/11 for the latest report, Council document 5676/1/11 for the scorecard).

2.2.2.3. A committee in search of a work methodology: The Harmony Project and the EU policy cycle in internal security

One of the early issues discussed within COSI has been the outcome of the Harmony Project, which sought to develop further the European Criminal Intelligence Model (ECIM) initially considered in the Hague Programme. The establishment of such a model in relation to organised crime has been strongly supported by some Member States, particularly the United Kingdom, which has fully embraced 'intelligence-led' policing through SOCA, the Netherlands and Belgium, which initiated and supported Project Harmony. The three abovementioned countries and EUROPOL formed the international steering group of the project. Some 95% of the project's funding has come from the European Commission's "Prevention of and fight against organised crime programme".

The final report of the Harmony Project was transmitted to COSI on 25 October 2010 (Council document 14851/10). The core of the prescriptions issued by the report rest on a generic perspective on process management (see **Figure 1 in the Annex**): an initiative is developed on the basis of the analysis of available information, resulting in a decision establishing a formal setting, which then leads to implementation and monitoring. The outcome of the implementation and monitoring phase is finally evaluated, and the evaluation feeds directly into the development and setting of a new initiative.

The application of the Harmony Project managerial model to EU internal security activities envisages a four-year policy cycle, based on the following options:

- EUROPOL should become the foremost body in charge of threat assessment (policy development stage). The Harmony report echoes familiar critiques of the OCTA report, and suggests several modifications to the methodology (or

lack thereof) used. COSI should serve as the advisory board for methodological matters. A new OCTA report should be drafted every four years (as opposed to the current two-year interval, and the previous annual cycle before 2009) and an interim threat assessment report should be drafted every two years to update it. It is recommended that TE-SAT be maintained as a separate 'product', albeit changed into a threat assessment document rather than a situational overview.

- COSI should prepare the political decision-making and the conclusions for the JHA Council to adopt concerning the priorities of the cycle. This is achieved through the elaboration of a Policy Advisory Document (PAD). The JHA Council would ultimately be in charge of the final decision on the orientations of EU internal security activities. COSI should again be tasked with steering the drafting of multi-annual strategic plans (MASPs) corresponding to each priority defined by the Council, and with endorsing them. COSI would among others have the competence to commission the relevant actors for this purpose, including the European Commission and the EU JHA agencies.
- Implementation should be based on annual operational action plans (OAPs) drafted under the supervision of COSI, which appoints the lead EU agency in cases where interactions between EU and national actors are necessary. OAPs are then incorporated into the work programmes of the concerned national and European agencies, bodies and services.
- Evaluation should take the form of a two-fold process: a yearly evaluation of the OAPs, mostly based on quantitative indicators, and an overall evaluation of the four-year strategic guidelines with a stronger qualitative component. COSI is the recipient of evaluations in both cases, but the overall evaluation is the only one that is forwarded to the JHA Council. This evaluation is to be conducted by the Working Group on General Matters (the former Multi-disciplinary Group, MDG). The result of the evaluation is then taken into account by EUROPOL in drafting a new threat assessment.

In September 2010, the decision was taken by COSI that the new approach would be applied firstly to serious organised crime, on the basis of a SOCTAs (Serious and Organised Crime) report drafted by EUROPOL, although some delegations (Italy) considered that an EU policy cycle should be started with regard to terrorism (Council document 12657/1/10, p. 6). The methodology for the SOCTAs would be developed by a group of experts hosted by EUROPOL (who would also convene the experts in charge of drafting the OAPs), with COSI acting as the Advisory Board, while the expert meetings for drafting the MASPs would be convened by DG Home (Council document 13871/10). These elements were drafted into the Council conclusions, submitted to COREPER in October 2010 and subsequently adopted by the JHA Council (Council document 14998/10). At the time of writing, the SOCTAs 'customer requirements' are being discussed (Council document 12983/11, not publicly available) and a first template for the OAPs has been produced (Council document 12587/1/11, not publicly available). The Commission and Council have nonetheless produced a Policy Advisory Document to be discussed by the JHA Council, on the basis of EUROPOL's 2011 OCTA report (Council document 9225/4/11).

A possible expansion of the mandate of COSI, in this context, should be scrutinised carefully, firstly due to the emphasis (albeit not always sustained in acts) on its 'capitals-based' constituency. Such a development could result in the reinforcement of intergovernmental, 'third-pillar like' practices of decision-making in the field of internal security to the detriment of the logic promoted through Lisbon of a collapse of the pillar structure and a convergence of decision-making procedures across EU policy domains. **A further reason to monitor future changes to the Council working structures in relation to COSI is the exclusion of operational cooperation matters from the ordinary legislative procedure established in Article 87(3) TFEU**. This provision **weakens the system of checks and balances** between the EU institutions, insofar as

Parliament is only 'consulted' as opposed to ordinary circumstances where it is on an equal footing with the Council.

2.2.2.4. The EU 'policy cycle' in internal security matters and the role of the EP

As pointed out above, the organisation of the policy cycle in internal security has been an important area of focus for COSI since its inception. A recent study commissioned by the LIBE Committee on the internal security policy process and Project Harmony points out, in this respect, a number of 'perils' in the implementation of such prescriptions.[55] This includes the lack of any monitoring arrangement involving the European Parliament. Although the role of the EP is limited in decision-making on matters of operational cooperation due to the provisions contained in Article 87(3) TFEU, the envisaged policy cycle touches upon areas where the EP has a role as co-legislator, and in any case where it remains the budgetary authority.

Of concern, here, is the fact that Project Harmony leaves very little room for any form of independent or external evaluation of the information and analyses leading to the development of internal security policies. It does not specify mechanisms through which, in accordance with Article 70 TFEU on impartial evaluation of EU policies, Article 71 TFEU on COSI and Article 6(2) of the COSI Decision, the European Parliament and national Parliaments are kept 'informed', and how their comments can be taken on board. In Project Harmony's 'ideal situation' indeed:

- Policy development is ensured through evaluation, data collection and analysis. A marked emphasis is placed on the reinforcement of EUROPOL's 'in-house' expertise.
- Decision-making is prepared by COSI on the basis of EUROPOL's threat assessment, and undertaken by the JHA Council which "remains the responsible political body which decides upon the priorities to be tackled, based on the policy advisory document" (Project Harmony final report, 14851/10, p. 58).
- Implementation is ensured by relevant law enforcement authorities at EU and Member State level. It is again up to the JHA Council to 'task' relevant bodies for all non-law-enforcement matters. Monitoring during the implementation phase is ensured internally by each concerned agency or body.
- Evaluation comprises both yearly and multi-annual reporting. Yearly evaluations can be conducted internally (e.g. the EUROPOL director reports to the Office's management board), whereas multi-annual evaluations should be conducted independently. The Harmony Project report proposes four options for such independent evaluation: the use of a small group of Member States, of a Support Unit with professional expertise, of COSI or of the Commission. For both types of evaluation, COSI is considered as the reception point: for yearly evaluations, it should be the end point, while it should act a clearing house for circulation to the JHA Council in the case of multi-annual evaluations.

One has to keep in mind, of course, that the Harmony Project is currently a set of prescriptions and not an effective practice. Its outcome should nonetheless be closely monitored. **While the Project has been designed with the purpose of reaffirming the need for simplification and efficiency of policy-making in the field of internal security, so far it seems that parliamentary monitoring or scrutiny has not been considered as a key aspect of the policy cycle**. The 'policy cycle' envisaged in the Harmony Project is a closed-circuit environment where inputs from outside the field of law-enforcement are markedly limited, with COSI as the main clearing house for policy development, decision-making, policy implementation and evaluation, and the JHA Council

[55] M. Busuioc and D. Curtin (2011), op. cit.

as the ultimate political authority. As such, one could question **how far the Harmony Project would contribute to a more accountable and transparent policy process in the field of internal security**. While the role of sound analysis in policy development and assessment is important, the provision of expertise should be approached as a contradictory process, which is the only guarantee of a properly evidence-based policy-making. In addition, the Harmony 'policy cycle' does not place much emphasis on the reinforced system of checks and balances, introduced by the Lisbon Treaty, and tends to overlook the fact that the AFSJ is simultaneously an area of freedom, security and justice, not one in which freedom, security and justice are compartmentalised policy fields.

A further preoccupation here is the recommendation issued by the Harmony Project final report that the production of strategic documents "for criminal phenomena that have not been identified by the JHA Council as a priority" should be stopped and that "[m]ulti-annual programmes (such as The Hague Programme, the Stockholm Programme and future Programmes) should not anticipate priorities" (Council document 14851/10, p. 60). For all their shortcomings, such strategy documents serve a fundamental purpose, which is **to ensure** as much of **a pluralistic debate** as possible about the overall orientations of the AFSJ, including on security priorities. **The establishment of priorities** in this area **should be a well-informed, evidence-based political process** rather than an expert and law-enforcement-driven cycle only.

In its recently adopted report on organised crime in the European Union,[56] the LIBE Committee has endorsed "the Council conclusions of 8-9 November 2010 on the EU policy cycle for organised crime", but called on "the Council to revise the decision and make provision for Parliament's involvement in determining priorities, discussing the strategic objectives and assessing the outcome of the policy cycle". Indeed, the JHA Council is not the sole body in charge of decision-making in the field of internal security, and the European Parliament has a crucial role to play in the future.

2.2.2.5. Bodies in charge of fundamental freedoms and rights do not seem to be fully included in the scope of COSI's activities

Among the core EU JHA agencies and bodies, firstly, CEPOL and EUROJUST seem to be considered as coming second to EUROPOL and FRONTEX, which have so far benefitted the most from the committee's attention. Despite the commitments laid out in the Stockholm Programme in this respect, bodies in charge of fundamental freedoms and rights do not seem to be included in the scope of COSI's activities. The EDPS, for one, has still to receive an invitation to the Committee's meetings. One can of course question why the situation should be otherwise, given COSI's mandate for operational matters. However, two points can be made in this respect:

- Firstly, bodies such as the EDPS or the FRA have a role to play in operational matters. The case of the 2009 Prior Notification Check transmitted by FRONTEX to the EDPS on the processing of personal data in so-called 'return' operations (see 2.4. below) illustrates the dynamics of such an involvement. There are thus grounds to include agencies and bodies in charge of fundamental freedoms and rights in the planning of operational priorities undertaken by COSI.
- Secondly, COSI's remit includes the evaluation of operational cooperation (Article 3(2) of the COSI Decision). That the Standing Committee gives priority to a law-enforcement evaluation of operational activities is understandable given its mandate. Less understandable, however, is why considerations of fundamental freedoms and rights should be excluded from such an evaluation. There is a mismatch here between the strategic objectives featured for instance in the Stockholm Programme and their

[56] S. Alfano (2011), op. cit.

implementation. Of further concern are the consequences that such a situation might have after 2014 when the ECJ's mandate is fully extended to the AFSJ. Over the years, the EU's operational activities in the field of internal security have been met with considerable and extensive criticism from the point of view of fundamental freedoms and rights. FRONTEX, for example, has been challenged several times over its role in the breaching of fundamental principles subscribed to by Member States, such as *non refoulement*. The possibility of legal action over operational activities coordinated by the EU, and the related need to ensure that fundamental freedoms and rights are upheld in these activities constitute a solid basis for involving bodies such as the FRA or the EDPS in the evaluations conducted by COSI.

2.3. EUROPOL

2.3.1. Background on the agency

- The Maastricht Treaty (1992): EUROPOL was established, with a Convention established in 1995. This intergovernmental European body is then defined as a central police office supporting Member States in the collection, analysis and dissemination of information and intelligence. EUROPOL is composed of two main services with distinct objectives: a service in charge of analysing and producing databases for European bodies and national Law enforcement representatives; a liaison officers' service in charge of facilitating the bilateral and/or multilateral cooperation between Member States.
- Since 1995, EUROPOL has known important evolutions with the adoption in 2000, 2002 and 2003 of protocols amending the 1995 Convention. In January 2006, the Austrian presidency opened a debate on the evolution of the EUROPOL institutional framework. The adoption of the Council Decision of 6 April 2009 introduced changes in the legal basis of EUROPOL and has led to an extension of EUROPOL's mandate and tasks, and improvements in data processing and protection as well as in EUROPOL's operational and administrative capabilities in general. EUROPOL is now financed from the Community budget, and is subject to the Commission Financial and Staff Regulations.

Article 88 of the TFEU provides for a new legal regime for EUROPOL. It stipulates that EUROPOL shall be governed by (a) regulation(s), to be adopted in accordance with the ordinary legislative procedure, i.e. by co-decision. The current challenge for the EP is indeed the fact that the **Lisbon Treaty gives the EP more control over EUROPOL activities.**[57]

2.3.2. Ongoing debates and challenges

The LIBE Committee is well aware of the major challenges concerning the democratic accountability of EUROPOL. In its 2007 Report on the proposal for a Council decision establishing the European Police Office Following the extension of EUROPOL's operational powers, the proposed improvements and amendments already demonstrated the EP concerns in the areas of data protection (the collection, storage, processing, analysis and exchange of information and intelligence) and democratic control. A systematic use of the European Data-Protection Supervisor and the Joint Supervisory Body was then called. As stated in the report, "EUROPOL's increasing role in the fight against organised crime and terrorism should be carried on in a way that will guarantee transparency and democratic

[57] Bigo D., and al., *The field of the EU internal security agencies*, Paris: Cultures et Conflits/L'Harmattan, 2007.

control. Only in this way will the results of EUROPOL's activities be recognised by civil society".

The 2009 Decision (EUROPOL's founding act - Council Decision of 6 April 2009) opens the way for regular and formal exchanges between the EP and EUROPOL, giving the EP the right to request at any time that the Presidency of the Council, the Chairperson of the Management Board and the Director appear before the EP to discuss matters relating to EUROPOL. Furthermore, the 2009 Decision includes provision concerning the obligation for the Joint Supervisory Body to forward its activity reports, which are drawn up at regular intervals, not only to the Council but also to the EP.

However, the **scope of the Decision is very vague and broad**. Even if the role of the EP is recognised (control of EUROPOL through the involvement of the EP in the adoption of the budget; enhanced control over EUROPOL by the EP in order to ensure that EUROPOL remains fully accountable and transparent; possibilities for the Presidency of the Council, the Chairperson of the Management Board and the EUROPOL Director to appear before the European Parliament at its request - Art 48), the mechanisms through which such provisions would be implemented remain undefined.

The 2011 Declaration of Brussels by the Conference of the Speakers of the Parliaments of the European Union called for concrete measures to improve democratic oversight of the intelligence and security services in EU member states and provided specific proposals for improving the 'democratic' accountability of Europol as the first case study.[58] One such measure is the launch of a network of European expertise relating to the monitoring of intelligence services (ENNIR – European Network of National Intelligence Reviewers) whose primary objective would be to improve the democratic control of the functioning of the security and intelligence services.

Furthermore, some concerns raised from the EP during the preparatory work of the 2009 Decision have been simply ruled out by the Council in the 2009 Decision, specifically in **the areas of democratic accountability and governance.**[59]

- The proposition on inter-parliamentary committee has been ruled out. Even if the transmission of the annual draft planning documents to the EP was accepted for information purposes, the idea of an obligation to appear before inter-parliamentary committee was not taken up by the Council, and was therefore not reflected in the text of the Decision.
- The Involvement of the EP in the procedures for appointing the Director has not been considered.
- The idea of directly involving the EP in data protection processes was not followed up.

2.3.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS

In the context of EUROPOL new mandate (from OC to all serious crimes) and legal basis, EUROPOL new leadership (with a new Director, Rob Wainwright, former Chief of the International Department of the UK Serious and Organised Crime Agency - SOCA) is seeking actively for a renewed legitimacy. One of the constant arguments put forward by EUROPOL representatives is the following: EUROPOL has unique capabilities but unrealised

[58] Conference of the Speakers of the Parliaments of the European Union (2011), *Presidency Conclusions*, Brussels, 4-5 April 2011, p. 7.

[59] See The Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of EUROPOL's activities by the European Parliament, together with national Parliaments (Brussels, 17.12.2010, COM(2010) 776 final)

potential. In the 2010-2014 EUROPOL new strategy, EUROPOL has set up priorities in the following areas:

- The improvement of its support capacities for law enforcement operations;
- The delivery of Threat Assessment;
- Enlargement of EUROPOL fields of expertise

Each of these priorities must be considered and underlie specific concerns that require further attention from the LIBE Committee.

2.3.3.1. The improvement of its support capacities for law enforcement operations

As EUROPOL does not have executive powers to conduct investigations, the recognition of its capabilities in term of support for Member States (MS) operations is critical. EUROPOL has developed in the field a wide range of communication tools, such as 'road show' and the issuing of promotional 'catalogue' in order to increase awareness on its tools and instruments. The Road shows consist of seminars organised in EU MS and gathering members of National representatives of Police, Customs, Finance, and members of EUROPOL Liaison Bureau and of the EUROPOL National Unit. They aim at promoting EUROPOL capacities and enhancing cooperation and information exchange between Law Enforcement Agencies at regional, national and European levels. Such road shows are organised throughout the year. The 'Catalogue of Products and Services' provides an overview of products and services delivered by EUROPOL to national law enforcement agencies. The brochure gives a general overview on the strategic products and services (Analysis Capabilities such as OCTAs and T-SATs) and on the operational products (Analysis Work Files, Joint Investigation Teams - JIT, information systems – SIENA, EIS -, Liaison Bureaux Network, EUROPOL Platforms for Experts, etc.). As an addition, the success stories of operations in which EUROPOL was involved are duly reported in the annual review (under intriguing operations codenames, such as 'Gasoline', ' Andromeda', 'Black leaves', 'Garnet', 'Typhon', 'Gomorrah', 'Rescue', etc.). Such communication and advertisement efforts are accompanied by various demands in terms of operational capacities from EUROPOL staff.

Among them are the strengthening of the information management capabilities, by ensuring full interoperability of EUROPOL's systems and improving interoperability between the data processing systems of EUROPOL, MS, Interpol and EU-related bodies. This claim has been a constant object of debates, and has been one of the main concerns of the LIBE Committee. EUROPOL representatives are indeed very keen on repeating that the safeguards are strong and that the data protection system is at its best, notably through the use of the 4by4 system[60] to evaluate the reliability of the information given, the full respect of the Joint Supervisory Body guidelines and of the 13 data protection principles, the independence of the Data Protection Officers (DPO) guaranteed, no unlawful data retention, etc.

However, in at least four areas, further and future developments will require and deserve full scrutiny from the EP:

- Even if the EUROPOL data protection framework seems to offer a pragmatic and effective solution to an increased possibility of data access against more detailed data protection provisions, **the modalities through which access to data base**

[60] Information are divided in 4 categories: 1) information whose accuracy is not in doubt; 2) information known personally to the source but not known personally to the official passing it on; 3) information not known personally to the source but corroborated by other information already recorded; 4) information which is not known personally to the source and cannot be corroborated.

are granted, exchanged and stored should be firmly monitored and guaranteed.

As presented in the 'EU information management instruments' document prepared by the Commission presenting a summary of instruments regulating the collection, storage or cross-border exchange of personal data for the purpose of law enforcement or migration management, the EUROPOL Information System (EIS) contains personal data, including biometric identifiers, convictions, and organised crime links, of persons suspected of crime falling under EUROPOL's mandate. Analysis Work Files (AWF) contain any personal data of relevance. EIS can be accessed by EUROPOL National Units, liaison officers, EUROPOL staff and the director. AWF access is granted to liaison officers. Personal data may be exchanged with third countries that have agreements with EUROPOL. Specific Data protection rules have been established by the EUROPOL Decision and Council Framework Decision 2008/977/JHA, CoE Convention 108, CoE Additional Protocol 181, CoE Police Recommendation R (87) 15 and Regulation (EC) 45/2001. As an addition, a review mechanism (a Joint Supervisory Body) monitors EUROPOL's processing of personal data and the transmission of such data to other parties. It submits periodical reports to the EP and the Council. EUROPOL also submits an annual report on its activities to the Council for endorsement and to the EP for information.

The adequacy of the review mechanism (JSB and EUROPOL annual reports) should be constantly assessed and updated. Furthermore, the spirit of the Lisbon Treaty and the 'depillarisation' process should have led to the suppression of Supervisory Bodies per agencies, as well as a common supervision system under the EDPS. Supervisory bodies within EUROJUST, EUROPOL should be at the very least interconnected.

- In the area of data exchanged, the information exchange between EUROPOL and third parties requires full attention.

The heated debates and controversies on the 'SWIFT agreement' in the context of the Terrorist Finance Tracking Programme (TFTP) show how sensitive the issue of data exchange is. EUROPOL has been at the centre of several controversies and has been pointed by many NGOs and civil rights charities. Furthermore, **the EUROPOL's supervisory body published a report on the implementation of the EU-US TFTP agreement in March 2011, underlining serious concerns about compliance of EUROPOL with EU data protection standards**. In particular, authorisation of data transfer seems to be given on the basis of oral, unrecorded information. The role of the EP has been crucial on that matter. The Parliament refused to give its consent to the EU's interim agreement on banking data transfers to the USA via the SWIFT network, amid concerns for privacy, proportionality and reciprocity.

In a document addressed to the EP (EUROPOL Activities in Relation to the TFTP Agreement Information Note) after the publication of the JSB Report, EUROPOL explains in length on what grounds EUROPOL believes it has discharged its responsibilities with great care and to a high professional standard. The document reminds that the EU review team, Commissioner Malmström, and the EUROPOL Management Board have all arrived at the same conclusion. The document however concedes that further improvements to EUROPOL's activities are necessary in line with the recommendations of the EU review report and JSB Inspection Report and that these recommendations are the subject of high priority attention by EUROPOL. A follow up on such declarations of intention is needed. If Europol were to be chosen as the EU central Terrorist Finance Tracking System (TFTS) authority, it would also deal with requests by data subjects for access, rectification and blocking.[61] Thus, **ensuring that such powers under discussion over data is**

[61] European Commission (2011), Communication: A European terrorist finance tracking system: available options, Brussels, COM(2011) 429 final

exercised in all in accordance with its existing legal framework and data protection provisions appears to be critical.

- In the area of data regulation, the provision of EUROPOL Convention on the process of personal data deserves particular attention.

The argument put forward by representatives of EUROPOL is invariably the need to have special categories of data concerning notably political opinions, religious or philosophical beliefs, on the ground that they are relevant for counter terrorism activities. The LIBE Committee must ensure that the provision that special categories of data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, party or trade union membership, sexual orientation or health **shall not be processed and saved (only) when absolutely necessary and proportionate for the purpose of a specific case and subject to specific safeguards**. The process of data and the subsequent 'technological' challenged are detailed further in the section 3.3.

2.3.3.2. The delivery of Threat Assessment

The willingness of EUROPOL to grow as a central 'information powerhouse' in the EU also include building an information platform capable of assessing trends and risks, i.e. indentifying the various threats (present and future) affecting the EU. OCTAs and T-SATs have hence become a proudly labelled 'EUROPOL product'.

As mentioned in the 'background' section, one of the major weaknesses of the EU strategy in the field of OC and terrorism in the last decade has been the knowledge challenge. The new mission given to EUROPOL analysts - scanning the environment for new developments in internal security threats and sharing the results through effective 'early warning system' arrangements – must therefore be accompanied by closer scrutiny. **Ensuring that the EU' policy in the counter-terrorism and Organised Crime area is adequately evidence-based and supported by the best available threat assessments thus remains a constant challenge**. In that domain, if threat assessments all come from the same group of specialised teams of professionals of security discussing only among them, the path dependency in terms of solution and consequentially the lack of imagination and alternative will be detrimental to the knowledge.

2.3.3.3. An enlargement of EUROPOL fields of expertise in the ISS context

As cybercrime has become a major issue in EU agenda and in an ISS context (with the foreseen establishment of a cyber crime centre), **the possibilities for EUROPOL to host a cybercrime centre are significant and are highly advocated by EUROPOL representatives**. The recent cyber attack on the Commission and External Action Service on the eve of a summit in Brussels at the end of March generated new debates on the protection of infrastructures. In its memorandum submitted to the House of Lords Sub-Committee dedicated to the EU ISS, EUROPOL argues that it already has the capacities to host such a centre, though its EUROPOL's High Tech Crime Centre (HTCC) which coordinates operational activities serves as a communication platform and produces strategic analysis. Hence, the establishment within existing structures of a cybercrime centre, through which Member States and EU institutions will be able to build operational and analytical capacity for investigations and cooperation with international partners, would avoid dispersion of investigative and analytical capacities in the fight against cybercrime.

In this claimed positioning, the place and role of the European Network and Security Agency (ENISA) needs to be addressed. ENISA's future role in the ISS is not very clear and requires further work, including through a budgetary perspective. In its

memorandum submitted to the House of Lords Sub-Committee dedicated to the EU ISS, ENISA defines its contribution to the ISS by an application of proven risk management techniques (identification of information security risks, global risk management and risk assessment, emerging threats and dissemination of good practices for risk Management and IT Contingency). In particular, the ENISA Work Programme 2011 includes efforts to enhance European cooperation to generate awareness about Networks and information Security, disseminate security relevant information and to assist Member States in coordinating these activities internationally. ENISA, established in 2004 and based in Heraklion in Greece had a mandate that was due to expire in March 2012. The EP and the Council recently decide to extend ENISA's mandate to 13th September 2013, which will allow time for debate on how to shape the Agency to meet future needs and challenges in network and information security. As highlighted in a EP report dedicated to the role and future of ENISA,[62] a possible extension of ENISA's mandate is foreseen in the area of cybercrime. In his speech given at the European parliament in May 2011, ENISA's Director stated the following: "ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between Computer Emergency Response Teams (CERTs) and law enforcement because we need the CERTs in the fight against cyber-crime. The important role of ENISA is to provide an interface between Law Enforcement and the cyber security community".[63] Thus, **debates on the better place to host the cybercrime centre should clarify the tasks given to EUROPOL and ENISA, in order to avoid duplication and budget expenses**.

Another field in which EUROPOL is investing is training, knowledge exchanges and law enforcement expertise. Article 5(4) of the EUROPOL Council Decision did invite EUROPOL to assist Member States through support, advice and research in the areas of training, technical support, crime prevention, technical and forensic methods and analysis, and investigative procedures. EUROPOL is since clearly investing efforts in pioneering new techniques to prevent and combat international serious crime and terrorism, strengthening the position of EUROPOL as a platform for specialist areas, and providing expertise and quality training in key law enforcement techniques. **In a context in which CEPOL is highly criticized and have lost legitimacy on the funding ground, such developments in EUROPOL need to be followed up and assessed**. Indeed, CEPOL has been given a reduced role in current internal security perspectives.

2.4. FRONTEX

2.4.1. Background on the agency

2.4.1.1. From a European Border Guard to the establishment of FRONTEX (Council Regulation (EC) No 2007/2004)

The story of the establishment of FRONTEX is already well documented.[64] A key point to understand the current state of play on the agency, however, is the tension that has lied since their inception in discussions on the creation of an EU body in charge of the external borders. Before FRONTEX was established, two positions informed these discussions. Some Member States and the European Commission envisaged the possibility to establish a body that would resemble a European unit of border guards with a degree of operational responsibilities. A feasibility study on the setting up of a European border police was for instance undertaken under the auspices of the Italian Ministry of Interior with the support

[62] J. Scott Marcus et al. (2011), "The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally", Brussels: European Parliament, PE464.432.

[63] U. Helmbrecht (2011), "ENISA today and in the future", Committee on Industry, Research and Energy, Mini-Hearing on ENISA, Brussels: European Parliament.

[64] See for instance the 2008 House of Lords report on the issue. See also the work of the CHALLENGE integrated programme researchers.

of Germany, France or Spain, and tabled in May 2002. Other Member States, among which Sweden or the United Kingdom, opposed the establishment of such a body, which was seen as unnecessary from an organisational point of view and politically undesirable as it would be susceptible of challenging the exclusive competence of Member State authorities regarding the control of their external borders. A middle ground solution was found for some time, combining the establishment of an External Borders Practitioners Common Unit within the framework of the Standing Committee on Immigration, Frontiers and Asylum (renamed SCIFA+ for the occasion) and the establishment of several *ad hoc* border centres in Member States volunteering to host them in the course of 2002. The system was however ultimately found lacking in a 2003 report from the Greek presidency, which led to the negotiation and adoption of Council Regulation (EC) No 2007/2004.

The FRONTEX Regulation establishes an organisation that reflects earlier controversies on external border control in the EU. The agency is framed as a technical body charged with operational coordination and lacking any direct operational competence with regard border control, which remains squarely within the remit of Member State authorities. **Although it was established as a first pillar body, in this regard, it appears much more as a third pillar agency**. It coordinates joint operations, but there is a significant degree of uncertainty as to its responsibility for the problems that might occur during such operations and the legal effects of its coordinating role. The agency is also an intelligence body, tasked with collecting information on developments at the external borders and compiling risks assessments. It is, finally, a support body in the context of the organisation by Member States of so-called Joint Return Operations (JROs). This was one of the most contentious aspects of the agency's initial remit, which led the European Parliament in particular to voice concerns in its opinion on the proposed regulation that FRONTEX would be turned into an 'expulsion agency'.

2.4.1.2. Rapid border intervention teams: Regulation (EC) No 863/2007

The first modification to the legal framework regulating the activities of FRONTEX has been the adoption of Regulation (EC) No 863/2007, which establishes Rapid border intervention teams (RABIT). RABITs are essentially a pool of border guard officials (the so-called 'Rapid pool') committed by participating Member States for the purpose of providing rapid and limited operational assistance "to a requesting Member State facing a situation of urgent and exceptional pressure, especially the arrival at points of the external borders of large number of third country nationals" (Article 1 of RABIT Regulation). RABIT teams are not meant to be deployed autonomously or under the authority of FRONTEX, but receive instructions from the border guard authorities of the requesting Member State. The agency appoints one of its official as coordinator of the deployment (Article 5 of RABIT Regulation). RABIT officers wear their own uniforms and are authorised to carry weapons according to the host Member State's legislation, and can use force under specific conditions. RABIT officers can perform all the tasks related to border control as defined in the Schengen Borders Code (Regulation (EC) No 526/2006), including border checks and border surveillance, the stamping of travel documents, the interviewing of undocumented persons and the consultation of databases.

Officers made available for RABIT deployment by Member States currently number between 500 and 600. The first deployment of RABIT teams lasted from 2 November 2010 until 3 March 2011, following a request from Greece, at the land border between this country and Turkey. According to estimates in the recently released annual report of FRONTEX for 2010, a total of 500 officers from 26 Member States were drawn for deployment from the Rapid Pool, with numbers effectively present on the ground comprised between 175 and 200 at any given time (FRONTEX General Report 2010, p. 10). RABIT 2010 was replaced in March 2011 by Joint Operation POSEIDON 2011, which includes a land and sea component.

2.4.1.3. Modification of the Schengen Borders Code: Council Decision 2010/252/EU

Following a number of highly publicised occurrences where distress calls involving boats carrying migrants have been left unanswered due to disagreements between Member

States over search and rescue responsibilities,[65] the Council adopted in April 2010 Decision 2010/252/EU supplementing the Schengen Borders Code. It specifies the rules applicable in the context of sea borders operations coordinated by FRONTEX. In particular, it enshrines the general principle that "[m]easures taken for the purpose of the surveillance operation shall be conducted in accordance with fundamental rights and in a way that does not put at risk the safety of the persons intercepted or rescued as well as of the participating units". It further indicates that operations of disembarkation or handing in of a person to a country's authorities must not contravene the principle of *non refoulement*. The rules and non-binding guidelines annexed to the Decision are to be incorporated in the operational plan drawn up for each sea border operation coordinated by the agency. The Decision has been recognised as a welcome clarification of rules which otherwise form part of Member States' international obligations under the law of the sea and the 1951 Geneva Convention by Amnesty International and ECRE among others.[66]

2.4.1.4. Current proposals for the revision of Council Regulation (EC) No 2007/2004

Most of the ongoing debates and challenges concerning FRONTEX that will be surveyed below concern **the revision of the agency's founding regulation, on which the Council and the Parliament have recently reached a political agreement** (Council document 11916/11). The European Commission tabled a proposal for the revision of the FRONTEX Regulation on 24 September 2010 (COM(2010) 61). Among the modifications foreseen by the proposal, the elements of interest for the purpose of this study include:

- the enhancement of the agency's role in joint operations and pilot projects;
- the clarification of the legal framework governing FRONTEX with particular attention to fundamental freedoms and rights issues;
- the possibility for the agency to have access to personal data, which was ruled out by the Commission in its initial proposal but reintroduced in the European Parliament's report on the proposal.

2.4.2. Ongoing debates and challenges

2.4.2.1. FRONTEX and the responsibility for joint operations and projects

The question of FRONTEX' responsibility with regard the various operational activities that it coordinates has been at the heart of the controversies surrounding the agency since it was created. This relates in particular to the unclear legal framework that has governed the agency so far (see 2007 ILPA submission to the House of Lords). As shown above, the decision that the agency should be a coordination body, similar in its remit to EUROJUST and EUROPOL in their respective fields, rather than a service effectively in charge of border controls, has generated a significant degree of uncertainty as to which authority should be held liable for possible violations of the rule of law in joint operations. When called upon to justify some of the problems raised by its activities, the agency has systematically emphasised that responsibility lay with Member State authorities. This has been the case, for instance, when requested by civil liberties organisations to disclose the legal instruments authorising some of its joint operations based in the Canary Islands (the HERA operations, see below 4.4.1).

The revision of the FRONTEX regulation is likely to clarify the legal framework governing the agency. Some provisions, on the one hand, would give FRONTEX more control over

[65] Including the case of a boat carrying some 20 people, mostly from Eritrea, which had to wait for more than 24 hours before being eventually rescued by a Libyan ship. While the ship laid in Malta's search and rescue area and within the 40 nautical miles zone of Italy, the authorities of both Member States failed to agree on responsibility for the rescue (see HCR briefing of 8 June 2011 on the incident, available from: www.unhcr.org/4c0e33b66.html).

[66] See joint Amnesty International & ECRE Briefing of September 2010, p. 10-11, available from: www.ecre.org/component/downloads/downloads/58.html).

operational activities. The new Article 3 of the regulation would for example place the agency in a position to "evaluate, approve and coordinate proposals for joint operations and pilot projects made by Member States", which implies that it could refuse such proposals. It further specifies that the agency "may initiate joint operations and pilot projects in cooperation with Member States" and "may also terminate joint operations and pilot projects if the conditions to conduct these initiatives are no longer fulfilled". Very tellingly, the Commission's impact assessment stresses that such provisions might result in increasing the possibility that the agency and its staff would be "exposed to situations of possible violations of fundamental rights" (SEC(2010) 149, p. 29). The comment acknowledges the fact that the agency's activities can have legal effect, and support the possibility of redress in front of the ECJ. A similar, if less explicit change, has been made to Article 9 of Regulation 2007/2004 on joint return operations. The new Article 9 specifies that FRONTEX may coordinate the organisation of JROs upon request of the Member States, and that this may involve a decision to finance or co-finance such operations. Financial support is "conditional upon the full respect of the Charter of Fundamental Rights". The provision not only establishes clearly that FRONTEX has an obligation to comply with the Treaty obligations regard fundamental freedoms and rights, but can also be considered to establish a responsibility of the agency should it decide to provide financial support to a JRO that would not comply with the CFR.

A second aspect of the proposal that clarifies the Agency's responsibilities is the **reference to the Schengen Borders Code**. The proposed Article 1(2) thus establishes that "the Agency shall facilitate and render more effective the application of existing and future European Union measures relating to the management of external borders, in particular the Schengen Borders Code, and in accordance with relevant Union law, International law, obligations related to access to international protection, and fundamental rights". The combination of provisions giving FRONTEX more control over joint operations and pilot projects as well as JROs with the clarification of the legal framework under which this enhanced control falls contribute overall to ascertaining that the agency indeed has a number of responsibilities that may induce legal effects if breached.

2.4.2.2. FRONTEX and fundamental freedoms and rights

The compliance of FRONTEX activities with fundamental freedoms and rights has been a source of concern since its inception. One initial concern lied with **the absence of a clear legal framework governing the agency's activities**. The FRONTEX Regulation was adopted before a legal definition of the EU's external borders could be agreed upon and rules about who is allowed to cross the border and how be adopted. This, as mentioned above, would be sorted with the modification of the FRONTEX Regulation and the explicit reference to the Schengen Borders Code.

A key preoccupation involves the joint operations coordinated by the agency and particularly sea border operations such as the HERA and NAUTILUS series. FRONTEX has acknowledged that its officials were conducting interviews with the persons intercepted in such operations for intelligence purposes, arguing that it is not their responsibility to hear out asylum claims, a task that falls within the remit of Member State authorities. As one scholar suggests, this is a highly legalistic interpretation of the separation of competencies between the agency and the Member States, and one that is unlikely to reflect the practical circumstances that FRONTEX officials face in operational context (Guild, 2010: 17).

Another debate involves **the agency's role in joint return operations**. Under the current legal framework, this role is underspecified (e.g. Carrera, 2007: 17). FRONTEX is expected to provide 'assistance' to Member States in the organisation of JROs (Article 9(1) of Council Regulation (EC) 2007/2004), but the exact scope of these assistance tasks is unclear. This has been a constant preoccupation, especially in the last three years where the agency's participation to JROs has increased exponentially: according to some estimates based on the figures provided by FRONTEX, the number of co-financed joint

return operations has doubled from 2008 to 2009, with funding increasing by 500%, with expectations that it would have doubled in 2010.[67] As mentioned previously, the modified FRONTEX regulation would bring more clarity in this domain, by reinforcing the control of the agency over JROs, and by clearly relating this activity to the Charter of Fundamental Rights and the common standards and procedures laid down in Directive 2008/115/EC on the Union's return policy (referred to in Recital 21 of the modified Regulation's Preamble), including the respect of the *non-refoulement* principle (Article 5) and the procedural safeguards included in Chapter III. The new Article 9(2) of the FRONTEX Regulation would further commit the agency to develop a code of conduct for return operations, comprising standard procedures "in full respect of fundamental rights, in particular the principles of human dignity, prohibition of torture and of inhuman or degrading treatment or punishment, right to liberty and security, the right to the protection of personal data and non discrimination". The new Article 9(3) additionally lays down the ground for an independent monitoring system of compliance with the Code of Conduct, with reference to the provisions in Article 8(6) of Directive 2008/115/EC.

Concerns with the compliance of FRONTEX activities with Treaty and international obligations in the field of fundamental rights and obligations are further reflected in the European Parliament's draft report on the Commission's proposed amending act of Council Regulation 2007/2004 (PE 475.754). The draft report features a number of contrasted amendments. Some are likely to reinforce the legal framework governing the agency and the monitoring of its activities from the perspective of fundamental freedoms and rights, while others are likely to reinforce controversies about the agency (most stringently with regard access to personal data, as discussed in the next point). Amendments concerning the legal framework include for example the introduction of a specific reference to the CFR and the 1951 Geneva Convention the new Article 1(2) of the Regulation.

The rapporteur further suggests in the report's explanatory statement that the different amendments mandating the agency to pay specific attention to Member States "facing specific or disproportionate pressures" (in the wording of the proposed amended Recital 1) would provide more support to those Member States facing a strain on their asylum system. The argument has been quite systematically made by Member States finding themselves in charge of large portions of the EU's southern maritime external border, including Spain, Italy, Malta and Greece. This reasoning, however, raises the question of whether the activities of FRONTEX should be considered a remedy to situations such as the one facing Greece at the moment. Can the reinforcement of border controls, of interception and diversion operations, and the intensification of returns, be considered an adequate option for the EU's asylum policy, compliant with the Treaty and international obligations of the Union and its Member States? Both the UNHCR and the Council of Europe have pointed out, in recent months, the dysfunctions of the Greek asylum system for example, highlighting the way in which the Dublin system opened up the possibility for other Member States to issue disproportionate requests to Greece for their asylum applications.[68] It seems difficult to consider that meeting the necessary revision of a dysfunctional EU asylum system with reinforced security measures in the guise of strengthened border controls can be a viable policy option.

2.4.2.3. FRONTEX and access to personal data

The question of access to personal data by FRONTEX has been another of the running debates since the establishment of the agency. Article 11 of the current FRONTEX Regulation mentions that the agency should facilitate the exchange of information relevant to its tasks with the Commission and the Member States, but makes no mention of access to or processing of personal data. This situation follows from the emphasis that

[67] See joint Amnesty International & ECRE Briefing of September 2010, p. 28, available from: www.ecre.org/component/downloads/downloads/58.html).

[68] S. Carrera and E. Guild (2010), "'Joint Operation RABIT 2010' – FRONTEX Assistance to Greece's Border with Turkey: Revealing the Deficiencies of Europe's Dublin Asylum System", Brussels: CEPS, 11.2010, pp. 12-15.

Member States have placed on their exclusive competence for the effective conduct of border controls. **Since FRONTEX is only a coordinating body, it does not need to have access to information systems holding personal data in relation to the control of the Union's external borders** (e.g. the Schengen Information System). The agency's senior staff has repeatedly challenged this view, arguing that the analysis work of FRONTEX in particular required more than access to statistical data which the agency has enjoyed since its inception, insisting that it should be granted some form of access to, and competence to process, personal data. In its initial proposal for a revision of Council Regulation 2007/2004 however, the Commission has explicitly ruled out the possibility of granting FRONTEX access to and process of personal data, preferring "to return to the question of personal data in the context of the overall strategy for information exchange" (COM(2010) 61, p. 4).

The EP's draft report on the Commission's proposal has gone against that option. Provisions regulating the access of personal data by the agency have been inserted in Article 11 of Council Regulation 2007/2004. The purpose of data processing is "to contribute to the security of the external borders of the Member States of the European Union". The processing of personal data by FRONTEX is limited to:

- "personal data obtained during joint operations or pilot projects or rapid border intervention missions";
- "persons who are suspected on reasonable grounds of involvement in cross-border criminal activities, in illegal migration activities or in human trafficking activities as defined in Article 1(1) (a) and (b) of Council Directive 2002/90/EC";
- "persons who are victims of such activities and whose data may lead to the perpetrators of such activities" and
- "persons who are subject to return operations in which the Agency is involved".

The retention period is not to exceed three months. Onward transmission to EUROPOL is authorised, as well as to "other European Union agencies or bodies", provided that FRONTEX has entered into a working agreement on the exchange of personal data with them, and subject to the prior approval of the EDPS. Onward transmission by the agency to Member States, third countries or other third parties is prohibited.

There are several aspects to be considered in this debate. On the one hand, **the EP's proposed amendment creates yet another challenge for ensuring the agency's compliance with its fundamental freedoms and rights obligations, this time in the field of data protection**. On the other, **the amendment only endorses the agency's existing practices**. In April 2009 indeed, FRONTEX communicated a notification for prior checking to the EDPS concerning the "Collection of names and certain other relevant data of returnees for joint return operations". The purpose of the collection was to compile information on the number and identity of returned persons, assess their health status, age and degree of 'risk'. The EDPS found the processing to be lawful under the agency's existing legal framework and through the application of Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies (FRONTEX being a first-pillar agency). It seems in this respect that the draft report from the European Parliament has followed the 'pragmatic' line that the EDPS tends to adopt with regard data processing in relation to law-enforcement activities and which is reflected in the latter's May 2010 Opinion on the Commission's proposal for the revision of Council Regulation 2007/2004: namely, that the clear spelling out of rules on the processing of personal data is preferable to the absence of such rules in circumstances where it is clear that data processing is likely to occur. In the meantime, this modification of the agency's mandate opens up yet another issue regarding fundamental freedoms and rights, namely the oversight of the processing of personal data by FRONTEX and of the transfer of such data to other European bodies falling under different data protection regimes. **It further raises the question of the**

risks associated with the transformation of FRONTEX into an all-purpose security agency, rather than one focused on its specific mandate of coordinating operational cooperation at the external borders of the Member States. The emphasis placed by FRONTEX on its analytical products, as well as the developments associated with EUROSUR, which would place the agency in charge of constituting a 'pre-frontier intelligence picture' (see below 2.5.3.1. and 2.5.3.2.), as well as the logic of the cooperation with EUROPOL which appears to lead to the entanglement of the mandates of the two bodies (see below 2.6.1.), reinforce this interrogation.

2.4.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS

2.4.3.1. Analyses and information on EU external borders

The production and circulation of analyses and information on EU external borders is the first area of concern to be considered in relation to FRONTEX. The agency has been very proactive in positioning itself as a central information hub for statistical information about the external borders and forecasts about possible future scenarios. Recent changes in the Council's working groups structure are likely to reinforce this trend. At stake here is the demise of the Centre for Information, Discussion and Exchange on the Crossing of Frontiers (CIREFI), which had been set up in 1992 to collect and encourage the exchange of information about various issues related to border crossing (legal immigration, irregular immigration and residence, facilitator networks, false and falsified documents, statistics from national authorities), compile and produce analyses. CIREFI's information collection and analysis functions have been transferred to FRONTEX in April 2010. The agency is making use of that information, among others, in its annual reporting as well as in its regular FRONTEX Risk Analysis Network publication (FRAN Quarterly). The FRAN Quarterly is only one of the agency's publications out of the few that are publicly available.[69] While this does constitute to some degree a departure from FRONTEX' policy of strict non-disclosure of its information 'products', a close reading of this type of documents illustrates the risks presented by the centralisation of information about external borders in a single body. This is a particularly important issue to follow in view of the new Article 4 of the FRONTEX Regulation, which gives a legal basis to the Common Risk Integrated Model (CIRAM) developed early on by the agency. Article 4 foresees that the agency "shall prepare both general and tailored risk analyses, to be submitted to the Council and the Commission", for the purpose of which "Member States shall provide the Agency with all necessary information regarding the situation and possible threats at the external borders". The provision potentially places FRONTEX in a monopolistic position with regard the development of situation assessments at the external borders.

FRAN Quarterly publications are put together by the agency's Risk Analysis Unit, on the basis of data provided by Member States border control authorities. They offer a largely quantitative analysis of the situation at the external borders, based on six indicators:

- Illegal border-crossing between border checkpoints (1a)
- Clandestine entries at border checkpoints (1b)
- Facilitators
- Illegal stay
- Refusals of entry
- Applications for asylum
- False travel-document users

[69] FRAN Quarterly reports have been made available on the agency's website since the eighth issue (first quarter of 2009.

There are several issues with this type of analyses. Some are openly acknowledged by the agency. These categories of data are not harmonised for the 30 countries participating in the FRAN, nor are the procedures for collecting and compiling this data. What research on the issue has shown as well is that even within a given Member State, the compilation and analysis of data concerning migration is a highly controversial exercise.[70] Of further concern here is the representation of the situation at the external borders that publications such as the FRAN Quarterly are providing to policy-makers, experts and scholars, as well as the general public. The abovementioned indicators **do not offer the possibility for a well-informed debate**, insofar as they only tell a partial story of crossings at the EU external borders. In particular, they do not relate irregular border crossings to the overall number of persons entering the EU for professional and personal purposes, as well as for tourism, which would be an important means for shaping the debate about the efforts to be delivered in the field of border control.

It appears important, in this respect, **to support pluralism in the production of information about the external borders, as well as a greater degree of transparency as to how the data aggregated in the various indicators used by publications such as the FRAN Quarterly is processed**. Just as with EUROPOL's various threat assessment reports, it appears fundamental to make sure that the methodology used in such reporting exercises is made fully transparent, so it can be externally assessed just like any other knowledge process. There are different ways to ensure such pluralism, but examples, such as the THESIM or CLANDESTINO research programmes mentioned at the bottom of this page, or the CARIM consortium initially funded under MEDA's regional programme[71] would constitute one possibility.

2.4.3.2. FRONTEX and border surveillance: The question of EUROSUR

A second area of importance regarding FRONTEX lies at the intersection between the discussion on the agency's access to personal data and its growing role as the central hub for information about the EU's external borders. It concerns the setting-up of the European Border Surveillance System (EUROSUR), which was officially launched by DG JLS in one of the communications comprised in its February 2008 'border package'. The development of EUROSUR has been funded through the External Borders Fund and the Schengen Facility, and supported by a number of projects funded under the FP7's Security Theme as well as on their own funds by FRONTEX and the European Commission's Joint Research Centre

EUROSUR is previewed as a 'system-of-systems' which would interconnect in the first place the maritime surveillance systems (civilian, law-enforcement and military) of EU Member States with responsibility over a segment of the EU's external sea borders. As previous research has shown (PE 408.285), FRONTEX would be acting as the central 'hub' of EUROSUR, effectively expanding on its current risk analysis tasks to become an intelligence agency in charge of elaborating and updating the 'common pre-frontier intelligence picture', which constitutes the core of the EUROSUR objectives. A number of objections have been raised regarding the EUROSUR project, among which the lack of a legal basis for developing the system, and a lack of clarity as to which kind of data would be processed. The extent to which EUROSUR would involve the processing of personal data, in particular, remains undetermined. DG JLS/Home has reported regularly, if sparsely, on the advancement of the system's development (SEC(2010) 171 and SEC(2011) 145), and tabled in 2010 a roadmap indicating that a legislative proposal would be issued in the course of 2011. The Commission's proposal for the amendment of the FRONTEX Regulation has foreseen a modified Article 2(1)(i) including "the necessary assistance to the development and operation of a European border surveillance system and, as appropriate, to the development of a common information sharing environment, including interoperability of systems" in the tasks of the agency. The Stockholm

[70] See for instance the outcome of the THESIM (www.uclouvain.be/en-7823.html) or CLANDESTINO (http://clandestino.eliamep.gr/) projects, both supported by the EU FP6.

[71] www.carim.org/.

Programme, the ISS and the Commission's ISS in Action communication, finally, have also endorsed EUROSUR as a key initiative.

The shift towards a more intelligence-driven logic relying on intensive data processing in the work of FRONTEX deserves close scrutiny. At the general level, this development echoes the reinforcement of the trend towards intelligence-led policing among EU agencies, bodies and services in the field of internal security. Regarding FRONTEX in particular, it implies that the interplay between the possibility now given to the agency to process personal data and the insertion of its risk analysis capacities in a broader computerised system will deserve more scrutiny, as it might lead the way to a broader remit in terms of data processing.

2.4.3.3. Oversight of the agency

The question of oversight is the third area of concern involving FRONTEX. Recent debates and developments have made it even more stringent to ensure that the agency's activities receive proper and continuous attention. Since it has become operational six years ago, the agency has experienced a considerable increase in its volume of activity, funding, and now remit. The European Parliament has played a role in this growth, since it has repeatedly increased the budget available to the agency, considering, in the words of one MEP, that it had "no interest in seeing FRONTEX walk. We want it to run at great speed, and this explains why we have done this".[72] The outcome of the revision of Council Regulation 2007/2004 is likely to add to this expansion, in several ways.

Firstly, as explained above, the revised regulation would give more decision-making powers to FRONTEX on the staging of joint operations and projects. According to the new Article 3b, the agency would also be able to deploy more officials via the FRONTEX Joint Support Teams (FJST) mechanism. FJST would consist of a pool of national border-guard officers seconded by their Member State for a period of six month every twelve months, which will be deployed at the request of the agency for any joint operation or pilot project. The setting-up of FSJT can potentially make more complex the ascertaining of responsibilities in case of a violation of the rule of law in the context of a FRONTEX joint operation. FSJT officers are to be considered, according to the new Article 10(2) as 'guest officers', who "shall comply with Union law, in accordance with fundamental rights, and the national law of the host Member State". The FSJT mechanism thus establishes a situation where three parties can be held liable for possible violations: the Member State sending the guest officer, the 'host Member State' and FRONTEX.

Secondly, the expansion of the agency's remit involves additional possibilities to engage with third countries. Two provisions deserve more scrutiny here, inserted in the Regulation's new Article 14, which opens the possibility for the agency to send liaison officers to third countries, and to benefit from Union funding to establish technical assistance projects in third countries. FRONTEX liaison officers are expected to join already established local or regional networks of immigration liaison officers (ILOs) established by Member States in third countries on the basis of Council Regulation No 377/2004. According to Article 2 of this Regulation, ILOs are expected to establish direct contacts with the authorities of the country they are deployed to, collect operational and strategic information regarding irregular and regular migration, and assist and facilitate the identification and returning of persons to their country of origin. In other words, ILOs conduct extraterritorial, intelligence-based policing activities, which are extremely complex to control. The revised FRONTEX Regulation specifies that the agency's liaison officers "shall only be deployed to third countries in which border management practices respect minimum human rights standards" while "[p]riority for deployment should be given to those third countries, which on the basis of risk analysis constitute a country of origin or transit regarding illegal migration". Several points can be raised regarding these provisions:

[72] House of Lords, "European Union Committee, 9th Report of Session 2007-2008: Minutes of Evidence", House of Lords, London, 5 March 2008, pp. 24-25.

- What are 'minimum human rights standards'? FRONTEX is bound by law to respect the Charter of Fundamental Rights in all its activities, including beyond the territory of the Member States of the EU. These cannot be derogated to.
- The phrasing of the provision is unclear. It seems to imply that border management practices can be isolated from the rest of a country's legal framework as respecting human rights. The respect for human rights in border management practices follows from the general rule of law applicable across all domains of society in a given country: it is therefore unlikely that one can single out border management practices respectful of human rights standards in countries that otherwise violate them.
- Given the two first observations, one is tempted to ask which priority should be respected in the deployment of ILOs: human rights standards or risk assessments?

Of further concern in this regard is the fact that **the provisions concerning the initiating of technical assistance projects by the agency do not include any mention of human rights criteria.**

These few observations highlight the necessity of a stricter framework of oversight for the agency. While the revised Regulation would confer upon FRONTEX the possibility to evaluate the border management practices of Member States and terminate joint operations should they fail to meet acceptable standards, including with respect fundamental freedoms and human rights, it says very little on who should evaluate the agency itself. Administrative oversight still lies with the Commission's DG Home, but assessments and evaluations of the kind published in the February 2008 'border package' should come more frequently, arguably on a yearly basis. There should be, in addition, a degree of political oversight. The Council points out in the summary of the key points in the draft compromise text agreed upon with the European Parliament that a Consultative Forum on Fundamental Rights and a Fundamental Rights officer shall be established. This, together with the other elements inserting fundamental freedoms and rights provisions in the agency's activities, could contribute to make FRONTEX more transparent and more accountable. There should be, however, room for more monitoring on a more regular basis, and with more involvement from the European and national Parliaments.

2.5. CEPOL

2.5.1. Background on the agency

2.5.1.1. The Maastricht Treaty and the Declaration on Police Cooperation

Discussions concerning the establishment of a European police structure for training were first developed among directors of national senior police courses and academic experts in the second half of the 1980s. Following a meeting of the former in Copenhagen in 1989, two proposals were tabled: the first one in 1990 by a group of experts gathered by the Dutch Ministry of Interior, the second by the director of the German Polizeiführungsakademie in Münster, Rainer Schulte, in 1992. From the onset the debate focused on whether such a structure would take the form of a full-blown European Police Academy, or whether it would just be a secretariat coordinating a network of national police training institutes. These ongoing discussions were relayed in part by the German delegation at the Luxembourg European Council (28-29 June 1991) and resulted in the appending of a *Declaration on police cooperation* to the Maastricht Treaty (Declaration No 32) which included considerations on training committing Member States "to consider on the basis of a report, during 1994 at the latest, whether the scope of such cooperation should be extended". Questions of training were further incorporated in the 1995 Europol Convention (Article 2 and 3). In the meantime, the promotion of transnational cooperation

in the field of police training were sustained by initiatives outside the Community framework: the founding of the *Mitteleuropäische Polizeiakademie* (MPA) in Vienna in 1993 (involving Austria, Germany, Hungary, Poland, the Czech Republic and Switzerland), the creation of the *European Law Enforcement College* in Brussels in 1995 as a joint venture of the Belgian, British and Dutch governments, and the launching of the *Association of European Police Colleges* (AEPC). AEPC was initially founded by means of an agreement between the Dutch, German and British police academies with the aim of creating a European Police Academy in accordance with the phased approach outlined in the 1992 Schulte report. While not formally associated with the EU, AEPC nonetheless established links with the Council Police Cooperation Working Group (PCWG) and its official launch event on 25 January 1996 was placed under the auspices of Swedish commissioner Anita Gradin, holder of the JHA portfolio in the Santer College. By December 1996, the membership of AEPC had extended to include all national police academies of EU Member States.

2.5.1.2. The Tampere Programme and Council Decision 2000/820/JHA

The creation of the European Police College was formally considered in the Tampere 'milestones' adopted by the European Council on 15-16 October 1999 (Conclusion No 47). Council Decision 2000/820/JHA establishing CEPOL was adopted on 22 December 2000.[73] The Decision establishes that the CEPOL constitutes "a network of existing national training institutes" and frames the creation of the College in relation to the then-ongoing enlargement process: "It is desirable to develop quickly a relationship between CEPOL and national training institutes in applicant countries with which the European Union is conducting accession negotiations." CEPOL is established in particular to provide a training framework for senior and middle-ranking police officers, as well as police officers with specific responsibilities regarding cross-border crime and particularly organised crime (Article 7). CEPOL is further expected to "support and develop a European cooperation to the main problems facing Member States in the fight against crime, crime prevention, and the maintenance of law and order and public security, in particular the cross-border dimension of these problems" (Article 6(1)). Various options were discussed under the auspices of the Finnish, Portuguese and French Presidencies, involving the scope that should be given to the initiative: for some Member States such as Italy, the new body should include a distinctive European dimension, while others such as France favoured the mutual strengthening of Member State capacities. Decision 2000/820/JHA reflects these disagreements: it establishes the College as a network of national training institutes, but foresees that the CEPOL's governing council should appoint a permanent secretariat headed by an administrative director.

2.5.1.3. Council Decision 2005/681/JHA and the establishment of CEPOL as an EU agency

The adoption of Council Decision 2000/820/JHA generated a number of issues. Despite the adoption of the College's annual work programme for 2002 and of the CEPOL financial regulation and budget for 2002, the College was nonetheless prevented from starting its work because no decision had been taken on the seat of its permanent secretariat, and more importantly because it lacked a legal personality. Following a discussion in CATS, a provisional seat was provided by Denmark.[74] It is only from January 2004, following the approval by the body's Governing Board of its three-year report that discussions within CATS took a sharper focus.[75] The incoming Irish Presidency introduced in December 2003

[73] Council Decision of 22 December 2000 establishing a European Police College (CEPOL) (2000/820/JHA), OJ L336/1, 30.12.2000.

[74] Council of the European Union (2002), "Provisional management solution for the European Police College (CEPOL)", 6603/02, 26.2.2002.

[75] Council of the European Union (2003), "Three-year report on the operation and future of the European Police College", 15722/03, 9.12.2003; Council of the European Union (2004), "Three-year report on the operation and the future of the European Police College", 5136/04, 8.1.2004.

a proposal for the adoption of an amendment to Council Decision 2005/681/JHA to provide CEPOL with a legal personality, while the United Kingdom delegation put forward in January 2003 a proposal to establish that the College's permanent seat be located in Bramshill, on the premises of the UK Police Staff College.[76] The JHA Council nonetheless concluded that "the organisation and structure of CEPOL should be kept under review" after the adoption of these proposals.[77] In October 2004, the European Commission introduced a proposal for a Council Decision establishing the CEPOL as a body of the European Union, in particular to provide the College with a clear staff regulation and the possibility of being financed through the Community budget.[78] Council Decision 2005/681/JHA, adopted on 20 September 2005, establishes the CEPOL as a body with legal personality, a permanent seat and staff, revenues drawing from a subsidy of the Community and considered as an agency for the purpose of staff rules.[79]

2.5.2. Ongoing debates and challenges

2.5.2.1. An administrative viability under question

Since its establishment as a body of the European Union, implemented in 2006, CEPOL has been placed under observation due to its handling of its budget. Starting in 2006, the reports of the European Court of Auditors (ECA) on the annual accounts of the College have highlighted a number of problems. For the year 2007, the Court noted the high level of carry-overs and cancellations of appropriations, the lack of a proper commitment accounting system, internal controls and cases where appropriations were used to finance private expenditures.[80] For the year 2008, the Court observed that some management problems persisted, together with difficulties tied to procurement procedures and to the migration to a new accounting system, as well as the absence of any ex-post control on the private use of appropriations it reported the year before.[81]

The ECA's report on the annual accounts of the College for 2008 led the European Parliament to postpone its decision on granting discharge to the Director of the CEPOL in respect of the implementation of the College budget for that year.[82] In the attached resolution, the European Parliament questioned the steps taken by the new Director of the College (Ferenc Banfi, appointed in February 2010), pointing out in particular that the "small size of the College calls into question its capacity to handle effectively the complexities of the EU's financial and staff regulation".[83] The refusal was confirmed by a second Decision, adopted in October 2010, based on the alleged 'vagueness' of the measures proposed by the Director of CEPOL regarding the financial management of the

[76] These proposals were adopted in July 2004. See Council Decision 2004/566/JHA of 26 July 2004 amending Decision 2000/820/JHA establishing a European Police College (CEPOL), OJ L251/19, 27.7.2004 ; Council Decision 2004/567/JHA of 26 July 2004 amending Decision 2000/820/JHA establishing a European Police College (CEPOL), OJ L251/20, 27.7.2004

[77] Council of the European Union (2004), "Three year report on the operation and future of the European Police College", 5880/04, 2.2.2004.

[78] European Commission (2004), Proposal for a Council Decision establishing the European Police College (CEPOL) as a body of the European Union, COM(2004) 623 final, 1.10.2004.

[79] Council Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA, OJ L256/63, 1.10.2005.

[80] European Court of Auditors (2008), "Report on the annual accounts of the European Police College for the financial year 2007 together with the College's replies", OJ C311/136, 5.12.2008.

[81] European Court of Auditors (2009), "Report on the annual accounts of the European Police College for the financial year 2008 together with the College's replies", OJ C304/124, 15.12.2009.

[82] Decision of the European Parliament of 5 May 2010 on discharge in respect of the implementation of the budget of the European Police College for the financial year 2008 (2010/556/EU), OJ L 252/232, 25.9.2010.

[83] European Parliament (2010), Resolution of the European Parliament of 5 May 2010 with observations forming an integral part of its Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year 2008, OJ L252/233, 25.9.2010.

College.[84] The same development occurred with regard to the accounts of the College for 2009, with the European Parliament initially postponing discharge on the basis of the ECA's report,[85] before finally granting it in its Decision of 25 October 2011.[86]

Despite the tensions arising from the questioning of CEPOL's administrative viability, these developments demonstrate what an effective control of the European Parliament over the activities of EU agencies, bodies and services in the field of internal security could look like.

2.5.2.2. Network or academy? The inheritance of past decisions and the possible merger with Europol

In the various resolutions accompanying its decisions on discharge in respect of the implementation of the CEPOL budget for 2008 and 2009, the European Parliament has mentioned repeatedly the fact that, given its current size and administrative difficulties in coping with the requirements of EU financial and staff regulation, the possibility of a relocation of the College and a merging of its responsibilities with those of Europol.[87] The difficulties encountered by the CEPOL, beyond specific individual responsibilities, are however largely an effect of the tension between the 'network model' and the 'academy model' that have informed discussions on European police cooperation in the field of training since the late 1980s.

The establishment of CEPOL as a body of the European Union, in this regard, did not bring any change to the situation. Besides giving the College legal personality, Council Decision 2005/681/JHA reproduces the orientations and language of Council Decision 2000/820/JHA. As reported in a letter from Caroline Flint, MP (at the time Parliamentary Under Secretary of State at the Home Office) to the House of Lords European Union Committee, the proposal from the Commission was initially met with fierce opposition from some Member State delegations, to the extent that discussions did not even take place at the meeting of the Police Co-operation Working Party (PCWP) that was supposed to examine it in December 2004.[88] The CEPOL Governing Board approved it, on the condition that "the role and position of the CEPOL network would not be affected and that the authority of the Governing Board would not be diminished".[89] The note accompanying the transmission of the final version of the Council Decision establishing CEPOL to COREPER notes in this respect that "the Council wishes to re-affirm that CEPOL maintains its network character […] notwithstanding certain provisions of the current proposal for a Council Decision".[90]

---

[84] Decision of the European Parliament of 7 October 2010 on discharge in respect of the implementation of the budget of the European Police College for the financial year 2008 (2010/756/EU), OJ L320/11, 7.12.2010.

[85] Decision of the European Parliament of 10 May 2011 on discharge in respect of the implementation of the budget of the European Police College for the financial year 2009 (2011/619/EU), OJ L250/268, 27.9.2011.

[86] European Parliament Decision of 25 October 2011 on discharge in respect of the implementation of the budget of the European Police College for the financial year 2009 (C7-0241/2010 – 2010/2181(DEC), pending publication in the Official Journal, 25.10.2011.

[87] European Parliament (2011), European Parliament resolution of 25 October 2011 with observations forming an integral part of its Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year2009 (C7-0241/2010 – 2010/2181(DEC)), A7-0330/2011, 25.10.2011.

[88] House of Lords (2004), Select Committee on European Union Fourth Report: Letter from Caroline Flint MP to the Chairman, London, 15 December 2004 (www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/16/16216.htm).

[89] Ibid.

[90] Council of the European Union (2004), Adoption of a proposal for a Council Decision establishing the European Police College (CEPOL), 10534/05, 24.6.2005, p. 1.

The merging of the College's training activities, in this respect, had already been discussed at the time when CEPOL's establishment as a body of the European Union was considered. However, both Europol and representatives of national police colleges were opposed to this scenario.[91] The five year external evaluation on the College, approved by the CEPOL Governing Board on 16 March 2011, suggest that this proposal is still currently met with strong opposition among the members of that body (80% dissenting opinions). It further points out that such a development would negate the efforts currently underway by EU JHA agencies to strengthen cooperation among themselves.[92] Rather than 'co-location' between the CEPOL secretariat and Europol, the evaluation suggests to examine the possibility of merging agency administrative functions such as audit or human resources management. In any case, the European Parliament has requested the ECA to conduct a study in the course of 2012 on the feasibility and effects of such a merger.

2.5.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS

2.5.3.1. The CEPOL five-year report

The CEPOL five-year report, adopted by the College's Governing Board on 16 March 2011, is the follow-up to the previous 2006 CEPOL two-year report and the 2003 three-year report.[93] It depicts an agency that is among the smallest of EU bodies in terms of budget and staff[94] - the often quoted figure here, including by the European Parliament resolutions on the College, is that the CEPOL Secretariat has around 20 staff, and 27 Member State representatives on its governing board. The report echoes other evaluations and the European Parliament's comments, in pointing out the problems raised by the size of CEPOL Governing Board meetings where some Member States can sometimes send several representatives, including with regard to the pace of decision-making in such conditions and the costs incurred by the organisation of large meetings.[95] CEPOL is also one of the few EU bodies, together with EUROJUST, where the European Commission holds a non-voting observer position on the Governing Board – despite having the power to define the amount of the subsidy granted to the College from the Community budget.

The CEPOL five-year report raises a number of questions as regards the future of the College in the context of the Lisbon Treaty and the ISS. These questions become particularly relevant when considering the emphasis placed on cooperation between JHA agencies in the activities of the COSI as well as in the CEPOL's own strategy document. They can be summarised as follows:

1. **Should CEPOL be made into a full agency of the European Union?** At the moment, CEPOL is considered an agency in its observation of EU financial and staff regulation, but its functioning is still heavily influenced by the tensions between the 'network' and 'academy' models in European cooperation in the field of police training. The other option here would be the discontinuation of CEPOL's autonomous activities and its re-location, both physical and administrative, within Europol. Making CEPOL a full agency of the EU, on the other hand, would mean revising Council Decision 2005/681/JHA. Such a revision would include reconsidering the division of labour between the Governing Board and the

[91] Ramboll-Euréval-Matrix (2009), "Evaluation of the EU decentralised agencies in 2009 – Final Report Volume III: Agency level findings", Brussels, December 2009, p. 25.

[92] Council of the European Union (2011), *CEPOL five-year report*, 7764/11, 17.3.2011, p. 41.

[93] See Council of the European Union (2006), "Two Year Report on the Operation and Future of the European Police College", 5727/06, 7.2.2006 ; Council of the European Union (2003), "Three year report on the operation and future of the European Police College", 15722/03, 9.12.2003.

[94] Compare with the report from the European Parliament's Budgetary Support Unit to the Committee on Budgets: Jones, Fabia (2007), "Agencies: origins of tasks, local conditions and staffing, PE 381.092, European Parliament, Brussels, 17.10.2007.

[95] See Council document 7764/11, op. cit., pp. 30-36.

Secretariat. The five-year report recommends for instance to reduce the size of the Governing Board and to clearly distinguish between operational tasks, entrusted to the Director, and strategic tasks, which would remain within the remit of the Governing Board.[96] By the same token, the possibility of granting voting rights to the Commission representative on the Governing Board would reflect the influence that this institution exercises over the budgetary orientations of CEPOL. Besides the merger with Europol, such transformations would also enable the European Parliament to ensure that its budgetary checks on the College and related observations have been taken into account.

2. **What should the priorities of CEPOL be?** The five-year report argues for a clarification of the College's mandate and a greater focalisation on European and cross-border issues, in line with the priorities laid out in the EU Internal Security Strategy and European Commission *ISS in Action* communication on serious and organised crime, terrorism and cyber-crime. In line with the observations laid out so far in the study, however, one could argue that there is also a need to further develop the work of CEPOL in the areas of accountability, transparency and fundamental rights in EU internal security policies, as well as in the promotion of a European area that effectively combines freedom, security and justice.

2.5.3.2. The status of training in EU internal security priorities and the CEPOL strategy

The discussion on CEPOL's standing in the current landscape of EU internal security agencies, bodies and services is indeed related to a broader issue, i.e. that of the status of training as a priority in EU internal security policies. In the EU Internal Security Strategy, training is associated with innovation and the use of technology for internal security purposes. The stated aim is to establish "law-enforcement, judicial and border management authorities that have advanced technology and are at the forefront of their specialisation", to promote "a shared culture among European law-enforcement bodies" and to facilitate transnational cooperation.[97] The model advocated by the EU ISS, however, is of distributed training responsibilities among "European agencies and bodies, especially CEPOL".[98]

These specifications raise three questions:

1. **Should European cooperation in the field of training be aimed at specialisation?** CEPOL activities are already focused on senior- to middle-management police officers. The ISS further seems to suggest that training should be delivered in priority to specialised police units, in order to reinforce their already highly focused areas of competence. **Should an effort be made, in this regard, to reach out to local and municipal police forces, which might be the ones confronted on the most regular basis with the criminal activities that mostly concern EU citizens?** In a similar way, the promotion of a 'shared culture' goes hand in hand with common understandings of criminal offences. In its recently adopted report on organised crime in the European Union, the European Parliament calls for example on the Commission "to submit, by the end of 2013, a proposal for a directive which contains a more concrete definition of organised crime and better identifies the key features of the phenomenon".[99] Legal definitions and operational definitions of organised crime used in the work of EU agencies, bodies and services have also been found to be contradictory in some cases.[100]

[96] Ibid., pp. 104-106.

[97] Council document 5842/2/10, p. 16.

[98] Ibid.

[99] European Parliament (2011), *Report on organised crime in the European Union (2010/2309(INI))*, A7-0333/2011, 6.10.2011, p. 10.

[100] V. Mitsilegas (2011), The Council Framework Decision on the Fight against Organised Crime: What can be done to strengthen EU legislation in the field?, PE 453.195, European Parliament, Brussels, 7.2011.

Here the CEPOL could provide some inputs, on the basis of the work that it is supporting on police research and science, bringing together academics and practitioners, but also through its post-course evaluation work, which was identified as a well-functioning area of CEPOL activities in the five-year report on the College.[101]

2. **Should training responsibilities be distributed among EU agencies, bodies and services?** Previous points have highlighted the tension between the notion of a European Police College, related in its form to a 'police academy' model, and its actual functioning as a network. **Should the reinforcement of CEPOL, rather than its physical and administrative re-location within Europol be considered, one issue for discussion is clearly whether it is interesting to have different training networks**, e.g. such as the Frontex Partnership Academies network. Since CEPOL is already operating as a network, there is hardly any possibility that such a discussion might lead to the constitution of a centralised, EU-wide facility for the training of all internal security professionals, or that the specific training requirements of each profession (e.g. customs, border guards, organised crime units or gendarmerie-like forces) would eventually be denied. It would also reflect ongoing cooperation, for example between CEPOL and FRONTEX, or the work being conducted by CEPOL and EUROJUST on the development of a common curriculum on EUROJUST.[102]
3. **Should a 'shared culture' among EU internal security agencies, bodies and services promote the AFSJ as a whole?** The new legal framework introduced by the Lisbon Treaty implies that European internal security professionals will regularly have to assess how their activities relate to the Charter of Fundamental Rights and the case-law of the ECJ. Human Rights are specifically mentioned as a training priority in the CEPOL strategy for the next five years adopted a year ago.[103] It does not, however, explicitly envisage coordination mechanisms between the College and bodies such as the European Data Protection Supervisor and the Fundamental Rights Agency, which could certainly contribute to the devising of common curricula alongside the work already done on judicial matters with EUROJUST.

2.6. EUROJUST

2.6.1. Background on the agency

- 1999: The decision to establish a permanent judicial co-operation unit to improve the fight against organised crime and transborder crimes is taken during the Tampere Council.
- 2002: EUROJUST is formally established (Council Decision 2002/187/JHA setting up EUROJUST)

EUROJUST constitutes the first European judiciary unit in charge of coordinating and promoting cooperation between Member States in relation to criminal justice. Its mission is to enhance the development of cooperation on criminal justice cases throughout Europe. Its intergovernmental dimension has for consequence that each prosecutor sitting in the College of EUROJUST is a 'national member' representing his own Central authorities. EUROJUST is composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to its legal system.

[101] Council document 7764/11, op. cit., p. 108.

[102] For an overview, see the examples provided in Council of the European Union (2011), "Report on the cooperation between JHA Agencies in 2010", 5675/11, 25.1.2011.

[103] Council of the European Union (2010), "CEPOL Strategy", 15068/10, 18.10.2010.

- 2005: EUROJUST developed an autonomous system of data management

Following the adoption of rules of procedure concerning the treatment and the protection of personal data by the Council on 24 February 2005, EUROJUST established an autonomous system of data management (Case Management System – CMS). The aim of CMS is the safe exchange of judicial information between EUROJUST members and national judicial authorities. In 2006, EUROJUST started developing a system of data treatment through the E-POC (European Pool against Organised Crime) project framework III, in order to improve information exchange between various national support E-POCs. EPOC III+ was launched in April 2008 with the aim of increasing the user-friendliness of the CMS.

- 2007: the European Commission proposed legislation for increasing the powers of EUROJUST.

The proposals include the harmonisation of the powers held by the national representatives, which currently vary, with a minimum set of powers and a minimum three year long renewable term to increase continuity. Members would also have automatic access to national databases, terrorist cases, and criminal, DNA and prison records. In particular, the connection of EUROJUST to the Schengen system went live in December 2007. This connection allows EUROJUST national members to access the SIS system.

- The Council Decision 2009/426/JHA on the strengthening of EUROJUST entered into force in 2009.

The significant changes that it introduces in the legal framework of EUROJUST required substantial implementation efforts from both the Member States and EUROJUST that are still underway[104]. The Decision gives a central place to strengthening EUROJUST casework capacities. The Decision makes new powers available to EUROJUST; information flows and co-ordination with national authorities are facilitated; the 24/7 nature of EUROJUST's work is put on a formal basis; and EUROJUST host the Secretariat of the Network for Joint Investigation Teams and other network secretariats.

2.6.2. Ongoing debates and challenges

2.6.2.1. An agency in search of a positioning

The EUROJUST's search for an identity cannot be understood without taking into account EUROJUST counterpart in the European security landscape: EUROPOL. **The main problem of EUROJUST is its positioning in between prosecution (Home Affairs) and Justice (including Human Rights).** While some actors wished the creation of EUROJUST to see it one day control EUROPOL and at the very least prove European judicial cooperation more efficient than police cooperation, these ambitions have ever since been fully abandoned. It seems that the relations between police and justice at the European level have rather evolved in favour of the police component. Indeed, EUROJUST's College is nearly exclusively composed of national prosecutors (a part from the police officers appointed by some countries in accordance with their national systems and from the notable exception of the Austrian member) – in other words of magistrates from the respective Member States accusatory authorities. This development is crucial because the latter are increasingly following or at least submitted to an intelligence-led rationale. Indeed, although prosecutors focus on deeds of 'real' individuals (as opposed to profiles), their main role is to assist the police in transforming the data collected into legally compelling evidence that can be used in a court of law. In this respect, given the preventive logic prevailing in judicial and investigatory police activities since 9/11, prosecutors are *de facto* involved in the intelligence approach to threats as opposed to an

[104] See House of Lord (2004), "Judicial Cooperation in the EU: the role of Eurojust", Special Report, London.

approach focusing on the rights of the defence. At the European level, we are hence witnessing a dual judicial subfield: one mainly linked to prosecutors and very close to the accusatory authorities of the Member States and a second more marginalised one focusing less on the accusation than on procedural rights and especially the rights of the defence. Since the division of DG JLS in the European Commission, EUROJUST is dealt with by DG Justice, which does not contribute to clarify this aspect.

2.6.2.2. An agency in search of recognition

Furthermore, in comparison to other agencies, EUROJUST has been less visible and publicized in the European landscape since its establishment. Even though EUROJUST has pulled great efforts in the last years to improve its image in the European public, through marketing exercises (such as conferences at the *Ecole Nationale de la Magistrature* – ENM, College de Bruges, etc), EUROJUST still suffers from a lack of recognition. As reminded by some of the EUROJUST staff, EUROPOL rings a bell in public opinion because of the "POL" suffix that is understandable. It's not the case for EUROJUST, and no one really knows what EUROJUST is precisely doing.

Some Joint Investigations Teams (JITs), with measurable effects both in terms of operational efficiency and effective cooperation with EUROPOL constitute few exceptions where EUROJUST is advertised publicly. 'Operation Koala', a case involving sexual abuse of children is for instance often presented as one of the success stories of EUROJUST. The operation began in 2006 and involved offenders from Australia, Belgium, and Italy. Success was achieved in this operation by the provision of valuable data by Member States and Interpol and crime analysis for more than a year carried out by specialists in online child sex abuse cases at EUROPOL and the judicial co-ordination carried out by EUROJUST. EUROJUST and EUROPOL, working in close co-operation, invited representatives from 28 countries to several operational meetings in The Hague. At EUROJUST, the Belgian and Italian National Members took the initiative to co-ordinate, on a judicial level, all the countries involved. Subsequent investigations were initiated by the national authorities, which led to a significant number of arrests and the seizure of a considerable amount of child abuse material.

The under-use of EUROJUST capacities has been indeed an ongoing challenge since its establishment in 2002. Even if EUROJUST multiply initiatives to publicize its tools and 'added value', lack of information prevails and explains partly some MS' reserves to refer to EUROJUST in criminal investigations. Mutual trust and the importance of informal or personal relations are still privileged to improve the cooperation logic. Noticeable evolutions are underway, with a significant increase of co-ordination meetings. Such meetings have become the most common vehicle for the exchange of information on linked investigations and for planning joint actions. These meetings allow competent national authorities and EUROJUST National Members, including representatives from relevant EU partners such as EUROPOL and OLAF, where appropriate, to agree a common strategy between Member States, to plan and co-ordinate simultaneous investigations and actions (such as arrests, searches, and seizure of property), to anticipate and resolve legal difficulties, and to facilitate the execution of subsequent Mutual Legal Assistance (MLA) requests. The 2009 figures available in EUROJUST annual report show that most meetings were requested by France, the UK and Italy, with 29, 19 and 14 co-ordination meetings, respectively.

The 2009 EUROJUST report gives optimistic views on these matters and underlines a substantial increase in the number of cases that Member States referred to EUROJUST. There was a 15 per cent rise in caseload compared to the preceding year, with almost 1,400 new cases registered on EUROJUST's Case Management System. The setting up of Joint Investigation teams (JITs) is also seen as a real improvement to overcome MS reserve. Nevertheless, the lack of information about the possibilities offered by the Framework Decision of 13 June 2002 on Joint Investigation Teams, as well as the practitioners' lack of familiarity with the concept of JITs, have been constantly targeted as problems. In an effort to remedy the situation, the JIT Manual, created jointly by

EUROJUST and EUROPOL, is now available as Council Document 13598/09 of 23 September 2009 in all 23 official languages.

However, the EUROJUST report does not mention the difficulties encountered in JITs. If a JIT does indeed facilitate cooperation, successful cooperation remains dependent on numerous other factors, such as clear legal framework, mutual understanding and agreement between various MS and professional cultures, and, more importantly, on a willingness to engage in intensified cooperation on the strategic, the operational, as well as the political level.[105] Moreover, if the establishment of the European Arrest Warrants (EAWs) is presented in EUROJUST Reports as a EUROJUST 'added value', the legal obstacles are indeed difficult to overcome. In 2009 the legal instruments most often used in judicial co-operation were the 1959 and 2000 Mutual Legal Assistance Conventions, and the Framework Decision of 13 June 2002 on the EAW and the surrender procedures between Member States. A total of 256 cases were registered at EUROJUST in 2009 concerning the execution of EAWs. This figure amounts to almost 19 per cent of all cases registered in the year. However, numerous problems have been flagged by Member States, European and national parliamentarians, groups from civil society and individual citizens' in relation to the operation of the EAW[106]:

- no entitlement to legal representation in the issuing state during the surrender proceedings in the executing state;
- detention conditions in some Member States combined with sometimes lengthy pre-trial detention for surrendered persons;
- non-uniform application of a proportionality check by issuing states, resulting in requests for surrender for relatively minor offences that, in the absence of a proportionality check in the executing state, must be executed.

However, as a result of the entry into force of the Lisbon Treaty and the legally binding nature of the Charter of Fundamental Rights, the provisions in the Lisbon Treaty governing legislative instruments in the area of police and judicial cooperation have changed the context in which the EAW operates. The Commission is currently working on a roadmap for strengthening the procedural rights of suspected or accused persons in criminal proceedings. The roadmap indentifies the following six priority measures: the right to interpretation and translation; the right to information about rights (Letter of Rights); pre-trial legal advice and at-trial legal aid; a detained person's right to communicate with family members, employers and consular authorities; protection for vulnerable suspects; a green paper on pre-trial detention.

2.6.3. Key areas of concern for the future in the context of the Lisbon Treaty and the ISS

The key areas of concern are the following:

1. EUROJUST and a quest for a renewed position in the security landscape;
2. The issue of Data regulation & protection;
3. EUROJUST' accountability ;
4. Articles 85 (powers of initiating investigations) & 86 (EPPO) of the Lisbon Treaty

[105] C. Rijken (2006), "Lessons learnt from the first efforts to establish a JIT", *www.utrechtlawreview.org/* Volume 2, Issue 2.

[106] See COM(2011) 175 final, Brussels, 11.4.2011. REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL On the implementation since 2007 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

2.6.3.1. EUROJUST and a quest for a renewed position in the security landscape

Within the EU security landscape, EUROJUST is often perceived as an 'outsider'. For instance, many EUROJUST representatives lament the fact that the EUROJUST contribution in OCTAs and TE-SATs is underestimated, and that EUROJUST is not invited to present the TE-SATs along with EUROPOL at the European Parliament. At the national level, the fact that none of the EUROJUST staff has been invited to submit evidences or participating to the hearings undertaken by the House of Lords EU Sub-Committee (Home Affairs) investigating the EU ISS is quite enlightening. This example is even more explicit when the fact that UK is one of the most frequent 'client' of EUROJUST capacities is taken into account.

At the European level, EUROJUST has been almost 'forgotten' in the elaboration of the ISS. A member of EUROJUST confessed that the participation of EUROJUST in the joint report (EUROPOL, EUROJUST, FRONTEX) has been negotiated *in extremis*. Most of the EUROJUST described a feeling of "unease" when it comes to ISS and underlined the police prevalence, the persistent lack of understanding between magistrates and police representatives. At the COSI meetings, only France, Belgium and Netherlands send representatives of the judicial authorities. A certain current degree of frustration is perceivable.

Among them, the quest for legitimacy of EUROJUST in counterterrorism issues is perceivable. Even if terrorism cases represent no more than 21 cases in 2009 and have known a constant decrease since 2004, EUROJUST claims for its added value in the field. After the Madrid Bombings, EUROJUST took the initiative to set up technical meetings and to build up a network, in order to have a clear view of the legislative implementations. According to EUROJUST members of staff, EUROJUST has acted since as a facilitator for judicial cooperation in terrorism cases. Where EUROPOL claims for its added value in terms of prevention and anticipation, EUROJUST claims for the acknowledgment of its value at the 'end of the cycle', i.e. on convictions. Furthermore, EUROJUST is investing since 2008 in a 'terrorism convictions monitor' (TCM) which gathers information on terrorism convictions and acquittals based on open sources and provides analytical and statistical information.

EUROJUST also promote its role in OCTAs and T-SATs Reports. EUROJUST has indeed contributed to the last OCTA Report. Frustrations generated by this undermined contribution have been numerous. The result is that EUROJUST is thinking of producing its own report on Organised Crime. On Te-Sat Report, according to the team responsible for providing information to EUROPOL analysts, you can easily identify part of the report made by EUROJUST, with no mentions of EUROJUST contributions.

According to some EUROJUST officials, substantial contributions should be channelled through EUROJUST participation in COSI meetings. The idea of EUROJUST acting as a mediator between the Consultative Forum of the General Prosecutors and Directors of Public Prosecutions and COSI is underway. This forum, established in 2010 and consisting of the Prosecutors-General and the Directors of Public Prosecutions from among the 27 Member States of the European Union, meet at the invitation and under the direction of the country holding the Presidency of the EU Council and takes place at the headquarters of EUROJUST in The Hague. The aim of such meetings is the building of a network of contacts between senior officials of the Member States of the European Union responsible for the judicial system.

More generally, **EUROJUST is clearly seeking an identity in the ISS, while trying to increase its involvement in the EU security landscape**.

2.6.3.2. The issue of data regulation & protection

In handling personal and other data EUROJUST is subject to the data protection provisions of the EUROJUST Decision. A Data Protection Officer has been appointed in 2003. Although working under the authority of the EUROJUST College, the Data Protection Officer has an independent role in ensuring the lawfulness and compliance of EUROJUST

processing of personal data with the requirements of the Decision. External supervision is provided by an independent Joint Supervisory Body.

As rightfully underlined by the LIBE Committee in his report (LIBE Report 2008 A6-0293/2008), **it is of critical importance to ensure an adequate level of personal data protection in activities of EUROJUST**. Taking stock of the strong data protection system established at EUROJUST, the rapporteur submitted additional safeguards to data protection at EUROJUST. In particular, the Rapporteur highlighted the following amendments:

1. Persons who have been the subject of a criminal investigation based on a EUROJUST request but have not been prosecuted should be informed about that investigation no later than one year after the decision not to prosecute has been taken;
2. Only personal data on persons who are witnesses or victims in a criminal investigation or a prosecution can be processed. No other data can be processed
3. In case of data sharing with third parties, it is important to clarify how adequacy of data protection level could be assessed and not to leave to third parties and organisations to decide upon that on a case-by-case basis. Indeed, it is not yet clear what happens afterwards to the information transmitted to partners (international organisations and bodies and third countries).

In the 2008 Council Decision on the strengthening of EUROJUST, EUROJUST should be authorised to process certain personal data on persons who, under the national legislation of the Member States concerned, are suspected of having committed or having taken part in a criminal offence in respect of which EUROJUST is competent, or who have been convicted of such an offence. Furthermore, EUROJUST is given the opportunity to extend the deadlines for storage of personal data.

The elusive formulation of the Decision requires full attention and, therefore EUROJUST' future use of data should be monitored. In particular, any process of personal data should receive further EP attention. Under the changing of circumstances provided by the Lisbon Treaty (co-decision), the European Parliament can now be more involved in data protection issues and should receive reports prepared by the Joint Supervisory Body of EUROJUST on that matter. Among the review mechanisms, by June 2014, the Commission is to review data exchange between EUROJUST's national members. By June 2013, EUROJUST is to report to the Council and the Commission on the provision of national access to its case management system. The process of data and the subsequent 'technological' challenges are detailed further in the section 3.2.

2.6.3.3. EUROJUST accountability

As advocated by the LIBE Committee, information on operation of EUROJUST should not only be sent to the European Parliament. The possibility to hear a EUROJUST representative coming in person, and allowing Members of the European Parliament to ask questions and to have a debate should be established on a regular basis. However, **the form of the involvement of the European Parliament and national Parliaments in the evaluation of EUROJUST's activities remains to be determined**.

2.6.3.4. Articles 85 & 86 of the Lisbon Treaty: power of investigations and the European Public Prosecutor

On a longer-term basis, the Lisbon Treaty opens up two areas for debate concerning EUROJUST: the power to initiate investigation (article 85), and the possibility of a European Public Prosecutor's office - EPPO (article 86).

EUROJUST is seen as the origin of any future EPPO, the creation of which is provided for under the Lisbon Treaty (Article 86 TFEU). However, if the Lisbon Treaty opens up the debates, the strong resistance of some MS (notably UK and the Netherlands) shall not be overcome in a near future. Furthermore, and as debated during the strategic seminar

organised by EUROJUST ("EUROJUST and the Lisbon Treaty: towards more effective action", Bruges, September 2010), the possibilities of an EPPO require many clarifications of critical importance such as:

1. Which crimes will be under the competence of the EPPO and from which definitions (the definitions of the national criminal law systems or those of the EPPO's regulations?);
2. Would it be a centralised or a decentralised body?
3. Would the authorities work only within the EPPO and/or also for the Member States?
4. How the relationship between EUROJUST and EPPO will be agreed? If the power to 'initiate' according to Article 85 is made use of, are the services of the EPPO rendered dispensable? And is the continued development of EUROJUST necessary if the EPPO is established?

Moreover, once the structure of the EPPO is better defined, answers to other questions should be found as well, such as those concerning the gathering of evidence, defence, appeals, possible harmonisation, and recognition of other Member States' standards.

Article 85 offers concrete possibilities to give more operational powers to EUROJUST, and opens the possibility for EUROJUST to initiate investigations particularly those relating to offences against the financial interests of the Union. As an addition, the 2009 Decision grants EUROJUST binding powers to ask MS to initiate investigations. However, at the present time, EUROJUST is still a simple 'mediator', without any decision-making or binding powers with regard to prosecution.

2.7. The undefined role of the Counter Terrorism Coordinator, OLAF and SitCen

In the ISS strategy, some of the JHA actors directly linked to judicial and police cooperation seem to have been left apart, marginalised, or ignored. Their role in the ISS context is therefore unclear.

2.7.1. The EU Counter Terrorism Coordinator

The future role of the Counter Terrorism Coordinator (CTC), for instance, is not obvious in an ISS context. This position, created in 2004 after the Madrid bombings of March 2004, has been held by Gilles de Kerchove since 2007. The CTC operates within the Council Secretariat and has the responsibilities of coordinating the counter-terrorism work of the JHA Council (including a multitude of working groups and working parties); maintaining an overview of the relevant EU instruments in this area; ensuring effective follow-up of Council decisions; monitoring the implementation of the EU Counter-Terrorism Strategy, including making reports to the Council; fostering better communication between the EU and third countries; and ensuring that the EU plays an active role in the fight against terrorism as a whole. As underlined in the House of Lords Report on the EU ISS, while the ISS does not exclude a continuing role for the CTC, the extent to which his role would overlap with COSI's work for instance is uncertain. As reminded by the CTC in his latest EU Action Plan on combating terrorism (2010), 'The Lisbon Treaty offers new possibilities for the European Union collectively – the Member States and the European Institutions - also in the field of counter terrorism. Many steps to implement the treaty have yet to be taken. All players have to adjust and to adapt to the new situation. Especially in the field of external relations, the creation of European External Action Service offers new opportunities to better coordinate between traditional external policy instruments and internal instruments. The CTC will continue his

contribution to this cohesion of internal and external aspects'. The CTC is indeed now positioning himself to play a major role in coordinating the internal/external aspects of terrorism. However, **its positioning and its role *vis a vis* the External Action Service remain to be defined, and the value of its contribution assessed.**

2.7.2. The European Anti-Fraud Office (OLAF)

The positioning of the European Anti-Fraud Office (OLAF) in an ISS context is even vaguer. While the Action Plan Implementing the Stockholm Programme mentions the 'crucial' role of OLAF, OLAF continues to appear somehow as a kind of 'ghost agency', with undefined tasks. Even if OLAF may have a revival under the current Euro Crisis, and despite practical agreements among the agencies, OLAF fiercely protects its autonomy and is excluded from the collaborative efforts (which have been quite difficult for years and not totally satisfactory) undertaken by EUROPOL and EUROJUST. Despite shy progresses (such as the first visit of the OLAF's director at EUROJUST in July 2011), OLAF seems to act a 'free electron' in the European security landscape.

2.7.3. The EU Situation Centre (SitCen)

The EU Situation Centre was established following the appointment of Javier Solana as High Representative for the Common Foreign and Security Policy and Secretary General of the Council of the European Union by the Cologne European Council (June 1999). It was initially envisaged as the equivalent of the Operational Centre created within the State Department in 1961, during the planning stage of the Bay of Pigs attack on Cuba, but became over the years a meeting point for Member State civilian intelligence agencies with internal and external remits (e.g. the French *Direction Générale de la Sécurité Extérieure* DGSE and *Direction Centrale du Renseignement Intérieur* DCRI, the British MI-5 or the German Federal Office for the Protection of the Constitution BfV). The development of these intelligence functions has not been precisely documented.[107] It is tied, on the one hand, to the perceived need among the members of the Policy Planning and Early Warning Unit attached to the position of the High Representative (out of which the first director of SitCen, William Shapcott, would be selected) to have access to information (mainly that circulated within the diplomatic networks of the Member States) on pressing issues.[108] It involves, on the other hand, the interest expressed by some Member States in the framework of the Counter-Terrorism Group (CTG[109]) to circulate information and detach experts from internal security services to SitCen following the attacks of 11 September 2001 in the United States and the bombings of 11 March 2004 in Madrid. The SitCen in itself was established without a legal basis in the Treaties, through an administrative decision of Javier Solana acting as Secretary General of the Council, in order to avoid locating it within either the EU's Second or Third Pillars.[110]

---

[107] For an 'insider's' view, see the transcript of the hearings of former SitCen Director (2000-2010) William Shapcott at the House of Lords' European Union Committee: House of Lords (2005), "European Union Committee 5th Report of Session 2004-05 - After Madrid: the EU's response to terrorism - Report with evidence", London: The Stationery Office Limited; House of Lords (2011), "European Union Committee 17th Report of Session 2010-12 – The EU Internal Security Strategy", London: The Stationery Office. For "outside" views, see the analysis published by the European Union's Institute for Security Studies, B. Müller-Wille (2004), "For our eyes only? Shaping an intelligence community within the EU", *Cahiers de Chaillot Occasional Papers*, No. 50, as well as the Eurowatch analysis in J. van Buuren (2009), *Secret Truth: The EU Joint Situation Centre*, Amsterdam: Eurowatch.

[108] House of Lords (2005), "After Madrid", op. cit., pp. 53-54.

[109] Established shortly after the events of 11 September 2001, the CTG is an offshoot of the Berne Club focused on issues related to terrorism. The Berne Club is an informal structure for the exchange of information between representatives of counter-intelligence services of European countries, originally established in the 1970s.

[110] As then-SitCen Director William Shapcott pointed out to the House of Lords in 2005: "the Situation Centre has always been in the Secretariat. We have been quite careful, even from the beginning, not to formally have it in […] the Second Pillar. We have played with Solana's double-

Until the entry into force of the Lisbon Treaty, the SitCen has thus operated across the 'pillar divide'. Several partially declassified documents from the Council suggest that the SitCen's Counter-Terrorism Cell has been providing reports to the Working Party on Terrorism, for instance, and there have been attempts at promoting cooperation with EUROPOL, particularly in the context of the latter's TE-SAT reports.[111] SitCen does not, however, have its own intelligence-gathering capacities. It deals with so-called 'assessed intelligence', i.e. intelligence reports that are the outcome of analytical work conducted by the intelligence services of the EU Member States, and which are synthesised and combined by SitCen analysts. The main exception is the work conducted by SitCen on persons of interest for the CP931 Working Party, created in 2007 to replace the informal consultation mechanism among Member States authorities for the implementation of Common Position 2001/931/CFSP and Council Regulation (EC) No. 258/2001 on the placing of persons and groups on the EU terrorist list and the freezing of their financial assets.[112]

Following the entry into force of the Lisbon Treaty, the Council adopted Decision 2010/427/EU establishing the organisation and functioning of the European External Action Service.[113] Article 4(3)(a) of the Decision transfers different bodies and services of the Council to the EEAS, including the SitCen. It nonetheless establishes that despite this transfer, "the specificities of these structures, as well as the particularities of their functions, recruitment and the status of the staff shall be respected". This provision raises a question as regards SitCen. **Should SitCen be authorised to continue operating across the EU's internal and external security policies despite having been transferred to the EEAS? Where does the responsibility of the activities undertaken by SitCen lie?** The Centre now officially falls under the responsibility of the High Representative, but is still intended to report to Council bodies in charge of internal security. The outcome of proceedings of the CATS meeting held on 11 February 2010, for example, highlight that the "Director of SITCEN, Mr Shapcott, reassured delegations that SITCEN would continue to provide its usual services to the Terrorist Working Group, CATS, and the Council for JHA policies, also during and after its integration into the External Action Service".[114] The response of the Council Secretariat to the questions on the current status of SitCen raised by MEP Martin Erhenhauser in January 2011 emphasise in this respect the limitative provision laid out in Article 4(3)(a) of Decision 2010/427/EU.[115] Finally, the appointment in December 2010 of the head of the Finnish *SuPo*, a security service with a remit for both internal and external security issues, at the head of SitCen,

---

hatting. He is the Secretary General; we are attached to his cabinet, so we are squarely in the Secretariat General. We are not exclusively a Second Pillar body. As discussion about our role has developed, Justice and Home AVairs ministers have said, "We don't know much about the SitCen and is that not something that works for Solana?" and we have said, "Come what may, in the future our goal is to work for you. We very much want Justice and Home AVairs ministers to be co-owners of this project; to control it, to the extent that their interests are the interests of the services which they supervise and are involved; and to be customers, quite clearly". House of Lords (2005), *After Madrid*, *op. cit.*, pp. 60-61.

[111] See Council of the European Union (2005), *EU SitCen Work Programme*, 5244/05, 11.1.2005 (declassified 20.12.2005); Council of the European Union (2007), *Overview of SitCen reports and Political Recommendations*, 7261/07, 12.3.2007 (declassified 28.5.2009).

[112] Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP), OJ L344/93, 28.12.2001; Council Regulation (EC) No. 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, OJ L344/70, 28.12.2001.

[113] Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU), OJ L201/30, 3.8.2010.

[114] Council of the European Union (2010), "Outcome of proceedings of CATS on 11 February 2010", 6557/10, 11.2.2010, p. 4.

[115] Council of the European Union (2011), "Expansion of the Joint Situation Centre (SitCen)", 5626/11, 24.1.2011.

confirms the notion that despite its relocation within the EEAS, SitCen will continue to operate along established venues.

2.8. Current trends in agency and institutional cooperation in EU internal security policies

2.8.1. Cooperation between EU agencies, bodies and services in the field of internal security

Cooperation between EU agencies in the field of internal security has become a significant stake in the last two years. In October 2009, following an informal meeting of the JHA Council, The Swedish presidency requested EUROPOL to draft a report on relations between the four EU 'JHA agencies' (CEPOL, EUROJUST, EUROPOL, FRONTEX). This report was forwarded to COSI and the JHA Council on 9 April 2010.[116] In January 2011, the four agencies submitted a scorecard to COSI together with a report, to provide feedback on progress in the implementation of the actions envisaged in their 2010 report.[117] The following pages provide a general assessment of these relations (2.6.1.1.), and further detail three dimensions: the formal relations between the agencies, the working relations beyond formal agreement on cooperation, and the state of information exchanges and information flows between them, including strategic/operational information and personal data when applicable. For the last two entries, only the most significant relations are emphasised.

2.8.1.1. General assessment

EUROPOL can be seen as one of the main 'winner' of the ISS. As underlined previously, the agency has deployed numerous communication products and is gaining a status of leadership in many areas, such as threat assessments, database and technical platforms. EUROPOL is certainly a major agency at the centre of the European security issues. According to the EUROPOL staff, EUROPOL has gained legitimacy, as the agency protect efficiently sensitive intelligence and is in the 1st league in terms of strategic and operational work. As proudly reminded during our visit at the Agency, the added value of EUROPOL has been assessed very positively by an independent organization, EPSI Rating.[118] Operation Rescue (March 2011) is also presented by EUROPOL representatives as an insightful example of what EUROPOL is now able to achieve. This operation works as a 'showcase', which has a 'real life input' ("some children were safe"). The Operation indeed led to the disruption of an international (from Australia to Italy) child sex abuse network. The EUROPOL staff is also very confident on the future of their work and inputs, and highly advocate the further development of their 'niche products', such as the "Check the web" or the OCTAs, forthcoming SOCTAs and TE-SATs reports. As mentioned earlier, the current positioning of EUROPOL in the field of cybercrime, and its claim to host the European cybercrime centre is very much in line with this strong position of EUROPOL in the ISS.

The second agency to benefit from the current state of play in EU internal security policies is FRONTEX. As shown above, the agency should see its mandate reinforced, with increased control over the initiating of joint operations and pilot projects. Much like EUROPOL, it appears to be gaining an increasingly central role in the collect and analysis of information regarding the external borders, in the field of risk analysis and threat assessment on the one hand, and with regard to access to electronic data, including the

[116] Council of the European Union (2010), "Final report on cooperation between JHA Agencies", 8387/10, 9.4.2010.

[117] Council of the European Union (2011), "Report on the cooperation between JHA Agencies in 2010", 5675/11, 25.1.2011; Council of the European Union (2011), Draft Scorecard – Implementation *of the JHA Agencies report*, 5676/11, 9.4.2010.

[118] See www.epsi-rating.com/

processing of personal data, on the other. In the longer run, the coming online of EUROSUR is likely to place the agency in the position of an intelligence body.

The two other main JHA agencies, EUROJUST and CEPOL, appear in a much weaker position. Does this point to a tendency to reinforce the security, coercive aspects of the AFSJ to the detriment of its justice and freedom components? While agencies such as EUROPOL and FRONTEX are mentioned at several points throughout the ISS, the section does not make any reference to the EDPS or the FRA for instance. It seems that the 'Freedom' agencies have been included at the margin of the ISS, underlying significantly how the fundamental rights challenge detailed in the next chapter is of paramount importance.

2.8.1.2. Formal relations between agencies, bodies and services

Over the past five years, all four EU JHA agencies have concluded formal cooperation agreements with each other. They are detailed in the following pages (for a synthetic view, see **Table 4 in the Annex**). The only exception is the relation between EUROJUST and FRONTEX, which are still to complete their negotiations on this matter.

- **CEPOL / EUROJUST Memorandum of Understanding**

A Memorandum of Understanding (entered into force on 1 January 2010) is in place between **EUROJUST and CEPOL**, the goal of which is to define, encourage and improve training for police and prosecutors in the fight against serious crime. Co-operation between EUROJUST and CEPOL continued to develop through EUROJUST's support of CEPOL's training activities, and CEPOL's attendance at EUROJUST seminars and conferences. EUROJUST and CEPOL have agreed to explore the options to establish training of senior police officers and prosecutors about JITs. In addition, EUROJUST will contribute to the development and implementation of course materials and a Common Curriculum on EUROJUST.

- **CEPOL / EUROPOL**

CEPOL has signed a strategic agreement with EUROPOL, which entered into force on 1 September 2007, on the basis of Article 8(1) of Council Decision 2005/681/JHA. The purpose of the agreement (Article 1) relates to the strengthening of training activities for senior police officers and involves both the organisation of training activities and the development of training material such as common curricula and course contents. Through this agreement, EUROPOL has obtained the formal possibility to perform updates in the EUROPOL common curriculum implemented by CEPOL. The agreement enables the establishment of contact points between the two agencies (Article 2), as well as the possibility for exchanges of information (excluding personal data) for the purpose stipulated in Article 1 (Article 5).

- **CEPOL / FRONTEX**

CEPOL and FRONTEX signed a cooperation agreement, which entered into force on 25 June 2009. The dispositions of the agreement mirror that of the CEPOL/EUROPOL strategic agreement.

- **EUROJUST / EUROPOL agreement**

From a legal and formal perspective, the first EUROJUST/EUROPOL agreement, signed in 2004, has been replaced in 2009. The new agreement takes stock of the Council Framework Decision of 13 June 2002 on Joint Investigation Teams (JITs), the Council Decision of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism, the Council Decision of 2009 implementing the rules governing EUROPOL's relations with partners, including the exchange of personal data and classified information. The 2009 agreement (entered into force in January 2010) covers the following areas: consultation and cooperation between the two agencies

(including the JITs), the Exchange of information, processing of information, and the issue of confidentiality.

- **EUROPOL/EMCDDA cooperation agreement**

EUROPOL has a cooperation agreement with EMCDDA since 2001. The purpose of this Agreement is to enhance the co-operation between Europol and the EMCDDA in particular through the exchange of strategic and technical information on drug-related issues and money laundering. However, and as analyzed further in the section devoted to the "Current trends in agency and institutional cooperation in EU internal security policies", the cooperation agreement is limited to a strict law enforcement perspective.

- **EUROPOL/FRONTEX**

The Strategic Agreement between EUROPOL and FRONTEX entered into force on 29 March 2008. It was the first agreement concluded by FRONTEX with another JHA agency. The main purpose of the Agreement, as laid out in its Article 1, is the exchange of strategic and technical information. The Agreement as it currently stands explicitly excludes the exchange of personal information, though the degree to which this might change in the future due to the revision of the FRONTEX Regulation will require scrutiny. The type of information exchanged between the two agencies on the basis of this agreement is specified below (2.6.1.4.). The agreement establishes a basis for contacts both at management level and at unit level (Article 4). It also lays down dispositions for the exchange and use of expertise between the two agencies, for training purposes as well as the provision of expertise (Article 6). It further establishes the possibility for the two agencies to exchange confidential information (Article 7 and 8), on the basis of a principle of equivalent protection (information received by one Party should be given an equivalent level of protection as that used by the sending Party) and by limiting such exchanges to the EUROPOL RESTRICTED classification level, which should be classified as EU classified information by FRONTEX at the level RESTREINT UE. FRONTEX, in other words, is expected to apply the classification used by the Council to the information forwarded by EUROPOL.

The two agencies concluded an additional Cooperation Plan in October 2009.[119] The contents of this Plan remains undisclosed to the best of our knowledge. It takes into account the modifications to EUROPOL's mandate introduced by the EUROPOL Decision of April 2009. It is pointed out in several documents that the cooperation plan specifies the various dispositions of the strategic agreement of March 2008, including on the use of information and communications technology.

- **EUROPOL/OLAF administrative agreement**

OLAF and EUROPOL have an administrative agreement concluded in 2004 that includes provisions on the exchange of strategic or technical information. Such strategic or technical information does not include personal data. It may include relevant information from the Europol Information System, the Customs Information System or any other OLAF or Europol database, and may also be used to support operational analysis carried out by the Parties. However, working relationships with EUROPOL are almost non-existent. Interestingly, the OLAF annual reports hardly mention EUROJUST or EUROPOL.

2.8.1.3. Working relations and information exchanges

The following pages offer a non-exhaustive overview of working relations and information exchanges between EU JHA agencies, beyond the formal provisions laid out in the corresponding cooperation agreements. Information exchanges are particularly central in the relations between EUROJUST and EUROPOL, on the one hand, and EUROPOL and FRONTEX on the other.

- **EUROJUST/EMCDDA**

[119] Although not disclosed, the Cooperation Plan is filed under the Europol file number 3710-588.

The two agencies have also established relations. The EMCDDA and Eurojust share knowledge and information on the differences between, and the enforcement and implementation of, drug trafficking laws across Europe. In 2007 EUROJUST designated the National Member chairing the Trafficking and Related Crimes team as the EUROJUST contact point for all EMCDDA-related matters. The EUROJUST representative was invited to the annual EMCDDA legal experts meetings where trafficking issues were discussed. Comparative information about precursor trafficking laws and national requirements to authorise controlled deliveries has in turn been passed to EUROJUST from the EMCDDA.

- **EUROJUST / OLAF**

The working relation between **EUROJUST and OLAF** has demonstrated a degree of strain. Despite practical agreements (notably the 2008 Practical Agreement on arrangements of cooperation between EUROJUST and OLAF), exchanges between OLAF and EUROJUST are irregular. According to the latest EUROJUST annual report, in 2010, OLAF referred only four cases to EUROJUST and EUROJUST referred only one case to OLAF. In July 2010, the President of EUROJUST and the Acting Director General of OLAF met in Brussels to evaluate co-operation and discuss the need to improve methods of identifying appropriate cases that would benefit from a collaborative approach. The need to explore synergies between the two bodies was stressed in the context of possibilities under the Lisbon Treaty. However, the two agencies still struggle to define and separate their fields of competences. The problematic positioning of OLAF in the security landscape is addressed further in the section devoted to the “undefined role of some players in the field”.

- **EUROJUST / FRONTEX**

Article 26.1 of the EUROJUST Decision states that EUROJUST shall establish and maintain ‘cooperative relations’ with EUROPOL and FRONTEX. While the relation with EUROPOL, as detailed above, is currently framed by a formal agreement, relations with FRONTEX have proceeded at a slower pace. In 2010, EUROJUST intensified contacts with FRONTEX to establish and maintain co-operative relations. As reported in the EUROJUST annual report, on 29 April 2010, as a follow-up to informal contacts between the two organisations, the President of EUROJUST and the Executive Director of FRONTEX met at Eurojust to discuss possible areas for future of co-operation. Eurojust initiated contacts with FRONTEX for the possible negotiation of a draft co-operation instrument in accordance with Article 26.1 of the EUROJUST Decision. Following this development, negotiations with FRONTEX are currently under way and the conclusion of a formal agreement was expected in 2011.

- **EUROJUST / EUROPOL**

The exchange of information includes the obligation of EUROPOL (at its own initiative or upon a request of EUROJUST) to provide EUROJUST with analysis data and analysis results, including interim analysis results if judicial follow-up is required, and the obligation for EUROJUST to actively support EUROPOL by stimulating the flow of information to EUROPOL from the competent national authorities and by providing it with opinions based on analysis carried out by EUROPOL. EUROJUST provides, at its own initiative, EUROPOL with the findings of an analysis of a general nature and of a strategic type and provides on a regular basis EUROPOL with relevant data for the purpose of its analysis work files, as well as other information, including information on cases, provided that they fall within the competence of EUROPOL and advice which may be required for the objectives and tasks of EUROPOL. Article 13 of the agreement addresses the issue of transmission, and article 15 addresses the Right of Access, reminding that “any individual shall have the right to have access to personal data concerning himself transmitted under this Agreement, to have his data corrected and deleted, or to have such data checked, in accordance with the applicable provisions of the Party to which the request is addressed”. Article 18 states that “Personal data shall be deleted immediately when it is no longer necessary for the purposes for which it was transmitted. A retention review must take place within a maximum period of three years, and when prescribed under the regulations

of the Party retaining the data. If the storage of data transmitted from one of the Parties exceeds a period of three years, the need for continued storage shall be reviewed annually".

The 2009 agreement, therefore, covers operational, strategic or technical information, as well as personal data. The EU created two independent 'joint supervisory bodies' (JSBs) for EUROPOL and EUROJUST, which review the activities of these agencies in order to ensure that the processing of personal data is carried out in accordance with the applicable legal framework. In order to fulfil their tasks, both JSBs have access to all files and premises where personal data is being processed. EUROPOL and EUROJUST have to supply all documents, paper files or data stored in EUROPOL's or EUROJUST's data files. The mandate and powers of JSB are detailed in a recent study on the "Parliamentary Oversight of Security and Intelligence Agencies in the EU".[120] The study underlines the fact that the work of the JSBs has attracted little interest from the EP despite the dissemination of their activity reports to the EP. Recent progress is however reported. For example, the EUROPOL JSB's report on the Terrorist Financing Tracking Programme has generated significant interest from MEPs. In this context, the chair of the EUROPOL JSB presented to Parliament the conclusions of its first inspection of Europol's role in the implementation of the TFTP agreement.

EUROJUST also contributes to OCTAs and TE-Sats. This contribution is, however, a source of tensions, as described above.

- **EUROPOL/FRONTEX**

The main purpose of the March 2008 Strategic Agreement between EUROPOL and FRONTEX is the exchange of information. To this day, as mentioned earlier, the exchange of personal data is excluded from the scope of the agreement, since FRONTEX did not have at the moment of its entry into force a mandate to process such data. Two categories of information are included under Article 2 of the agreement: 'strategic' and 'technical' information (the details are listed in **Table 5 in the Annex**). It is important to note, however, that these lists are not limitative.

The exchange of information falling into these different categories, furthermore, is limited to specific 'areas of criminality', which "relate to the performing of the tasks of Frontex and to relevant areas of crime within Europol's mandate" (Article 3). The list of criminal offences involved in such 'areas' is included in an annex to the agreement. This list, in turn, can be modified on the basis of a written proposal of Europol, subject to a written acceptance by Frontex (see **Table 6 in the Annex** for the list of criminal offences falling within the scope of the agreement).

The list is identical to the forms of crime annexed to Council Decision 2009/371/JHA on the establishment of EUROPOL. This observation does raise a number of interrogations, on the risks incurred by the emphasis on cooperation between JHA agencies. **To what extent, for instance, does the exchange of information between EU JHA agencies contribute to the blurring of the respective mandates of these agencies?** The main focus of the mandate of FRONTEX, in this case, is the coordination of operational cooperation among the Member States of the European Union for the control of their external borders (Council Regulation (EC) No 2007/2004, Article 2(1)(a)). **Does the exchange of strategic and technical information with EUROPOL reinforce this mandate, or does it increase the possible overlaps between the remits of the two agencies?** The question is all the more stringent, as the possibilities of oversight of such exchanges remain limited. The July 2011 note from the Belgian delegation to the JHA counsellors and COSI support group on the final report of Project Group 'Measure 6' is very telling in this respect.[121] The aim of the Project Group was to "improve the collection,

[120] Wills, A. *et al.* (2011), *Parliamentary Oversight of Security and Intelligence Agencies in the EU*, Brussels: European Parliament, PE 453.207

[121] This project group was set up following the adoption by the Council of the so-called 29 measures for reinforcing the protection of external borders and combating illegal migration. See: Council of

processing and systematic exchange of relevant information between FRONTEX, other EU Agencies and Member States".[122] Besides the fact that an important effort was required on the Council side to identify and trace the various information flows between EUROPOL, FRONTEX and the Member States, the report underlined that "[w]e lack a framework at EU level for what has to be shared between the EU agencies, bodies and Member States".[123]

There are of course limits to these exchanges of information. The most notable is the exchange of personal data, which is ruled out so far since FRONTEX does not yet have the mandate to process such information. Possible evolutions tied to the revision of the FRONTEX regulation will need to be scrutinised carefully. Another important limit, which is pointed out in the final report of the 'Measure 6' Project Group led by the Belgian delegation, is the fact that the Strategic Agreement between EUROPOL and FRONTEX only applies to strategic and technical information, and does not give legal grounds to the exchange of operational information. FRONTEX, furthermore, does not have a connection to EUROPOL's Secure Information Network Application (SIENA), which does not allow for the secure transmission of sensitive information. EUROPOL, similarly, does not have access to the FRONTEX-controlled ICONet information exchange system. As the 'Measure 6' report concludes, "This kind of cooperation between the two agencies must be translated into a common activity programme. The current cooperation is too 'ad hoc' and such an activity programme could improve more formal cooperation between all agencies and avoid the risk of duplication".[124] The question, of course, is how this activity programme could actively include both the agencies and bodies in charge of freedom and justice within the AFSJ, while offering the adequate degree of transparency and accountability with regard to the European Parliament and national Parliaments.

2.8.2. The drive towards intelligence-led policies

As mentioned in the 'background section', in the field of counter-terrorism and OC, the underlying logic that has prevailed in the EU strategy in the last decade demonstrates a focus on intelligence-led tools and strategy. 'Connecting' intelligence, liaise and cross-check data, profile and predict have been key concepts used by law enforcement specialists in the fight against OC and terrorism. As a consequence, the 'prevention' side is exclusively tackled from a law enforcement and coercive perspective. If prevention is ranked at the one of the main objectives of the Internal Security Strategy for the EU, it is strictly understood as 'anticipation of crime', fuelled by profiling needs.

The working relations established between EU ISS agencies and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)[125] further illustrate this aspect. These working relations mainly concern the law enforcement perspective on drug-related issues. The cooperation commitment between Europol and EMCDDA, for instance, started at the end of the 1990s and involve today a series of collaborative activities. The actions take into account the adoption of the *EU Drugs action plan for 2009–12* (2008/C 326/09). More specifically, the cooperation focuses on three sets of objectives: those directly related to the EU Drugs action plan for 2009–12; objectives related to the exchange of methodology and strategic information; and actions in support of the implementation of Council Decision 2005/387/JHA. The EMCDDA and Eurojust share information on the differences

---

the European Union (2010), Council Conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal migration, 6975/10, 1.3.2010.

[122] Council of the European Union (2010), "*Final report and recommendations of Project Group 'Measures'*", 7942/2/11, 6.7.2011.

[123] Ibid., p. 7.

[124] Ibid., p. 11.

[125] EMCDDA was established in 1993 and is based in Lisbon (Portugal). It provides the EU and its Member States with a factual overview of European drug problems and a solid evidence base to support the drugs debate.

between, and the enforcement and implementation of, drug trafficking laws across Europe, and the cooperation between the EMCDDA and CEPOL is currently being formalised and covers the issue of drug supply and supply reduction in Europe. **Unfortunately, a large part of EMCDDA's work is not taken into account in the EU ISS**. The agency has indeed developed a number of mechanisms to describe the availability and nature of responses to drugs in term of prevention, not necessarily linked to policing, as well as a variety of tools to evaluate them. EMCCDA gives evidence of interesting findings that could influence the debate over drug-related crimes and over the current fight against drugs trafficking and its priorities. For instance, EMCCDA findings, based on qualitative research based in the European Union, show there is little evidence of crime consequences from the vast recreational drugs scene across Europe. EMCCDA also stresses that primary prevention strategies may have beneficial effects on social functioning, including criminal behaviour and that there evidence that treatment programmes, which reduce drug consumption, also generally reduce crime.

The ISS clearly focus rather on mechanisms of 'prediction', such as analytical tools or early-warning systems. The importance of impact assessments is furthermore strongly advocated in the ISS, in order to "deepen our understanding of the different types of threats and their probability and to anticipate what might happen, so that we are not only prepared for the outcomes of future threats but also able to establish mechanisms to detect them and prevent their happening in the first place".

The elaboration of a European Criminal Intelligence Model (ECIM) and the subsequent designing of the so-called Project Harmony described above derive from this quest to constantly assess, prevent (in a law enforcement perspective) and predict. EUROPOL made, unsurprisingly, a leading contribution in the elaboration and implementation of the ECIM and is unquestionably at the centre of ECIM implementation.

Anticipative logics and profiling have major consequences that should not be underestimated. Among them, the technological challenge, detailed in the next chapter, encapsulates all the aspects linked with a vast collection of data and their protection.

At a societal level, such logics could unfortunately hinder processes of social integration, weakening any effort against exclusion and marginalisation and therefore contributing to shake the social cohesion of the EU while in return enhancing feelings of insecurity. Initiatives such as 'Check the Web Project', directly linked to the strategic prevention of radicalisation, targets quasi exclusively what is referred to as 'Islamist terrorist' or 'jihadist activities' websites. Launched in 2007, the 'Check the Web' Project is coordinated by EUROPOL (who hosts the information portal) and aims at strengthening cooperation and sharing the task of monitoring and evaluating open Internet sources on a voluntary basis. If this surveillance' main goal is to prevent the misuse of the Internet for terrorist purposes, the focus on 'Islamist terrorism' demonstrates again the targeting of the 'usual suspects'.

Moreover, the cost of such mechanisms, compared to their benefits in term of 'more security' and their costs in term of social harm should be questioned. As recommend in the LIBE report on the EU Counter-Terrorism Policy,[126] the Commission should conduct a compulsory proportionality test and a full impact assessment for each proposal involving the large-scale collection of personal data, detection and identification technologies, tracking and tracing, data mining and profiling, risk assessment and behavioural analysis or similar techniques. Such assessment should acknowledge not only the legal challenges encountered, but also long-term logics on the social level.

[126] S. Int'Veld (2011), "Report on the EU Counter-Terrorism Policy: main achievements and future challenges", op. cit.

2.8.3. The role of the freedom agencies of ISS

Along 'traditional' players in the field of the European landscape, EU freedoms agencies now also have a voice in the debate on the ISS. Special attention is here given to the EU Freedoms and Rights agencies that play an increased role in the shaping of EU internal security policies and that should be fully mobilised to ensure democratic accountability in the areas covered by the EU ISS: the European Agency for Fundamental Rights (FRA), the European Data Protection Supervisor (EDPS) and the Article 29 Working Party. This section also reviews the potentialities offered in the field of EU ISS for other EU actors, notably the European Ombudsman.

2.8.3.1. The European Agency for Fundamental Rights (FRA)

The FRA is an advisory body of the European Union established in 2007 by Regulation (EC) n° 168/2007[127] and is based in Vienna (Austria). The FRA's mandate is to ensure that fundamental rights of people living in the EU are protected. According to Council regulation (EC) n° 168/2007, the Agency carries out its tasks within the competencies of the Community, as laid down in the TEC. In the post-Lisbon context, the Agency refers to fundamental rights within the meaning of Article 6(2) of the Treaty on European Union, including the European Convention on Human Rights and Fundamental Freedoms, and as reflected in the Charter of Fundamental Rights.

If the FRA and EUROPOL are reportedly planning to produce a joint contribution for their respective work programmes for 2012 and are exploring possibilities for further joint products reflecting policing and security issues together with fundamental rights considerations (Note for the LIBE Committee, 2011), more formal involvement of the FRA should be implemented. The recent mid-term report of EUROJUST to COSI acting as chair of the JHA Agencies cooperation for January-May 2011, which confirms the joining of FRA in the cooperation (Council document 10404/11), is hence a welcomed initiative.

The recent FRA opinion on the Passenger Name Record demonstrates the usefulness and legitimacy of its involvement. At the request of the EP in April 2011, the FRA added its own opinion to those provided by the EDPS and the Article 29 Working Party on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final), which was released in June 2011. Even though the FRA welcomes the introduction of guarantees in the current proposal that reduce the risk of direct discrimination and discriminatory profiling, it nonetheless identifies concerns regarding compliance of the Directive's proposal with the Charter of Fundamental Rights of the European Union, specifically in the following matters:

- the lack of safeguards in the transmission of data by air carriers;
- the lack of precision in the 'list' of special categories of data allowed to be transmitted;
- the need of statistics to assess the efficiency of the PNR system (total number of persons whose PNR data were collected and exchanged; number of persons identified for further scrutiny; number of subsequent law enforcement actions; number of persons later found to have been unjustifiably flagged as suspicious by the PNR system);
- the need of clarification in the types of crimes covered (serious transnational crime, serious crimes, minor offense, etc) and the limitation of the list of crimes covered (sufficiently serious);
- special attention to the treatment of innocent people;

[127] Regulation (EC) No. 168/2007 establishing a European Union Agency for Fundamental Rights

- the need to comply with the right to protection of personal data

Such opinion should become systematic, and the FRA should include issues of criminal matters in its annual report. If the chapter 3 of its latest annual report (2011) deals with 'Information Society and data protection' and the technological challenge in general, the FRA should also be active in every fields of criminal matters that affect civil liberties and human rights. The issue of profiling and its consistency as regards to the Charter (non-discrimination) for instance deserve full attention, as well as the consequences of anticipative logics on the course of action in a fair trial or the over criminalisation introduced in the EU Framework Decision on organised crime.

2.8.3.2. The European Data Protection Supervisor (EDPS) and Article 29 Committee

Despite mentioning data protection and privacy issues in the section dedicated to the information exchange model, the ISS does not make any reference to the EDPS. The EDPS has nevertheless the possibility to intervene on the policy debates on data protection matters, by providing his expertise and publishing opinions.

Established in 2004, the legal basis of the EDPS are article 286(2) of the Treaty of European Community (39) and art. 41 of Regulation No. 45/2001/EC(40). The duties of the EDPS imply a wide range of activities encapsulated in the following: supervision, consultation and cooperation.[128] The EDPS has for instance intervened in the debate over the "Data Retention Directive", concluding that such Directive "does not meet the requirements set out by the right to privacy and data protection".[129] He has also express opinion on the heated controversies over the new Passenger Name Records (PNR) proposal, indicating that "the Proposal with its current content does *not* meet the requirements of necessity and proportionality, imposed by Article 8 of the Charter of Fundamental Rights of the Union, Article 8 of the ECHR and Article 16 of the TFEU".[130]

EDPS is clearly legitimate to ensure the respect of rights in EU security-related matters, specifically in cases of processing of personal data. Similarly, the Article 29 Data Protection Working Party has a meaningful role to play. The Article 29 WP was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has an advisory status and acts independently. The Working Party was set up to achieve several primary objectives: to provide expert opinion from member state level to the Commission on questions of data protection; to promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities; to advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy; to make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community. The Article 29 Working Party complements

[128] P. de Hert and R. Bellanova (2009), "Data Protection in the Area of Freedom, Security and Justice: A system still to be fully developed?", European Parliament, Brussels

[129] EDPS (2011), Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May, p. 14.

[130] EDPS (2011), Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 25.3.2011.

the work of the EDPS. In the case of the PNR Directive for instance, it reached similar conclusions in its April 2011 opinion on the Commission proposal.[131]

As an addition, the EU does have mechanisms that promote the vitality and dynamics of democratic rights in a transparent manner. There are potentialities to open up debates on issues covered by the EU ISS and to ensure the participation of the EU citizens and residents in the Union's democratic functioning. The position of the European Ombudsman and its mission illustrates this point.

2.8.3.3. The European Ombudsman

The Lisbon Treaty introduces a horizontal amendment, replacing "institutions (and/or bodies)" with "institutions, bodies, offices or agencies". With this amendment, some general principles (e.g. the right of access of EU citizens to documents or the right to file complaints to the European Ombudsman) would apply explicitly to European agencies as well.[132] Thus, **the administrative accountability of the EU agencies involved in the ISS is increasingly safeguarded by the European Ombudsman, who has the power to investigate complaints of maladministration**. The Treaty of Lisbon also broadened the Ombudsman's mandate to include possible maladministration in the framework of the Common Foreign and Security Policy, including the Common Security and Defence Policy.

The office of European Ombudsman was established by the Maastricht Treaty as part of the citizenship of the European Union. Article 24 of the Treaty on the Functioning of the European Union (TFEU) provides for the right to complain to the European Ombudsman as one of the rights of citizenship of the Union. This right is also included in the Charter of Fundamental Rights of the EU (Article 43). Possible instances of maladministration come to the Ombudsman's attention mainly through complaints, although the Ombudsman also conducts inquiries on his own initiative.

According to his mission statement, "the European Ombudsman seeks fair outcomes to complaints against European Union institutions, encourages transparency, and promotes an administrative culture of service. He aims to build trust through dialogue between citizens and the European Union and to foster the highest standards of behaviour in the Union's institutions".[133] Inquiries can be opened by the Ombudsman in a rather easy fashion. Complainants can submit their requests online. Citizen of a Member State of the EU, or who reside in a Member State, can make a complaint. Businesses, associations or other bodies with a registered office in the EU may also complain to the Ombudsman.

In ISS-related issues, interesting past examples illustrates **the potential for the European Ombudsman to be more involved in JHA matters**. In 2009, a case was submitted to the Ombudsman.[134] The complainant requested public access to a note from the Council Presidency. The requested document was a note from the Presidency of the Council to Coreper in response to a letter from the European Parliament concerning the transfer of information to Parliament's Temporary Committee on the alleged use of

[131] Article 29 Working Party (2011), Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 00664/11/EN, WP 181.

[132] S. Andoura and P. Timmerman (2008), "Governance of the EU: The Reform Debate on European Agencies Reignited", CEPS, Brussels

[133] European Ombudsman Annual Report, 2010

[134] The case 523/2009/TS is detailed on the European Ombudsman's website: http://www.ombudsman.europa.eu/

European Countries by the United States' Central Intelligence Agency for the transportation and illegal detention of prisoners. The note was registered by the Council under reference number 14483/06 and classified as 'RESTREINT UE'. The complainant was refused this access, and submitted a complaint to the Ombudsman in March 2009, upon which the Ombudsman opened an inquiry. The complaint was then forwarded to the Council, which provided its opinion, which was sent to the complainant with an invitation to make observations. The complainant submitted his observations in November 2009. In December 2009, the Ombudsman inspected the document in question at the premises of the Council. The report of the inspection was subsequently forwarded to the complainant and to the Council.

In his assessment, the Ombudsman gives details on how the case was handled, and declares that on the basis of his investigation, and having accessed the document in question, he concludes that, in this case, the statement of reasons set out by the Council for applying the exception based on the protection of public interest as regards international relations was sufficient. The Ombudsman considers that the brevity of the statement of reasons is acceptable in light of the fact that mentioning additional information, in particular making reference to the contents of the document concerned beyond what is stated above, would negate the purpose of the exception. On the basis of the above, the Ombudsman concludes that there was no maladministration by the Council.

If the Ombudsman's decisions are not legally binding and do not create legally enforceable rights or obligations for the complainant, or for the institution concerned, the use of such democratic tools should be publicised. Sensitive areas for the EU citizens such as data protection, watch lists, and more broadly attempts to freedoms and rights within the EU, could be brought to the European Ombudsman's attention.

2.8.3.4. Conclusion: the perpetuation of the third pillar?

Taken together, the developments highlighted so far in Chapter 1 and 2 raise the question of whether the third pillar has effectively disappeared in EU AFSJ policies. The point is not to deny the legal changes brought about by the entry into force of the Lisbon Treaty. In some respects, actors from the former third pillar have taken stock of the new system of checks and balances and its effects. A good example of this is the fact that the Hungarian Presidency has shown a degree of compliance with the obligation laid down in Article 87(3) TFEU and Article 6(2) of the COSI Decision to keep the European Parliament and national Parliaments informed of the developments taking place in the field of operational cooperation in law enforcement by recently forwarding a letter detailing the activities of COSI in 2010-2011 to the chairman of the LIBE Committee. COSI should discuss in its upcoming meeting of 8 September 2011 a draft report to the European and national Parliaments on the same question (Council document 12980/11, not available publicly). On the side of the cooperation between agencies, the FRA was invited for the first time by EUROPOL to attend, together with EUROJUST, EMCDDA, OLAF and SitCen the November 2010 meeting of the JHA Heads of Agencies.[135] During the first semester of 2011**, the FRA has officially been welcomed as a new JHA Agency by EUROJUST**[136], which holds the chairmanship and secretariat of JHA Agency cooperation until the end of 2011 (FRONTEX is to take over in 2012, CEPOL in 2013). By the same token, FRA representatives have also been invited to attend some COSI meetings, for instance on the occasion of the discussion of the Commission's *ISS in Action* communication in October

[135] Council of the European Union (2011), "Report on cooperation between JHA Agencies in 2010", 5675/11, 25.1.2011.

[136] Council of the European Union (2011), "JHA agency cooperation – Midterm report January-May 2011 – Activities and Key Findings", 10404/11, 19.5.2011.

2010.[137] The revision of the FRONTEX Regulation indicates an effort, albeit limited, to take into consideration the obligations regarding the compliance of the agency's activities with fundamental rights provisions in the treaties.

In the meantime, **a number of developments might result in these changes being minor adjustments, reflecting an inclusion at the margin rather than full integration**. Some of the old working habits of the third pillar, including the tendency to engage with security matters on a strictly intergovernmental basis and in confidential settings, are still at work. There are several issues at stake, which will be further refined and explored in the next chapter, regarding the policy process and the possibilities of oversight in internal security activities, as well as in view of the compliance of these activities with fundamental freedoms and rights obligations. The preservation of the established working habits associated with the third pillar, in addition, operates alongside a number of shifts in the orientations of EU internal security policies. To some extent, these orientations have been present for some time, and most find their origins in the developments surrounding the creation of the first European police and justice bodies and in the unfolding of the Schengen cooperation in the 1990s. They are currently encompassed under the notion of 'intelligence-led policing' and its correlates, such as the systematic promotion of a pro-active posture with regard risks and threats. **The 'EU' policy cycle in internal security, in this regard, can potential enable the preservation of law-enforcement cooperation as an intergovernmental domain despite the end of the pillar system**. One of the most crucial aspects of these orientations is the combination of an intelligence-led and pro-active approach with increasing reliance on technology and surveillance. Current developments involving FRONTEX and the establishment of EUROSUR reflect this trend, and the related challenge posed by technology. Finally, an essential aspect that has not been scrutinised so much up to now in this study is the question of the external effects of internal security policies and of the entanglement between internal and external security. All the EU agencies, bodies and services evoked so far are engaged in activities in, or cooperation with, third countries. This is the last challenge that will be surveyed in the next chapter.

[137] Council of the European Union (2010), "Standing committee on operational cooperation in internal security (COSI) – Summary of discussions", 14651/10, 8.10.2010.

3. CHALLENGES OF EU INTERNAL SECURITY

KEY FINDINGS

- The study of the ISS underlines the need to address three main challenges: the policy process, the issue of data protection and an effective compliance of external activities.
- The analysis of the methodology currently used in the internal security policy process highlights the need for more transparency (including access to information) and external assessment. An evidence-based EU policy in the field of internal security can only benefit from a pluralistic and contradictory debate.
- There are also not only legal grounds, but also a real need for more active engagement from the EP in the field of internal security, in the oversight of proposals made by the Council and various EU agencies, in COSI's activities, and in the process of threat assessments.
- In the area of Human Rights, freedom agencies play an increasing role in the ISS, which help inflecting the European security model advocated in the EU ISS that supports an all-encompassing definition of internal security and neglect the issue of Fundamental Rights. The FRA, the EDPS and the Article 29 Working Party have a legitimate role in assessing and influencing the ISS from a fundamental rights perspective.
- Furthermore, the role of such EU actors is critical in a context of technology intensive internal security policies relying on the processing of personal data. The need for a single data protection framework for increased oversight of law enforcement activities involving the processing of personal data is high in this regards.
- This aspect is enhanced by the security cooperation with third countries that raises a number of challenges and can be highly sensitive, as demonstrated by controversies around the EU-US TFTP and PNR agreements. The gist of the challenge regarding external relations is the possibility to ensure effective compliance of external activities in the field of internal security with the principles governing the AFSJ as a whole, and particularly with Treaty-based obligations in the field of fundamental freedoms and rights. In this specific area, there is clearly a need for monitoring the arrangements and agreements concluded by EU agencies and bodies with third countries.

3.1. The policy challenge

The centremost challenge for ensuring the proper functioning of the EU system of checks and balances, guaranteeing democratic accountability and enforcing compliance with the fundamental freedoms and rights obligations laid down in the Treaties, relates to the organisation of internal security policy. It is to devise a policy process that is inclusive of all stakeholders and does not narrow internal security activities to discussions among law-enforcement specialists. By reinforcing the powers of the European Parliament and despite the derogations to the ordinary legislative procedure in the field of police cooperation and

operational activities, the Lisbon Treaty also places additional demands on the EP to engage actively with the monitoring of EU initiatives in the field of internal security. Monitoring and oversight involve three key areas: the development of an evidence-based EU policy in these areas, the enforcement of effective consultation at all stages of the EP, and the guarantee of a more open participation in internal security policies.

3.1.1. Towards an evidence-based EU policy

3.1.1.1. The knowledge challenge

As explained in the background section, how we come to define and give priority to the threats and risks affecting the EU is of paramount importance in order to ensure that EU internal security policies, including the areas of counter-terrorism and organised crime, is adequately evidence-based and supported by the best available assessments. The consequences of the various threat assessments reports produced by EUROPOL or FRONTEX should not be underestimated, both in terms of reliability and impact. As noted in a recent report for the LIBE Committee[138], even though EU agencies such as EUROPOL and EUROJUST are not meant to set priorities or make policy, they do have a specific role in the policy process, as their assessments will inform political priority-setting and policy in the area. The long-term investment of EUROPOL in such activities, for instance, offers the agency the possibility of shaping future EU policy. The emerging organisation of work around the EU policy cycle and COSI is likely to further reinforce this trend. EUROPOL's expertise is expected to support the development of a large ecosystem of policy-planning documents, including PADs, MASPs and OAPs, which will steer internal security activities in forthcoming years.

The methodology used to develop these documents should be made publicly available to enable external and independent reviewing and assessment. The TE-SAT reports should receive similar scrutiny and supervision. The same holds for the methodology of the risk assessments produced by FRONTEX, where some methodological issues are openly acknowledged by the agency itself. Here again, there exists a significant degree of expertise pooled among the research projects funded under the EU's 6th and 7th Framework Programmes to ensure an external evaluation of the highest quality[139]. It is worth noting, for instance, that other bodies of the European Union have relied on such external and independent support and review in this area. The abovementioned FP6 Project THESIM thus provided expertise to the European Parliament, EUROSTAT as well as national bodies in the context of the negotiations that led to the adoption of Regulation (EC) No 862/2007 on Community statistics on migration and international protection. CEPOL, and to a lesser extent FRONTEX (and more recently) have also demonstrated a degree of willingness to involve external review, including from recognised scholars in the social sciences, so this can be considered as an accepted practice among JHA agencies.

The question of knowledge, however, cannot be limited to the provision of expertise to internal security agencies, bodies and services, be it external and independent. An evidence-based EU policy in the field of internal security can only benefit from a pluralistic and contradictory debate. **There are a number of tools available to the EU institutions to ensure that such a debate takes place**. These include the briefing notes and studies that can be requested by the European Parliament, but also the research projects funded under the EU's Framework Programmes. In recent years however, the handling of the latter with regard to security research, and especially of the

[138] M. Busuioc and D. Curtin (2011), op. cit. The report also underlines how the dividing lines between policy advice and actual policy-making become blurry in practice, particularly given the close link between threat assessment, political priority-setting and ensuing policy choices.

[139] The European Commission's report on EU research on migration provides information on a number of projects that have worked on the statistical treatment of migratory dynamics, which is of key importance for FRONTEX: European Commission (2009), "Moving Europe: EU research on migration and policy needs, DG Research, Brussels.

FP7 Security Theme (FP7-ST), has become a source of concern.[140] The FP7-ST will be examined in more details below, but it is important to point out that the priorities and funding of research in the field of security is an area where the European Parliament has a strong capacity for intervention through its powers as budgetary authority.

3.1.1.2. The question of access to information

The corollary of a broader evidence base and more pluralistic knowledge base in the field of internal security is access to information. The key question is the possibility for actors beyond the narrowly defined law-enforcement sector to have access to some information deemed classified or confidential. Internal security agencies, bodies and services are keen to emphasise that confidentiality is a pre-requisite for efficiency and for confidence building among security practitioners. The question has emerged probably most strongly in ongoing discussions about the recast of Regulation (EC) 1049/2001 regarding public access to European Parliament, Council and Commission documents. The counter-terrorism coordinator usefully recapitulated the view of security practitioners in an April 2010 meeting on the issue of access to documents after the entry into force of Lisbon, by pointing out that as far as intelligence cooperation was concerned, confidentiality is a prerequisite for trust, and intelligence services want to be able to ensure that "information they supply should not be passed on without the consent of the originator"[141]. But as the CTC recognises himself in the same intervention, there is very little involvement of Member State intelligence services *per se* at the EU level, the only major exception being SitCen (and for external relations matters, the EUMS intelligence division).

There are, in fact, two discussions here. The first one concerns public access to documents and the extent to which rules of confidentiality designed for intelligence materials should be considered fitting for other types of documents, including items such as FRONTEX or EUROPOL risk assessments. The second one involves checks and balances and Parliamentary oversight, which should not be confused with full disclosure of confidential documents. On this second point, it is worth noting that all Member State national Parliaments have, to one degree or another, developed mechanisms of oversight for policies involving classified materials, and that this should be a priority for the European Parliament as well.

The independent assessment concerning the counter-terrorism costs (see Report for the LIBE Committee, May 2011) shows that EU CT related spending increased from €5,7 m in 2002 to €93,5 m in 2009. As underlined by the LIBE Rapporteur on the Counter-Terrorism Policy[142], a proper evaluation of ten years of counter-terrorism policies would provide the basis for an evidence-based, needs-driven, coherent and comprehensive EU counter-terrorism strategy. A panel of independent experts could carry such an in-depth and complete appraisal. Such panel should not only set out clearly the results of the policies in terms of increased security in Europe, but also include a full overview of the accumulated impact of counter-terrorism measures on civil liberties.

3.1.2. Effective consultation and involvement of the European Parliament and of bodies in charge of fundamental freedoms and rights

In order to strengthen the democratic accountability of JHA matters, the first objective should be to oblige the European Council and the Council of the European Union to make their preparatory work more transparent. In the meantime, the effective consultation and involvement of the European Parliament and of bodies in charge of fundamental freedoms and rights is also central.

---

[140] See the studies conducted on behalf of the LIBE Committee on security research in the FP6 and FP7 (PE 393.289 and PE 432.740).
iojdsf

[142] S. Int'Veld (2011), op. cit.

3.1.2.1. The effective involvement of the European Parliament at all stages

An efficient cooperation between the European Parliament and national parliaments and the establishment of inter-parliamentary oversight is critical. In particular, a way to break the current de facto *conventio ad excludendum* of the European Parliament and some national parliaments could be for the national parliaments to share among themselves and the European Parliament the information/preparatory texts of general interest.

The Commission should regularly assess the democratic scrutiny of counter-terrorism and OC policies. If it is clear for the LIBE Committee that such assessment must cover the access of information and preparatory documents; the time and rights to modify the proposals, to overview the legal basis used for each policy measure, it is also of similar importance to establish an independent mechanism of oversight and follow up of each measures taken in the name of security.

Moreover, and beyond the need for consultation, **the need for more active engagement from the European Parliament must be tackled**. For COSI activities for instance, Article 71 TFEU mentions the need to keep the EP and national Parliaments informed. The provision provides a legal basis for the EP to actively stage hearings within the relevant Committees. Hearings can be based on Rule 193(2) of the European Parliament's rules of procedures. Regular hearings could promote the new system of checks and balances introduced by the Lisbon Treaty and contribute to the regular monitoring of activities in the field of internal security. For more prominent cases, there are two possibilities:

- Rule 184 of the EP's rules of procedure provides for the creation of special committees, on a proposal from the Conference of Presidents. The term of office of such a committee may not exceed 12 months, unless decided otherwise by Parliament upon its expiry. One possibility would be to set up a special committee with powers to monitor internal security activities and see that all the agencies, bodies and services involved inform the EP. While not a durable solution, it might provide for oversight in the upcoming year or more while the framework of internal security policies is being put in place by COSI and the agencies
- Temporary committees of inquiry: particular potent tool with a treaty base (Article 226 TFEU, Rule 185 of the EP's rules of procedure). The EP can convene such committees to investigate alleged contraventions or maladministration in the implementation of EU law, except where the alleged facts are already being investigated by a court.

An intensive and extended parliamentary representativeness in the JHA activities should be brought forward. This does not only cover the involvement in the threat assessments and the oversight of proposals made by the Council and various EU agencies. Parliamentary representativeness at all stage of the decision-making level should be promoted.

3.1.2.2. The involvement of EU bodies in charge of fundamental freedoms and rights

The Lisbon treaty brings two crucial modifications in terms of HR: it gives the Charter of Fundamental Rights legally binding status and introduces in the Treaty on European Union a general commitment to such principles as freedom, the rule of law and respect for human rights (Article 2 TEU).

As noted earlier, despite the Commission's commitment, in its Action Plan on implementing the Stockholm Programme, to a "Zero Tolerance Policy" regarding violations of the Charter of Fundamental Rights, the *ISS in Action* does not regard the transposition of this policy in the field of internal security as a strategic objective. If the communication frames EU internal security policies as being based on common values and refers both to

the EU Charter of Fundamental Rights and to the Commission's strategy for its implementation, it offers a rather restrictive definition of the articulation between security, freedom and justice.

The ISS thus offers little provisions in terms of ensuring liberty to individuals across the EU. This element has not only consequences that should not be underestimated (such as the infringement of civil liberties). Law enforcement officials have indeed much more to gain to ensure that fundamental freedoms are respected within the EU. As rightly put by EU experts in the field, "when people know that their rights are protected by law, law enforcement officials are secure in the knowledge that their actions are fully compatible with fundamental rights and the accused are guaranteed a fair trial, a truly effective ISS will be achieved. (...) The EU's ISS should be built around the objective of delivering to everyone living in the EU the twin rights of Rule of Law and protection of Fundamental Rights"[i][143]. Thus, **the involvement of EU "Freedoms Agencies" should not be seen as a concession offered to "civil liberties" supporters, but as an efficient way to promote debates and comply with the Rule of Law and, in doing so, avoid heated controversies**, as well as financial compensations for wrongdoings.

As described above, freedom agencies play an increasing role in EU internal security policies, and an enhanced use of existing EU agencies responsible for the respect of Human Rights would help inflecting the European security model advocated in the EU ISS that supports an all-encompassing definition of internal security and neglect the issue of Fundamental Rights.

In particular, the FRA should make use of its current (post-Treaty of Lisbon) powers to assess the ISS from a fundamental rights perspective and it should also see its competences expanded as regards independent and objective evaluation (not only research activities) of EU policies covering in particular the domains of police cooperation and criminal justice[144][ii]. Furthermore, a FRA representative could attend COSI meetings. It would provide more balance to the COSI composition, where the justice element is barely represented, with the exception of the EUROJUST representative present at COSI meetings. As an addition, the **EDPS, the Article 29 Working Party, and the FRA should be consulted on a systematic basis on data processing and exchanges with third parties schemes for internal security purposes**. The issue of data protection, as well as initiatives undertaken by the EDPS and the Article 29 Committee are detailed further in the section devoted to the 'technological challenge'.

Along with this need to fully involve the FRA, the EDPS and Article 29 WP (in COSI's scope of activities for instance), a more integrated cooperation and coordination between these agencies would be welcome.

3.2. The technological challenge

The reliance on technological systems in EU internal security policies has become over the past few years a central feature of a growing number of initiatives. Significant budgetary resources have been earmarked for the purpose of researching security technologies: the 'security theme' of the Union's 7th Research Framework Programme has been endowed with an overall budget of €1.4 billion. Programmatically at least, then, the reliance on technology for internal security is a central issue.

Outlining the 'technological challenge', however, requires that a number of questions be raised. **To what extent do the post-Lisbon initiatives in the area of technology and security, and the priorities singled out in the EU ISS differ from previous policy**

[143] E. Guild and S. Carrerra, (2011), op. cit.

[144] E. Guild and S. Carrerra, (2011), *Towards an Internal (In)security Strategy for the EU?*, CEPS, Brussels

orientations? Technology has been central in a number of controversies over the past decade, particularly in cases where the reliance on technical systems appeared to challenge the right to data protection and the right to privacy of EU citizens. Examples of such controversies have involved the European Parliament, as in the case of the transfer to the United States of America's Department of Homeland Security of financial data generated by the Swift company for the purpose of the TFTP programme implemented by this body,[145] or in the case of the transfer and processing of Passenger Name Record (PNR) data.[146] Others have remained more discrete and limited to expert discussions, as in the case of the delays encountered in the deployment of the second-generation Schengen Information System (SIS II).[147] **Have these controversies been taken into account in foreseen initiatives?**

At the heart of the 'technological challenge' **lies the question of the processing of personal data by internal security agencies, bodies and services of the EU and its Member States**. Data processing is a central feature of the priorities singled out in the EU ISS. The objective outlined by the document is that there should be "interaction" between "all the different EU databases relevant for ensuring security […] as far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximising the opportunities presented by biometrics and other technologies for improving our citizens' security within a clear framework that also protects their privacy" (p. 13). **Which mechanisms of oversight are available to ensure that this prescription is implemented?**

3.2.1. The drive towards technology-intensive EU internal security policies

The reliance on some technologies, such as computerised information exchanges, for internal security purposes is a long-standing trend, both in individual Member States and in the European context. The first pan-European police database, in this respect, was the Schengen Information System (SIS), which came online in 1995. The current period differs from earlier initiatives by the **significant programmatic inflation** that can be observed with regard to the use of technology for purposes of internal security. **Multiple initiatives, particularly with regard data-processing schemes, are being programmed in close succession, raising the question of possible overlaps and of the actual necessity of the different envisaged systems**. In the meantime, the programmatic focalisation on technology and the alleged need for forward-looking policies in this field **have broadened the range of actors involved in EU internal security policies, particularly from the private sector**. Programmatic inflation, however, **raises the question of practical implementation: to what extent have programmed technical systems, including those funded through EU instruments, become operational so far?**

3.2.1.1. Technology and programmatic inflation in EU internal security policies

The emphasis on technology as a crucial component of the Union's policies in the field of internal security is not specifically tied to the entry into force of the Lisbon Treaty and the adoption of the EU Internal Security Strategy. Discussions on the use of technology have been going on across a number of issue areas, and involving different groups of participants, since the end of the 1990s. Modifications to the SIS, for one, were envisaged on a regular basis after it came online, for example to accommodate its extension to new Schengen countries. With the inclusion of the Nordic countries in the system, SIS became 'SIS I+' and, following on a decision from the

[145] For an overview, see inter alia A. Amicelle (2011), "The Great (Data) Bank Robbery: Terrorist Financing Tracking Program and the 'SWIFT Affair'", Paris: CERI, QDR No. 36.

[146] See e.g. P. De Hert and R. Bellanova (2011), "Transatlantic Cooperation on Travellers' Data Processing: From Sorting Countries to Sorting Individuals", Migration Policy Institute, Washington, D.C.

[147] See J. Parkin (2011), "The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law", CEPS, Brussels.

December 2006 JHA Council, 'SIS one4all' to allow the system's extension to the new EU Member States.[148] New categories of records (such as the 'informal' inclusion of persons listed on the UN terrorist lists), new functionalities, and new access possibilities have been added over time to the system.[149] Measures towards the establishment of SIS II were initiated from the end of 2001 onwards, in parallel to the ongoing modifications of SIS[150] – in some cases, such as the SIS 'one4all', because of the delays encountered in its development[151] - while the purposes of the system were only formalised with the adoption of the SIS II Regulation in December 2006.[152] In the field of visa policy, the principle of a computerised consultation system on visas (VISION) among Schengen Member States was established in Document SCH/II-Vision (99) 5 of the Schengen Executive Committee. After the events of 11 September 2001, discussions among Member State representatives within the Visa Working Party resumed with the possibility of using visa-related information for counter-terrorism purposes. The establishment of VIS followed the same pattern as SIS II: namely, a Council Decision was adopted in June 2004 to enable the Commission to initiate the technical development of the system, while the VIS Regulation as such, which defined its purpose and contents, was adopted only in July 2008.[153]

If discussions on the use of technology for internal security purposes have been going on regularly among EU Member States and within the European institutions since the end of the 1990s, the formalisation of this question as a strategy issue in the context of the AFSJ is more recent, starting with the 2004 Hague Programme. The first item under the "Strengthening Security" heading of the programme deals with "Improving the exchange of information". The main measure envisaged to this effect is the implementation of the "principle of availability" according to which "throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State, and […] the law-enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigation in that State".[154] The implementation of the principle of availability "should make full use of new technology" according to the programme. The other reference to the use of technology for internal security purposes in the Hague document

[148] See e.g. S. Peers (2008), "Key Legislative Developments on Migration in the European Union", *European Journal of Migration and Law*, Vol. 10, pp. 77-104.

[149] Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism (OJ L162/29, 30.04.2004) and Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism (OJ L68/44, 15.3.2005), for example, introduce the possibility for Eurojust, Europol, national judicial authorities and authorities responsible for issuing or examining visa applications or issuing residence permits to access the SIS. For a more systematic view of subsequent modifications to the SIS, see E. Brouwer, "Digital Borders", op. cit., pp. 71-116.

[150] The technical development of SIS II was enabled by the adoption of Council Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II), OJ L 328/1, 13.12.2001 and Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), OJ L 328/4, 13.12.2001.

[151] See for instance: House of Lords European Union Committee (2007), "Schengen Information System II: Report with Evidence", London: The Stationery House, 9th Report of Session 2006-07, pp. 13-14.

[152] See Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4, 28.12.2006.

[153] Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC), OJ L213/5, 15.6.2004; Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L218/60, 13.8.2008.

[154] Council document 16054/04, op. cit., p. 18.

involves the use of biometric identifiers and information systems for purposes of migration control, the key issue being interoperability of databases.

The pursuit of 'new technologies', and particularly of additional information exchange systems, in the field of internal security took on new dynamics following the adoption of the Hague Programme. **While SIS II and VIS, arguably the two 'core' systems in the field of internal security, experienced significant delays, proposals and initiatives for new systems have multiplied over the years**. In its November 2005 Communication on the principle of interoperability, for example, the Commission already foresaw that three new systems should be developed in the long-run, a European criminal Automated Fingerprints Identification System (AFIS), an entry/exit system (EES) combined with a border-crossing facilitation scheme, and one or several European register(s) for travel documents and identity cards.[155] At least one of these systems, the EES, had previously been ruled out as a policy option by DG JHA in the impact assessment attached to the 2004 proposal for the VIS Regulation.[156] This option was nonetheless re-packaged less than a year later as a long-term development for the AFSJ. The EES subsequently found its way into the European Commission's 2008 'border package' and is currently considered as part of the European Commission's 'smart borders initiative'.[157] In May of the same year, furthermore, seven Member States signed a convention, dubbed the Prüm Convention, on the stepping-up of cross-border cooperation, particularly in the area of counter-terrorism, cross-border crime and illegal immigration.[158] The Prüm Convention foresaw the establishment of yet another scheme for the exchange of information, including in the controversial area of DNA profiles. The fact that the Convention was concluded between seven Member States only could also be interpreted as the contestation of the principle of availability featured in the Hague Programme and otherwise supported by the European Commission.[159]

These two dynamics – multiplication of proposals, on the one hand, and re-framing of previously discarded or unsuccessful proposals, on the other – have nurtured the inflation in the number of programmes for the development and establishment of new technologies and technical systems for internal security purposes. The 'technological challenge', in this respect, should be in upcoming years to designs ways to regulate this process and ensure that it is embedded in proper oversight mechanisms. One specific issue that deserves more attention, in this respect, is the growing involvement of the private sector in EU internal security policies, which will be examined in the following point.

---

[155] See European Commission (2005), Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24.11.2005.

[156] The EES was found too costly and less advantageous than the option that was eventually selected, namely the setting-up of VIS with biometrics.European Commission (2008), Annex to the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas – extended impact assessment, SEC(2004) 1628 final, 28.12.2004.

[157] See, respectively European Commission (2008), Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008; European Commission (2010), Legislative proposal to set up Entry/Exit Syste*m*, JHA/2010/004, 8.2010.

[158] See Council of the European Union (2005), Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation particularly in combating terrorism, cross-border crime and illegal migration, Prüm*, Germany, 27 May 2005*, 10900/05, 7.7.2005.

[159] See inter alia the analysis in T. Balzacq et al. (2006), "Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats", CEPS Working Document No. 234, CEPS, Brussels.

3.2.1.2. Technology, internal security and the private sector

A growing dimension of the 'technological challenge' **is related to the involvement of the private sector in the development of technical systems to be used in EU internal security policies**. This involvement has been fostered by a number of initiatives supported by the European Commission's DG Information Society (INFSO) and DG Enterprise over the past decade, in the field of 'security research', starting with the Preparatory action in security research (PASR, 2004-2006) and currently continued under the Security Theme of the Seventh Framework Programme (FP7-ST, 2007-2012). Representatives from major companies in the field of defence and electronics have been actively involved in the formulation of priorities related to security research, through a series of high-level venues, starting with the Group of Personalities on Security Research (GoP, 2003-2004), the European Advisory Board on Security Research (ESRAB, 2005-2006) and the European Security Research and Innovation Forum (ESRIF, 2008-2009).

In its September 2007 communication, the European Commission has framed its support to security research and the organisation of such high-level venues as part of an ongoing effort to build a 'public-private dialogue'. In the words of the communication, this dialogue is expected to "bring together all the relevant stakeholders in order to discuss issues of cross-cutting, common concern, facilitate the assessment of their differentiated strengths and resources, identify areas for potential synergies, or joint programming".[160] A number of reports, some drafted by civil liberties organisations[161] and some supported both by the European Commission and by the LIBE Committee have nonetheless interrogated this notion of dialogue.[162]" They raise two questions. **Firstly, why has the dialogue involved so few representatives from the private sector?** In the 'public-private dialogue' as it currently stands, the 'private' part is mostly made up of major companies, which used to be very active in the field of defence and electronics, and are currently redeploying a part of their promotional, research and development and manufacturing activities towards internal security issues. **Secondly, why has the dialogue been limited to representatives from national and EU internal security agencies, bodies and services and representatives from these major companies?** In the impact assessment accompanying the communication on public-private dialogue, the European Commission indicates that civil society organisations have been involved in the GoP and ESRAB. The European Parliament had in fact expressed its concerns about "a balanced involvement of industrial representatives, research sponsors and public and private customers, scientific research bodies, public institutions and representatives of civil society" in such high-level venues on security research.[163] Research has shown, however, that out of the 660 participants in ESRIF, only 9 (1.4%) could be considered as representatives from civil society organisations, none of which were part of a civil liberties or privacy group.[164]

---

[160] European Commission (2007), Communication on Public-Private Dialogue in Security Research and Innovation, COM(2007) 511 final, 11.9.2007, p. 3.

[161] See e.g. the work conducted by Statewatch and the Amsterdam-based Transnational Institute: B. Hayes (2006), "Arming Big Brother: The EU's Security Research Programme", Amsterdam/London: Statewatch/TNI ; B. Hayes (2009), "Neoconopticon: The EU Security-Industrial Complex", Amsterdam/London: Statewatch/TNI.

[162] See the following studies commissioned by the European Parliament at the request of the LIBE Committee: J.P. Burgess and M. Hanssen (2008), "Public Private Dialogue in Security Research", Brussels: European Parliament, PE 393.286 ; J. Jeandesboz and F. Ragazzi (2010), "Review of security measures in the Research Framework Programme", Brussels: European Parliament, PE 432.740. See as well some of the outcomes of the INEX project (FP7), e.g. D. Bigo and J. Jeandesboz (2009), "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'", INEX Policy Brief No. 5, CEPS, Brussels.

[163] European Parliament (2006), Security Research: European Parliament resolution on Security Research – The Next Steps *(2004/2171(INI))*, OJ C133/135, 8.6.2006, p. 138.

[164] B. Hayes, 2009, op. cit., p. 24.

An additional question is raised by the notion, supported by the European Commission's DG Enterprise, that public-private dialogue should result in a degree of 'joint programming' in the field of security technologies. Because of their participation in the GoP, ESRAB and ESRIF, representatives from the defence and electronics industry have been strongly involved in the formulation of priorities for security research and development funding, while being simultaneously among the main beneficiaries of these schemes.[165] **The question, here, lies in the extent to which representatives from the private sector should be able to contribute to the shaping of public priorities**. Representatives from the defence and electronics industry have clearly expressed a number of views on what they consider to be the priorities in technological developments related to internal security. The not-for-profit European Organisation for Security (EOS), established in 2007 and representing the key companies and professional associations in the sector, has published a number of White Papers on what these priorities should be. For example, the November 2009 White Paper on Border Management promotes the development of a 'one-stop integrated border control concept' combining the elements from the proposals for the Entry/Exit system and others such as the Registered Traveller Programme (RTP).[166] **The approach promoted is technology-intensive and draws on policy options for which a political decision and a legislative instrument have yet to be adopted by the European Parliament and the Council**. Such an approach is under development as well in the numerous security research and development projects funded under the FP7-ST.

The issue of oversight, here, is again central. If the idea of a 'dialogue' on security and technology, involving all the concerned parties, is to be pursued, it can only benefit from a fully transparent, well-assessed and accountable process. This is all the more fundamental as the practical implementation of technologies in EU internal security policies, as shown above, demonstrates a weak track record over the past decade.

3.2.1.3. The issue of practical implementation

Practical implementation is the third central dimension of the technological challenge of EU internal security policies. The question of practical implementation arises, firstly, from the observation the two key systems of exchange of information in the field of internal security developed through the EU, the SIS II and the VIS, are not yet operational. The SIS II has been in development since 2001: the original deadline for its deployment was 2006, and is long passed. While the costs of development have exceeded initial projections by 500%,[167] the system is not yet operational. The VIS has been in development since 2004, but it is only on 21 September 2011 that the Commission has adopted the Implementing Decision on the start of VIS operations in so-called 'first region' countries.[168] **The obvious question, in view of such delays, is whether the foreseen development and establishment of new computerised data-systems is a viable policy option, considering how long it is taking the two most important of them to reach operational status**. One can think, in this respect, of the upcoming proposals from the European Commission on 'smart borders', introducing legal instruments for three additional systems (EES, RTP and the European Border Surveillance System EUROSUR)

[165] See the research results in J. Jeandesboz & F. Ragazzi, 2010, op. cit., pp. 18-28.

[166] See European Organisation for Security (2009), White Paper: A European Approach to Border Management, Brussels: EOS.

[167] See J. Parkin (2011), op. cit.

[168] See Commission Implementing Decision of 21 September 2011 determining the date from which the Visa Information System (VIS) is to start operations in a first region (2011/636/EU), OJ L249/18, 27.9.2011. First country regions are established in Commission Decision of 30 November 2009 determining the first regions for the start of operations of the Visa Information System (VIS) (2010/49/EC), OJ L23/62, 27.1.2010. The countries in which the VIS has started operating on 11 October 2011 are Algeria, Egypt, Libya, Mauritania, Morocco, and Tunisia.

and introducing a communication on an EU Electronic System of Travel Authorisation (ESTA), all of which had already been discussed in the Commission's 2008 'border package' communications. The issue has been raised for example by the Conference of European Data Protection Authorities in its April 2008 declaration on the aforementioned 'border package'. The declaration suggest that there is a need from the European institutions and the Member States to "first evaluate whether already existing legal measures are implemented and executed in an effective way" before deciding on new measures.[169]

The question of practical implementation also arises in relation to the effective operation of already operational systems. **To what extent are technologies used for internal security purposes functional and useful to security agencies, bodies and services in the field?** The issue has spurred a number of controversies in some Member States. In a January 2009 report, the French data protection authority CNIL (*Commission nationale de l'informatique et des libertés*), has for example found that only 17% of the records on indicted persons ('*personnes mises en cause*') in the largest national police database, the STIC (*Système de Traitement des Infractions Constatées*), were accurate.[170] Such doubts have recently been expressed, furthermore, in relation to the implementation of an EU-wide scheme, the 2006 Data Retention Directive (DRD), which was the object of a recent evaluation by the European Commission's DG Home.[171] **The report highlights a number of difficulties related both to the practical implementation of the DRD, and to the possibility for an evidence-based assessment of the effects of this implementation**. As of April 2011, the DRD has been unevenly transposed in Member State national law, despite a deadline of 15 September 2007, and the transposition has been annulled by several national constitutional court rulings in the Czech Republic, Germany and Romania.[172] Besides the question of transposition, however, another question which surfaces upon reading the Commission's evaluation is that of the effective assessment of the use of data retention by the agencies, bodies and services in charge of criminal investigation. The problem is clearly acknowledged in the document: on the issue of "obtaining reliable qualitative and quantitative data […] demonstrating the necessity and value of security measures such as data retention", the report points out that "it has not been possible to achieve this objective" due to the partial transposition of the DRD and to diverging statistical practices among Member States.[173] Based on the information available to DG Home, it appears that there were 11 requests for every 100 recorded crimes across 19 responding Member States.[174] Although it asserts that "data retention is an integral part of criminal investigation", however, the report remains piecemeal and inconclusive as to the role played by information obtained through data retention schemes in actual criminal prosecutions and convictions.[175]

---

[169] Conference of European Data Protection Authorities (2008), Declaration on three communications from the Commission on border management, Rome, 18 April, p. 1.

[170] Commission nationale de l'informatique et des libertés (2009), Conclusions du contrôle du système de traitement des infractions constates (STIC) – Rapport remis au Premier Ministre le 20 janvier 2009, Paris: CNIL.

[171] For the DRD, see Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks and amending Directive 2002/58/EC, OJ L105/54, 13.4.2006. For the evaluation by DG Home, see European Commission (2011), "Evaluation report on the Data Retention Directive (Directive 2006/34/EC)", COM(2011) 225 final, 18.4.2011.

[172] For a legal analysis of these rulings with particular attention to the *Vorratsdatenspeicherung* ruling of the German Constitutional Court (March 2010), see e.g. K. De Vries, R. Bellanova and P. De Hert (2010), "Proportionality overrides Unlimited Surveillance: The German Constitutional Court Judgement on Data Retention", CEPS, Brussels.

[173] Evaluation Report on the Data Retention Directive, op. cit., p. 19.

[174] Ibid, p. 23.

[175] Ibid, p. 25.

It has to be stressed that the difficulties encountered by the Commission in collecting statistics on, and evidence of, use of data obtained through the DRD mechanism in criminal prosecution and conviction has been experienced by other bodies. The Article 29 Working Party documents the same difficulties in its report on the second joint enforcement action on the implementation of the DRD, for example.[176] Despite the difficulty to assess the practical implementation and use of the DRD scheme, however, the European Commission appears to remain firmly committed to the fact that "the EU should support and regulate data retention as a security measure", arguing in particular that the data thus obtained "has resulted in convictions for criminal offences which, without data retention, might never have been solved".[177] Other assessments have considered a broader range of policy options, including repealing the DRD. Among civil liberties organisations, the European Digital Rights organisation (EDRI) for example concludes from its 'shadow report' on the Commission's evaluation that "the statistics provided by the Member States do not prove the necessity of data retention", asserting that the EU "should reject the principle of data retention".[178] The EDPS has added to this view in its opinion on the Commission's evaluation of the DRD. It concludes, firstly, that after examining the available evidence "the Data Retention Directive does not meet the requirements set out by the right to privacy and data protection".[179] It further notes that "the Commission seems to exclude the possibility of repealing the Directive, either per se or combined with a proposal for an alternative, more targeted EU measure", and "calls upon the Commission to seriously consider these options in the impact assessment as well".[180]

The evaluation and assessment of the practical implementation of technological schemes for internal security is therefore a major question for possible mechanisms of oversight. As the case of the DRD shows, **such mechanisms are already available for the legal aspects of implementation, including transposition.** These fall within the remit of the Commission. **What is missing, however, is the possibility to have detailed and comparable qualitative and quantitative evaluations of the practicality of such schemes, and the degree to which they are put to use by EU and Member State security agencies, bodies and services.**

3.2.2. The question of data processing

Most of the major technology-oriented initiatives launched through the EU framework over the past years touch upon the processing of personal data. This trend also echoes the relation between programmatic inflation and practical implementation examined previously and leads to the following question: **to what extent is it possible, even for the practitioners and experts involved in the development of these systems, to keep track of all existing and upcoming data processing schemes?**

This question appears all the more important as most recent initiatives **differ both quantitatively and qualitatively** from already existing data processing schemes, such as EURODAC or the SIS. Quantitatively, they would **involve the processing of massive amounts of personal data**. Qualitatively, they are **supposed to include new functionalities and serve simultaneously multiple purposes**. These 'new' forms of data processing, as we will see, raise in particular the question of the reliance on techniques of data mining and profiling.

---

[176] Article 29 Working Party (2010), *Report on the second joint enforcement action*, 00068/10/EN, WP 172.

[177] Ibid.

[178] European Digital Rights (2011), *Shadow evaluation of the Data Retention Directive (2006/24/EC)*, Brussels: EDRI, 17 April.

[179] EDPS (2011), Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May, p. 14.

[180] Ibid.

The question of keeping track of existing and upcoming personal data processing schemes and the quantitative and qualitative shift they seem to reflect raises a third question. **What are, within current discussions among the actors of the EU internal security landscape, the options envisaged for regulating data processing?**

3.2.2.1. Data processing schemes in EU internal security policies: brief overview and foreseeable developments

Keeping track of the various data processing schemes currently used, in development or foreseen in the framework of the EU has proven problematic. It is only in the course of 2010 that the Commission published, under the lead of DG Home, an overview of data processing schemes involving the use of personal of personal data.[181] The European Parliament, at the request of the LIBE Committee has also commissioned a number of assessments.[182] Based on these studies, it appears that some 25 systems for the exchange and analysis of information are currently in operation, in development or foreseen as part of the Union's internal security policies.[183] Some of these systems are controlled by EU agencies, such as Europol's TECS. Others are or will be managed by EU bodies, such as the SIS and SIS II, Eurodac and the VIS. Others yet are both controlled and managed by Member State authorities, including the system originating in the Prüm Convention and Decision or the so-called 'Swedish initiative' on the sharing of information between Member States for criminal investigation or criminal intelligence investigations.[184]

Among recent and forthcoming proposals, the following appear to be of particular importance for the future development of EU policies in the field of internal security:

1. **'Smart borders' initiative**: The Commission has introduced at the end of October 2011 a communication on 'smart borders' that examines the possibilities for creation three new systems, an Entry/Exit System (EES), Registered Traveller Programme (RTP) and European Electronic System of Travel Authorisation (ESTA).[185] **The fact that these systems are not new initiatives** (having been foreseen already in the Commission's 2008 'border package') **and have in some cases (the EES) already been ruled out in previous impact assessment documents, calls for an in-depth examination of their necessity**. In the meantime, the communication rules out the possibility of establishing a European ESTA for the time being. The European Commission expects to return to this issue in 2012.
2. **EU-PNR:** in February 2011, the Commission tabled a new proposal on an EU-wide system for the processing of Passenger Name Record data.[186] An earlier

[181] European Commission (2010), *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, 20.7.2010.

[182] See for instance Hempel, L. *et al.* (2009), *Exchange of information and data between law-enforcement authorities within the European Union*, Brussels: European Parliament, PE 419.590. For a complementary contribution, see Geyer, F. (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, Brussels: CEPS, CHALLENGE Research Papers No. 9.

[183] A full overview and assessment has been provided to the European Parliament in the study requested by the LIBE Committee on the updating of the EU data protection framework: D. Bigo et al. (2011), *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Brussels, EP study 453.216, Chapter 2.

[184] Established by Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union, OJ L386/15, 25.11.2005.

[185] European Commission (2011), "Smart borders – options and the way ahead", COM(2011) 680 final, 25.10.2011.

[186] European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 2.2.2011.

proposal, tabled in November 2007,[187] had been blocked following the European Parliament's decision to reserve its formal opinion due to concerns over the proposal's compliance with the EU Charter of Fundamental Rights and the European Convention on Human Rights,[188] and the Commission's choice of legal basis.[189] It was eventually withdrawn by the Commission, formally in light of the change in legal basis deriving from the entry into force of the Lisbon Treaty.[190] The new PNR proposal, however, has already proved controversial. In its March 2011 opinion, for example, the EDPS has indicated that "the Proposal with its current content does *not* meet the requirements of necessity and proportionality, imposed by Article 8 of the Charter of Fundamental Rights of the Union, Article 8 of the ECHR and Article 16 of the TFEU".[191] The Article 29 Working Party reached similar conclusions in its April 2011 opinion on the Commission proposal.[192] The FRA was consulted on the request of the President of the European Parliament. In its June 2011 opinion, it considers that the Commission has addressed a number of the concerns expressed in its previous opinion on the 2007 EU-PNR proposal, but still formulates a number of remarks related to the possibility of direct and indirect discrimination, to the need for more statistics to provide proper evaluations of the efficiency of PNR data processing, and to requirements regarding the limitation of rights envisaged in the Commission's proposal, particularly in relation to the principle of necessity and proportionality.[193]

3. **EU-TFTP:** the Commission tabled in July 2011 a communication on the establishment of an EU-TFTP system, derived from the U.S. Terrorist Finance Tracking Programme.[194] The proposal follows from the implementation of the second EU-U.S. TFTP agreement, signed on 28 June 2010, to which the European Parliament consented after a protracted negotiation process by adopting a legislative resolution on 8 July 2010.[195] The Commission's proposal for an EU-TFTP system builds on the outcome of the first review of the agreement and on the two reports drafted at the request of the European

[187] European Commission (2007), Proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) for law enforcement purposes, COM(2007) 654, 6.11.2007.

[188] Expressed by the EDPS, the Article 29 Working Party and the Fundamental Rights Agency.

[189] European Parliament (2008), Resolution of 20 November 2008 on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, P6_TA(2008)0561, 20.11.2008.

[190] See European Commission (2009), "Consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures", COM(2009) 665 final, 2.12.2009.

[191] EDPS (2011), Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 25.3.2011.

[192] Article 29 Working Party (2011), Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 00664/11/EN, WP 181.

[193] European Union Agency for Fundamental Rights (2011), Opinion on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final), 1/2011.

[194] European Commission (2011), "A European terrorist finance tracking system: available options", COM(2011) 429 final, 13.7.2011.

[195] European Parliament (2010), Legislative resolution on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purpose of the Terrorist Finance Tracking Program, P7_TA(2010)0279.

Commission by Judge Jean-Louis Bruguière on the TFTP.[196] Despite dissenting opinions, both assessments found the TFTP to provide significant added value to counter-terrorism policies. The proposal for an EU-TFTP system builds on this assessment, but also on the argument that such a system would address the "serious concerns […] in relation with its [the EU-U.S. TFTP Agreement] consequences on the fundamental rights of citizens" linked in particular to the transfer of bulk data to the U.S. authorities. The aim of the EU-TFTP system, then, would be "to ensure that the processing of such data would take place in accordance with EU data protection legislation and principles, and in accordance with the EU Charter of Fundamental Rights", particularly its Article 8.[197]

The overview of both existing and foreseen systems raises several questions:

1. **Policy impact assessment in internal security:** the fact that some initiatives, such as the Entry/Exit or EU-PNR systems, can be regularly resubmitted despite the fact that they have been either put aside or rejected in the decision-making process, raises a question with regard the quality of impact assessments in EU internal security policies. **The 'recycling' of policy initiatives might indicate that impact assessments have not been conducted properly at the moment of first submission, or that impact assessments do not have significant effects on the decision to table the proposal for a new data processing scheme**.
2. **Necessity and proportionality:** directly tied to the question of impact assessments is the issue of necessity and proportionality. As the number of data processing schemes increases in EU internal security policies, it appears that a growing number of controversies involve these two principles. Necessity and proportionality have been the key grounds on which the initial EU-PNR proposal was questioned by the EDPS and Article 29 Working Party, as well as by the FRA. The proposals composing the 'smart borders' initiative have raised similar interrogation when they were first formalised by the European Commission's DG JLS as part of its 'border package' of February 2008. Noting the "amazing pace" at which new proposals for data processing schemes in the area of movements of persons were being tabled, the EDPS requested for example "to see evidence that there is a master plan for all these initiatives, giving a clear sense of direction".[198]
3. **Effective implications of all concerned agencies, bodies, services, and institutions:** a number of policy practices appear to take shape where agencies and bodies such as the Article 29 Working Party, the EDPS and the FRA are consulted on a systematic basis on data processing schemes for internal security purposes. This is also certainly the case for the European Parliament, as demonstrated by the case of the initial EU-PNR proposal for instance, and even more so following the entry into force of the Lisbon Treaty. The degree to which the views of these actors are taken on board is up for discussion, of course. In the case of the EU-PNR system, for example, the opinions of the EDPS and Article 29 WP are certainly more negative than the FRA's. **Yet the persistence of some practices raises questions, in**

[196] European Commission (2011), "Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purpose of the Terrorist Finance Tracking Program", SEC(2011) 438 final, 17.2.2011.

[197] As well as with Article 16 TFEU. See European Commission (2011), "A European terrorist finance tracking system", op. cit., p. 3. For an analysis, see A. Amicelle (2011), "The Great (Data) Bank Robbery", op. cit.

[198] EDPS (2008), Preliminary comments of the European Data Protection Supervisor on three communications from the Commission on border management COM(2008) 69 final, COM(2008) 68 final, COM(2008) 67 final, 3 March 2008, p. 3.

particular the tendency, initiated with SIS II and the VIS, to begin the technical development of a system before a legal instrument establishing its scope and purposes has been adopted and all concerned agencies, bodies, services and institutions fully involved. This is the case, for example, of the European Border Surveillance system EUROSUR, on which the European Commission appears to plan a legislative proposal as part of its 'smart borders' initiative. As evidenced by progress reports submitted by DG Home, the development of the system has been ongoing at least since 2008.[199] On the basis of the technical specifications developed in the Commission's 2011 working paper on EUROSUR, costs incurred directly to the EU budget are of €5 million, with Member States using an additional €695 million from the External Borders Fund (45% of the EBF for the period 2007-2013), and about €106 million funded under the FP7-ST (first and second call estimate).

All three points **emphasise the question that has been sustained throughout this study, namely of the importance of mechanisms of oversight and full involvement of all the relevant EU actors in the process of policy development, decision, and implementation. With regard to data processing in internal security policies, this is all the more important as current trends indicate the growing emphasis placed on mass processing of the personal data of both foreigners and citizens.**

3.2.2.2. The shift towards mass processing of personal data

Two major trends are currently influencing the development of data processing schemes in the EU. The first trend is quantitative: **data processing in EU internal security policies is increasingly moving towards mass processing**. The second trend is qualitative: it involves **the shift towards the use of automated processing and data-mining with the aim of profiling categories of person and identify individuals** on the basis of the personal data held in EU databases, **in the name of prevention**.[200]

The first trend, i.e. **the quantitative shift in data processing**, is best illustrated by looking at the difference in scale between the SIS and the VIS, which are both used by Member State consular officials for the delivery of Schengen visas. As Figure 2 (available in the Annex) highlights, **the number of valid personal records stored in the SIS over the period 2004-2010 has never exceeded 1 million**, the largest category of personal records being collected under Article 96 of the Convention on the Implementation of the Schengen Agreement (CISA) concerning "[d]ata on aliens for whom an alert has been issued for the purposes of refusing entry".

In its 2004 impact assessment study on the establishment of VIS, the European Commission estimated that from 2007 onwards, Member States would receive about 20 million visa requests a year. Figure 3 and 4 (available in the Annex) provide information on the number of visa applications for categories A, B and C received by Schengen and non-Schengen EU Member States over the period 2005-2009, and the number of visas in categories A, B, C, VTL, D and D+C issued over the same period.[201] During this five-year

[199] European Commission (2009), Report on progress made in developing the European border surveillance system, SEC(2009) 1265 final, 24.9.2009; European Commission (2011), Determining the technical and operational framework of the European border surveillance system (EUROSUR) and the actions to be taken for its establishment, SEC(2011) 145 final, 28.1.2011.

[200] See the compilation of briefings requested by the European Parliament in: Baldaccini, A. *et al*. (2008), Controlling Security, Paris: L'Harmattan; G. Gonzalez Fuster et al. (2010), "Profiling in the European Union : A High Risk Practice", Brussels: CEPS, INEX Policy Brief No. 10.

[201] These figures were built on the basis of the information provided by Member States to the Visa Working Party. Data on visa applications and issuances for the year 2010 was not found available. To the best of our knowledge, there are no officially available figures on the total number of visas,

period, which corresponds to the data retention period applicable to personal records in the VIS, Schengen and non-Schengen EU Member States reported a total of 59.409.621 applications for visa categories A, B and C. They further reported the issuance of 63.399.852 visas, taking into account visa categories VTL, D and D+C. This is below the 2004 estimate of the European Commission, **but provides a rough idea of how many records will be held in the VIS at any given time, i.e. in the neighbourhood of 60 million**.[202]

Although it is clear that SIS and VIS do not operate along the same logic, the implementation of VIS does signal the change of scale in data processing for purposes of EU internal security. Mass processing is also at the heart of several envisaged systems, such as the Entry/Exit system and the EU PNR database. If the EES is limited to persons requiring a Schengen visa, it would overlap in terms of the number of personal records with the VIS. If the EES is extended to all 'third country nationals', as was suggested in one of the preferred policy options of the Commission's 2008 impact assessment document,[203] this number would be considerably higher. **To give a rough estimate of the scale of personal data collection in this second case**, the United Nations World Tourism Organisation (UNWTO) considers in its most recent *Tourism Highlights* report that Europe remained the most touristic region in the world, with the EU-27 registering **more than 350 million international (i.e. not regional) tourist arrivals last year**.[204] Tourists, of course, would only be one category of travellers whose comings and goings would be registered in the EE. **In the case of the EU-PNR database**, the estimates provided by the European Commission in the impact assessment document attached to its February 2011 proposal for an EU-PNR system are that **such a measure would concern over 500 million travellers, regardless of whether they hold EU citizenship or not** (these findings are summarised in **Table 7 in the Annex**).[205]

This change of scale raises questions as to guaranteeing fair treatment for the persons whose data, including biometrics in the case of VIS or detailed biographical information in the case of EU-PNR, is to be collected and processed, particularly if they are not EU citizens. **One issue, for example, is the probability of failed and mistaken matches in biometric identification**. The Commission submitted the initial VIS proposal on the understanding that the accuracy requirement of the system would be similar to that of Eurodac, leaving a margin of error between 0.1% and 0.5%.[206] The figure provided by the consortium in charge of the VIS feasibility study was of 12.000 cases on the basis of 12 million visa applications a year (between 12.000 and 60.000 in fact). **Given that records are stored and accessible on VIS for 5 years, however, the question is whether this number is accurate or should the calculation take into account the total anticipated number of records in the system for any five-year period, i.e.**

---

all categories included, delivered yearly by EU Member States, hence the choice to provide data on the total number of visas issued across all categories. This data, finally, should be considered as a rough estimate, as the information provided by Member State consular services to the Visa Working Party are sometimes incomplete or inaccurate, depending often on the infrastructures available to consular officers in the field.

[202] The initial study commissioned by DG JHA on the feasibility of VIS concluded on a figure of 70 million records at any given time on the basis of a 20 million visa applications per year. See European Policy Evaluation Consortium (2004), Study for the extended impact assessment of the Visa Information System, Brussels: EPEC, 12.2004.

[203] European Commission (2008), "Preparing the next steps in border management in the European Union", SEC(2008) 153 final, 13.2.2008, p. 50.

[204] United Nations World Tourism Organisation (2011), "UNWTO Tourism Highlights", Madrid: UNWTO.

[205] European Commission (2011), "Accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", SEC(2011) 133 final, p. 16

[206] See EPEC (2004), op. cit., p. 54.

between 60.000 and 300.000 cases? What should be done in case the use of VIS shows this margin of error to be too high?

This change of scale also raises political questions regarding the tendency towards generalised surveillance, whether through the use of personal data ('dataveillance') or by the conjunction of different technical instruments (sometimes qualified as the 'surveillance society'[207]).

3.2.2.3. The shift towards profiling in the name of prevent and anticipation

Changes in the scale of data processing are combined **with changes both in the purpose for which, and in the way in which data is processed**. As far as the purpose of data processing is concerned, the 'European Security Model' promoted by the EU Internal Security Strategy, as demonstrated previously, places strong emphasis on 'prevention and anticipation' and on a 'proactive and intelligence-led approach'. The EU ISS considers for instance that the European Passenger Name Record would enable internal security agencies, bodies and services "to deepen our understanding of the different types of threats and their probability and to anticipate what might happen, so that we are not only prepared for the outcomes of future threats but also able to establish mechanisms to detect them and prevent their happening in the first place".[208] **In other words, data processing is not only supposed to support the investigation of criminal acts or to enhance preparedness, but also to support the possibility of intervening before these acts are committed**. The Article 29 Working Party and the Working Party on Police and Justice (WPPJ) have highlighted this trend in their joint contribution on "The Future of Privacy" to the European Commission's consultation on the legal framework for data protection in the EU. They suggest that "the use of information focuses on earlier stages in the chain: in addition to the traditional use of information for the investigation and the detection of a specific crime, information is gathered and exchanged in order to prevent possible criminal acts".[209]

One of the main consequences of the emphasis on pro-activity in a context where data processing is becoming increasingly massive is the growing interest in the use of data mining and profiling. The proposals for a European PNR offer a good illustration of this interest, which has already been noted in other studies submitted to the European Parliament.[210] The impact assessment document accompanying the February 2011 Commission proposal for a Regulation on European PNR stresses that "PNR data are mainly used as a criminal intelligence tool, in particular for assessment, rather than as an identity verification tool".[211] **'Assessment' in the EU PNR proposal is used as a substitute for profiling**.[212] It relates to the use of criteria such as "ways of travel, behaviour, travel routes, etc."[213] to screen passengers and to identify "those who fit into the fact-based assessment criteria but who were previously unsuspected".[214]

---

[207] See e.g. Article 29 Working Party & Working Party on Police and Justice (2009), "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", Working Paper No. 168, 1.12.2009, p. 26; Surveillance Studies Network (2006), "A Report on the Surveillance Society, London, Report for the Information Commissioner, 9.2006.

[208] Council document 5842/2/10, *op. cit.*, p. 12.

[209] Article 29 WP & WPPJ (2009), "The Future of Privacy", op. cit., p. 25.

[210] See e.g. R. Bellanova and P. De Hert (2009), "Data protection in the area of freedom, security and justice : a system still to be fully developed ?". Brussels: European Parliament, PE 410.692, 3.2009, pp. 17-18 ; D. Bigo et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy", op. cit., Chapter 2.

[211] SEC(2011) 133, op. cit., p. 10.

[212] R. Bellanova and P. De Hert (2011), Transatlantic Cooperation on Travellers' Data Processing, op. cit.

[213] SEC(2011) 133, op. cit., p. 10.

[214] Ibid.

The question, here, is **whether such 'fact-based assessment criteria' amount to evidence, and provide sufficiently established grounds for action**. While profiling based on the analysis of the behaviour of persons who are already known (e.g. for which a criminal record already exist, or who can be linked to specific criminal facts) can be accommodated in a traditional criminal justice system, **profiling based on the identification of previously unknown persons through extrapolation based on patterns of behaviour that have been made anonymous, such as the proposed operation of the European PNR, appears to be more problematic**.[215] In their joint contribution, for instance, the Article 29 WP and the WPPJ point out that profiling "might stigmatize persons with certain backgrounds" while "[a]nalyses made on the basis of general criteria run the risk of high inaccuracies, leading to a high number of false negatives and false positives".[216] **The risk of discrimination has also been pointed out by the European Parliament in its April 2009 recommendation to the Council on profiling**, which remains to this day the only attempt by EU institutions to come up with a definition of this technique.[217] While this kind of profiling is yet to become common practice for EU-wide data processing schemes, it arguably requires a degree of attention in light of foreseeable initiatives such as the EU PNR and other proposals involving automated assessments and the processing of bulk data. The question, here, might be related to the decision-making process as such, and to the trend, identified as 'programmatic policy-making' or 'future perfect policy making' in another study requested by the LIBE Committee, consisting in multiplying proposals for new data-processing schemes before existing initiatives are implemented.[218]

3.2.3. The issue of oversight

The different dimensions of the 'technological challenge' examined so far all raise the question of oversight. In this last subsection, we examine how oversight is envisaged within EU internal security policies themselves, how it can be conceived through the issue of the right to data protection, but also through other procedures.

3.2.3.1. The regulation of data processing in internal security policies: the EU information management strategy

The expansion of data processing has led to the development of a number of proposals for their regulation within the framework of internal security policies. **The core strategy document here is the Information Management Strategy (IMS)**. The drafting of the IMS was initially discussed in the framework of the informal High Level Group for the future of European Home Affairs. The incoming Swedish presidency of the EU submitted a first draft of the IMS to the Council's Ad Hoc Working Group on Information Exchange on 26 June 2009, and the IMS was adopted by the JHA Council at the end of 2009. [219]

According to the Council, the IMS is "**a methodology** (the 'how') to ensure that decisions about the need for managing and exchanging data and decisions about the ways to do so are taken in a coherent, professional, efficient, cost-effective way, accountable and comprehensible to the citizens and the professional users. **It is not a legally binding**

[215] G. Gonzalez Fuster et al. (2010), "Profiling in the European Union : A High Risk Practice", , INEX Policy Brief No. 10, CEPS, Brussels.

[216] Article 29 WP & WPPJ (2009), "The Future of Privacy", op. cit., p. 26.

[217] European Parliament (2009), European Parliament recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)), OJ C184/119, 8.7.2010.

[218] D. Bigo et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament, Brussels, EP study 453.216, Chapter 2.

[219] Council of the European Union (2009), Draft Council Conclusions on an Information Management Strategy for EU Internal Security, 16637/09, 25.11.2009.

text".[220] It seeks, in other words, **to regulate data exchanges and processing, including with respect to the right to data protection and to privacy through the identification of a set of non-mandatory guidelines for agencies, bodies and services in charge of internal security.** Information management, for instance, is not a legal notion but is "functionally defined, i.e. depends on the task to be carried out, as opposed to competence-based or organisationally defined".[221] The guidelines laid out in the IMS are to be taken into account both in the management and development of cross-border information exchanges, and at the national level.

The IMS takes a strong stance in favour of data sharing and processing. It considers that one of its objectives is to promote "an attitude of data-sharing by default".[222] Issues related to data protection are mentioned in the IMS, which points out that "[c]ooperation with a view to ensuring the EU internal security places high demands on data protection".[223] In the management and development of information exchanges, therefore, "the legal requirements for protection of personal data and for security standards must be assessed together with business needs".[224] Two questions can be raised in relation to the possibilities for oversight involved in the guidelines laid out by the IMS. **Firstly, why is data security the only principle tied to the right to data protection that is explicitly mentioned in the strategy?** As mentioned by the EDPS, "data security […] is also a data protection principle but other principles relate to important preliminary issues, such as what is a legitimate purpose and what is legitimate access […] All principles together, including data security, determine whether an information system deserves to be implemented".[225] **Secondly, which are the agencies, bodies, institutions or services that should be involved in ensuring that 'information management' complies with all the requirements related to the right to data protection?** The IMS only makes references to Member State authorities and the European Commission. **What should be the role of EU and national data protection authorities, of the European Parliament and of national Parliament, in the management of information exchanges?** The IMS, in this respect, mirrors the managerial logic already at work through the EU 'policy cycle' in internal security as advocated by the results of the Harmony project.

3.2.3.2. Updating the EU legal framework on the right to data protection

Since EU internal security policies move towards technology-intensive activities involving in particular the mass collect, exchange and processing of personal data, the updating of the EU legal framework on the right to data protection becomes central. In this respect, the European Commission has adopted in November 2010 a series of proposals for a comprehensive approach on data protection in the European Union.[226]

The key elements that emerge from this communication as well as from various contributions discussing the 'comprehensive framework' as regards internal security are the following:

1. **The need for a single data protection framework:** at the moment, the legal framework for the protection of personal data in the EU's area of freedom, security and justice is fragmented. Matters that prior to the entry into force of the Lisbon Treaty belonged to the First Pillar are generally governed by Directive 95/46/EC,

[220] Ibid, p. 1.

[221] IMS, op. cit., p. 7.

[222] Ibid., p. 10.

[223] Ibid.

[224] Ibid., p. 11.

[225] P. Hustinx, P. (2009), "Data Protection and the need for an EU Infomation Management Strategy", Brussels: Council Ad Hoc Working Group on Information Exchange, Reception by the Swedish Presidency, 6.7.2009.

[226] European Commission (2010), "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, 4.11.2010.

also known as the Data Protection Directive (DPD).[227] Matters which belonged to the Third Pillar are governed by a separate legal instrument, Council Framework Decision 2008/977/JHA, also known as the Data Protection Framework Decision (DPFD).[228] The Commission's proposals, as well as the views expressed by data protection authorities and the European Parliament, insist that in order to reflect the changes brought about by Lisbon, a single legal instrument should be adopted that establishes general principles and rules across all EU policy domains.[229]

2. **The need for increased oversight of law enforcement activities involving the processing of personal data:** at the moment, oversight activities involving the right to data protection of EU bodies and information systems are fragmented. Europol, Eurojust and the SIS, for example, have their own Joint Supervisory Bodies (JSBs) composed of representatives of national data protection authorities. Proposals have surfaced to harmonise the methods used by these different bodies. The EDPS, for example, has suggested in his opinion on the Commission's proposals for a comprehensive data protection framework that the three layer, 'coordinated supervision' model, operational in Eurodac for instance and soon to be extended to VIS and SIS II, be generalised.[230] In this model, supervision is exercised at the national level by DPAs, at the EU level by the EDPS, and coordination is ensured through regular meetings where the EDPS is the lead body and provides secretariat functions.
3. **The need to pay particular attention to specific forms of data processing**: this question has, in turn, two dimensions. It involves firstly the question of so-called 'sensitive personal data', e.g. biometrics. The cases of SIS II, the VIS and the Prüm Decision highlight the trend towards the increased processing of such data. One principle advocated by the Article 29 WP and the WPPJ, in this respect, is that "[b]iometric data should only be used if the use of other less intrusive material does not present the same effect".[231] The question also involves the issue of profiling, the absence of a legal definition thereof, and the apparent tendency to avoid making explicit reference to profiling systems in policy documents.

In this perspective, a number of possibilities are currently being considered. The Stockholm Programme, for instance, expresses interest for 'privacy-aware' technologies.[232] In their joint *Future of Privacy* report, the Article 29 WP and the WPPJ suggest, in this regard, that 'privacy by design', namely the "idea of incorporating technological data protection safeguards in information and communication technologies" be made into a principle of the right to data protection.[233] Privacy by design, however, also reflects the notion that the right to data protection, despite having been given autonomous status as a fundamental right in Article 8 CFR, is embedded in a broader legal and regulatory framework offering multiple possibilities for oversight.

---

[227] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31, 23.11.1995.

[228] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008.

[229] See e.g. European Data Protection Supervisor (2011), Opinion on the Communication from the Commission "A comprehensive approach on personal data protection in the European Union", Brussels: EDPS, 14.1.2011. See the report from the LIBE Committee: European Parliament (2011), Report on a comprehensive approach on personal data protection in the European Union, Brussels, A7-0244/2011, 22.6.2011.

[230] EDPS (2011), Opinion on "A comprehensive approach on personal data protection in the European Union", op. cit., pp. 31-32.

[231] Article 29 WP & WPPJ (2009), "The Future of Privacy", op. cit., p. 27.

[232] Council document 5731/10, p. 34.

[233] Article 29 WP & WPPJ (2009), "The Future of Privacy", op. cit., pp. 13-15.

3.2.3.3. Oversight beyond data protection

Data protection is a central issue for oversight in a context of technology intensive internal security policies relying on the processing of personal data. At the same time, data processing impacts on a number of rights, including the right to privacy, the right to freedom of speech, of religion and so forth,[234] and on a number of principles, for instance accountability and transparency. **As such, oversight in the context of the 'technological challenge' cannot be limited to existing mechanisms put in place to safeguard the right to data protection, however central it might be**.

An interesting illustration of this issue can be found in the July 2010 opinion of the Article 29 WP on the issue of accountability.[235] The opinion expresses support for the inclusion in the revised EU data protection framework of a 'statutory accountability principle' which "would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request".[236] The need to "implement appropriate and effective measures" related to the legal obligations of the EU and its Member States with regard fundamental rights and freedoms, including to the right of data protection, point out the need to ascertain that the proper procedures are being used to develop policy initiatives in the field of internal security. **These procedures include, for example, respect of the impact assessment guidelines and checks on how proposed measures comply with the CFR, as established in several Commission documents.[237] Similar guidelines have recently been adopted in the framework of the Council's Working Party on Fundamental Rights, Citizens' Rights and Free Movement of Persons.[238]** Oversight, in this respect, can involve making sure that policy proposals systematically include properly designed impact assessment documents, and follow guidelines and checks on compliance with the CFR and other legal obligations of the Union and its Member States. Mechanisms such as that of notifications for prior checking in the field of data protection could be systematised to cover all the issues related to the implementation of the CFR, in relation for instance with the FRA.

Particular attention should also be paid to the involvement of the private sector in the field of internal security. In security research and development, the European Parliament has expressed concern, particularly by means of parliamentary questions, about the FP7-ST funded project INDECT.[239] In its resolution of 8 June 2011, the EP recalled in particular that "all research conducted within the FP7 must be conducted in accordance with fundamental rights as expressed in the European Charter" and requires the Commission to

---

[234] This is the reason why, for example, the ECtHR has systematically refused in its case law to mention privacy and equate it with data protection, preferring the terminology of the "right for the respect of private life" which encompasses the right to data protection but has a broader scope. See Bigo et al (2011), "Towards a New EU Legal Framework for Data Protection and Privacy", op. cit., Chapter 1.

[235] Article 29 Working Party (2010), Opinion 3/2010 on the principle of accountability, 00062/10/EN, WP 173, 13.7.2010.

[236] Ibid, p. 3.

[237] European Commission (2005), Compliance with the Charter of Fundamental Rights in Commission legislative proposals, COM(2005) 172 final, 27.4.2005 ; European Commission (2010), Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010), 573 final, 19.10.2010. Impact assessment guidelines, including on compliance with the CFR, are laid out in: European Commission (2009), "Impact Assessment Guidelines", SEC(2009) 92 final, 15.1.2009.

[238] Council of the European Union (2011), "Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies", 10140/11, 18.4.2011.

[239] "Intelligent information system supporting observation, searching and detection for security of citizens in urban environment", see the project website (www.indect-project.eu/) and its CORDIS landing page (http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=1&CAT=PROJ&RCN=89374).

give full access to all the documents tied to this project.[240] Beyond the specific case of INDECT, however, research has demonstrated the need for clearer guidelines and supervision of security research and development supported by the FP7 with regard to the legal obligations of the Union and Member States related to fundamental freedoms and rights.[241] **The key stake appears to involve the capacity of EU institutions to move beyond a case-by-case basis and establish a regulatory framework that would enable a routine follow-up of research and development initiatives involving private stakeholders**.

3.3. The internal/external relations challenge

The fourth challenge of EU internal security lies in the external relations of the Union. This is arguably an extremely variegated domain, comprising operational activities undertaken under the auspices of the EU in collaboration with third countries (e.g. the deployment of the networks of immigration liaison officers), the provision of financial and technical assistance to third countries (e.g. the BOMCA or EUBAM programmes respectively in Central Asia and Moldova and Ukraine), and the conclusion of partnerships and international agreements (e.g. the PNR and SWIFT agreements with the United States). The next subsection (3.4.1.) will provide a brief overview of the external dimension of internal security policies in the post-Lisbon context.

The gist of the challenge regarding external relations is the possibility to ensure effective compliance of external activities in the field of internal security with the principles governing the AFSJ as a whole, and particularly with Treaty-based obligations in the field of fundamental freedoms and rights. There are two aspects to this question. Compliance should be ensured, firstly, in relation to the impact that EU activities in the field of internal security might have regarding fundamental freedoms and rights in third countries (3.4.2.). It should, secondly, be ensured in relation to the impact that relations with third countries are susceptible to have on the guarantees provided by the EU legal framework to persons, and chiefly the transatlantic relation with the US (3.4.3).

3.3.1. The external dimension of internal security policies in the post-Lisbon context

3.3.1.1. The pre-Lisbon situation

The question of the relations between internal and external EU activities in the field of security received its first formal endorsement in the 2004 Hague Programme under the label of the 'external dimension' of the AFSJ. The development of this policy domain has been steered in part through the strategic documents tabled at a few weeks' interval by the Commission and the Council, respectively in October and November 2005. As noted in a previous study commissioned by the LIBE Committee (PE 410.688), the 'external dimension' has developed without a formal legal basis. Prior to the entry into force of the Lisbon Treaty, the main legal basis for external relations in the field of justice and home affairs laid in Title VI TEU Article 38 (with Article 24) which granted the EU a treaty-making competence in the domains pertaining to this Title. Outside of this specific activity, most EU initiatives were either 'implied' from Treaty objectives[242] or founded in other legal bases in the TEC (development or trade policies) and TEU (CFSP, ESDP).

[240] European Parliament (2011), European Parliament resolution of 8 June 2011 on the mid-term review of the Seventh Framework Programme of the European Union for research, technological development and demonstration activities (2011/2043(INI)), P7_TA-PROV(2011)0256, 8.6.2011, §.27.

[241] See the study requested by the LIBE Committee on the mid-term assessment of the FP7-Security Theme: J. Jeandesboz and F. Ragazzi (2010), "Review of security measures in the Research Framework Programme", PE 432.740, European Parliament, Brussels.

[242] Cremona suggests for instance that these have been in part implied from Article 63(3)(b) TEC on the objective of establishing the AFSJ (Cremona, 2008 : 5-6).

One outcome of this situation is that initiatives associated with the external dimension of the AFSJ have multiplied in a seemingly haphazard way, although some trends have emerged. With regard to the provision of financial and technical assistance, these comprise:

- The tendency to focus on candidate and/or neighbourhood countries.
- The tendency to prioritise the security aspect over freedom and justice.
- The tendency to concentrate on issues related to migration control, including border management.

In the case of the Western Balkans, for instance, 37% of the €470 million engaged by the Commission in the justice and home affairs sector have concerned border management and border security according to a recent European Court of Auditors audit report (Special Report 12/2009, p. 14). In a 2008 audit report, the Court found that out of the €104.7 million committed by the Commission to justice and home affairs in Belarus, Moldova and Ukraine through the TACIS instrument, 63.2% were dedicated to border management, the most significant project being the EU border assistance mission (EUBAM) deployed in Moldova and Ukraine since 2005 (Special Report 9/2008, pp. 10-11). A number of these financial and technical assistance projects are further underpinned by direct involvement from EU JHA agencies, chiefly EUROPOL and FRONTEX.

Another issue for concern in recent years has been **the direct involvement of the EU and its Member States in internal security operations in third countries**. The best-known example of such a situation is the HERA series of operations coordinated by FRONTEX since 2006, which are based in the Canary Islands. The HERA operations involve the diversion of crafts heading for the high seas or Spanish territorial waters towards Senegal and Mauritania. A number of such operations have been conducted directly in the territorial waters of both countries, on the basis of bilateral Memoranda of Understanding concluded by Spain, the host country of the HERA operations. The MoUs have remained confidential to this day, which constitutes an issue of accountability and transparency. More worrying, a number of reports have pointed out that the HERA operations might have led to the breaching of the principle of *non-refoulement*, and led to the persons 'diverted' in this fashion to experience intolerable conditions of detention in Mauritania and Senegal. Other, possibly less high profile activities include the deployment of immigration liaison officers in third countries, which has been pioneered in the Western Balkans and is supported by EUROPOL. A number of cooperative schemes also cover the exchange of confidential data between EU JHA agencies and third countries. One example is the so-called Neus network which should enable such exchanges between EUROPOL and the law-enforcement authorities of Bosnia Herzegovina, following the signing of a strategic agreement and the conclusion of a MoU on a secure communication link between the two parties.

A third set of questions regarding the external dimension involves **the impact of the security policies of EU partners on the guarantees regarding fundamental freedoms and rights afforded by the Union's legal framework.** At stake here is in particular the unfolding of the relationship between the EU and the US in security matters. To some extent, this question has placed a strain on transatlantic relations for some time. In the 1990s, the most notorious episode has involved the surveillance of telecommunications through the ECHELON network, where the European Parliament has played a key role in supporting the research conducted on this system and publicising the effects it had on EU citizens and other persons. The security policies implemented by the US administration after the attacks of 11 September 2001 have been met in two ways. On the one hand, some among the Member States and within the EU institutions have been keen on cooperating fully, including by giving in to demands concerning the transfer of banking and passenger data to the US security agencies and bodies. This pattern has been justified by arguing, for instance, that the bombings of 11 March 2004 in Madrid and 7 July 2005 in Madrid demonstrated that the EU and the US shared a common interest in promoting counter-terrorism policies. This has resulted in the signing of several

agreements, including a working agreement between EUROPOL and the US on data exchanges, agreements on mutual legal assistance in criminal justice matters and extradition, and the better-known PNR and SWIFT agreements. This orientation, however, has also been challenged, chiefly by the European Parliament, which expressed its opposition to the erosion of the respect for privacy and data protection, most notably in the case of the SWIFT agreement.

3.3.1.2. The post-Lisbon situation

The situation following the entry into force of the Lisbon Treaty is at this stage delicate to assess. On the one hand, a number of elements contribute to the reinforcement of the possibilities for ensuring effective compliance of the 'external dimension' of internal security with the freedom and justice sides of the AFSJ. External activities in the field of internal security have not been attributed a legal basis in the Treaties. In the meantime, the collapse of the pillar system and the incorporation of the Charter of Fundamental Rights in the Treaties mean that all EU policy areas have to comply with fundamental freedoms and rights guarantees. The redefinition of the position of High representative, together with the establishment of the European external action service, are susceptible to make practical interventions in this area more feasible for the European Parliament.

Another important change lies in the fact that the Lisbon Treaty grants the EU a single legal personality and provides a single legal basis for the conclusion of international agreements (Article 217 TFEU). Article 218 TFEU further establishes a single procedure for this purpose, where the consent of Parliament is required for all fields where the ordinary legislative procedure applies, and in the fields where the special legislative procedure requires consent (Article 218(6)(a) TFEU). In other cases, the Parliament is to be consulted, although the Council does have the option of fixing a time limit for the issuance of an opinion (Article 218(6)(b) TFEU). This implies that in matters falling under Article 87(3) TFEU (operational cooperation in internal security matters), Parliament may only be consulted, but this consultation is mandatory.

These two remarks suggest that **the post-Lisbon situation offers a number of possibilities for action, should the EP wish to continue on the course it has adopted so far regarding the external pursuit of internal security policies**. The situation has clearly changed with regard the EU's treating-making powers. Under the previous Treaty framework, Parliament interventions on the agreements on mutual legal assistance and on extradition, as well as on SWIFT, have been met with some degree of success insofar as they promoted greater transparency and insisted on compliance with fundamental freedoms and rights. Maintaining this course of action would seem the optimum way to make best use of the EP's new powers in this field and match upcoming developments. Changes regarding the conduct of operational activities by JHA agencies in third countries are less clear-cut. The question here is whether Article 87(3) should be considered as having effect in the field of external relations, and of the interface with CSDP, which is the other main policy domain where the ordinary legislative procedure and its correlates have not been extended.

3.3.2. EU internal security activities in third countries: key areas of concern for the future

3.3.2.1. The linkage between the internal and external aspect of security in the context of COSI and 'returns in internal security'

The question of the relations between internal and external security activities has recently been opened up in COSI discussions with the tabling of a note of the Hungarian Presidency on "Tightening links between the external and internal aspects of EU security" (Council document 5620/1/11). **There is a slight difference, however, between this issue and the overall question of the externalisation of internal security policies**. The main stake considered in the document is indeed the possibility for internal security actors to use CSDP activities for 'returns in internal security'. Two related points are brought up in the note:

- The possibility of "[e]nhancing the exchange of personal and strategic information and criminal intelligence between EU civilian crisis management missions and relevant EU agencies, namely EUROPOL, EUROJUST and FRONTEX" (5620/11, p. 2). Questions brought up by the Hungarian Presidency note include the feasibility of exchanging personal data between missions and agencies, but also of integrating CSDP sources of information in the devising of risk and threat assessments, using the civilian and military analysis capabilities of crisis management missions. A long-term aim would then be the integration of knowledge about security in the various 'products' of EU security agencies, including EUROPOL OCTAs, SOCTAs and TE-SATs, FRONTEX risk assessments or SitCen country and region reports.
- The possibility, accordingly, for internal security actors such as COSI or the JHA agencies, to participate in the planning of CSDP missions to streamline the principle of returns in internal security from the inception stage of crisis management missions.

These perspectives, of course, are not new. In November 2008, the JHA Council adopted conclusions "on possible cooperation mechanisms between civilian ESDP missions and EUROPOL as regards the mutual exchange of information" (Council document 15771/08), emphasising the importance of implementing such provisions as soon as possible in the context of the relations between EULEX and EUROPOL. A number of informal 'returns' have also been collected over the years by SitCen from ESDP/CSDP missions in the field, although the extent of this practice is difficult to assess due to this body's dedication to confidentiality.

The establishment of links between external and internal security would seem to be underway as far as Brussels actors are concerned. COSI adopted in June 2011 a 'working method' regarding the organisation of meetings among Brussels-based agencies, bodies and services (Council document 10715/11). The method foresees:

- The organisation of a quarterly inter-institutional information meeting between Council, Commission and EEAS. The meeting would include representatives from the different preparatory bodies of the Council involved in CSDP and internal security matters (e.g. PSC and COSI), the General Secretariat of the Council and Commission DGs (HOME, JUST and others if needed), as well as the EEAS and possibly other actors such as the CTC. The purpose of the meeting is mainly organisational, involving the preparation of agenda and exchange of information about past and upcoming meetings, the organisation of further joint meetings between Council bodies in charge of security issues, and relations with the European Parliament. The meeting would have officially no decision-making powers.
- The organisation of joint meetings between Council preparatory bodies on topical security issues, on the model of the first PSC-COSI meeting that took place on 1 June 2011, with possible presentations from the Commission and the EEAS. Besides PSC-COSI meetings, bodies under consideration would involve CIVCOM and the COSI Support Group, PROCIV (civil protection) and JAIEX (External JHA counsellors), the Council working group on terrorism (COTER) with the Terrorism Working Group (TWG) and possibly the CTC, and JAIEX meetings with the various geographical preparatory bodies in charge of external relations (e.g. COMAG/MAMA, COEST, COWEB, etc).
- The selection of key themes of common concerns to internal and external security practitioners. Tentative themes identified by the Hungarian presidency include terrorism, serious and organised crime as well as natural and man-made disasters.

There are two questions to address here. **Firstly, should these policy orientations be considered as a linkage between two distinct policy domains, or as a process of entanglement, which enables a degree of 'colonisation' of external security by internal security practitioners?** The second question concerns oversight. The issue, here, lies as much with accountability and transparency as with concerns for the compliance of such activities with legal obligations in the field of fundamental freedoms and rights. Internal security and CSDP are the two key EU policy domains that have been maintained out of the ordinary domain of EU law- and policy-making. It is where the Union's system of checks and balances remains the weakest. The monitoring of activities involving 'returns in internal security', in this regard, is a clear gap that should be addressed, all the more since the 'linkage' of CSDP and internal security is in the process of being formalised. **One point of entry, here, would be to insist on having truly inter-institutional quarterly information meetings that would not just discuss relations with the European Parliament, but actually involve representatives from the various Committees (centrally the LIBE Committee and Committee on Foreign Affairs)**. This can be justified on the basis of the provisions on information of the EP laid down in Article 87(3) TFEU, and would be without prejudice to the provisions on CFSP/CSDP and police cooperation in the Treaties, since the inter-institutional meeting does not have any decision-making powers.

3.3.2.2. The redefinition of relations with neighbouring countries in the field of freedom, security and justice

As mentioned above, neighbouring countries have been together with candidate countries key targets in the externalisation of EU internal security policies, whether through the activities of JHA agencies or through technical assistance project. While purported to include the full range of policies included in the EU AFSJ, a major part of these initiatives have focused on the security aspect. Engagement with neighbouring countries has for instance been an important component in the work of FRONTEX. Within the scope of the neighbourhood, the agency has entered into working arrangements with Ukraine, Moldova, Georgia and Belarus, and with countries that wield significant influence in the area, namely Russia and Turkey. As of February 2011, FRONTEX reports that it is at various stages of negotiations with Libya, Morocco and Egypt, and with countries in the close vicinity of the EU neighbourhood, namely Senegal, Mauritania and Nigeria.

The focalisation of external EU AFSJ activities on security has come under harsh criticism in the past few months in the light of the events in Tunisia, Egypt and Libya. The bulk of these criticisms have involved the engagement of specific Member States such as France and Italy with the security agencies and services of these countries, and their reaction to the arrivals on their territory of persons fleeing from areas of unrest. It has to do, more broadly, with the predominant concern that has informed the policies of the EU and its Member States over the past decade in relation to neighbouring countries, namely stability. One key question here is whether the use of initiatives such as the European neighbourhood policy as a channel for security activities is politically sound. In a recent communication, the European Commission and the High representative advocate for a 'new approach' to the neighbourhood in light of recent developments, which focalises on building and consolidating 'healthy democracies'. In the meantime, however, the JHA Council has insisted in its June 2011 conclusions on "enhancing the links between internal and external aspects of counter-terrorism" that the EEAS and the Commission "take a coordinated and coherent approach towards the strategic and multiannual indicative programming of the EU external assistance instruments such as the Development Cooperation Instrument (DCI) and the European Development Fund (EDF)" and "take into consideration the assessment of the terrorist threat when planning the allocation of funding from the European Neighbourhood Policy Instrument" (ENPI) (Council Document 11075/11, p. 9).

This aspect of the external relations challenge in the field of internal security can be met in two ways. Firstly, there **is clearly a need for monitoring the arrangements and agreements concluded by EU agencies and bodies with third countries in this**

area – with an emphasis on the activities of EUROPOL and FRONTEX. The derogation from the ordinary course of EU law- and policy-making established in Article 87(3) does not preclude the fact that the European Parliament and national Parliaments should be kept informed of such developments. Additionally, the use of hearings such as the ones recently held by the LIBE Committee on EU Counter-terrorism policy (April 2011) or on democratic accountability in the AFSJ (October 2010) organised together with national parliaments would ensure a degree of scrutiny on these questions. Secondly, the EP holds the possibility as budgetary authority to decide on the priorities of the EU's external assistance instruments such as the DCI, EDF and ENPI and their implementation by the European Commission. **Making sure that the new priorities adopted by the EEAS and the Commission for neighbouring countries are adequately funded is one way to see that all policy areas in the AFSJ are pursued in relations with third countries**.

3.3.3. The implications of third country security policies for EU fundamental freedoms and rights

3.3.3.1. Requirements of security cooperation with third countries and limitations of rights

Security cooperation with the United States has clearly placed the heaviest strain on EU policies in the field of freedom and justice in past years. The entry into force of the Lisbon Treaty has transformed the legal and institutional environment where this cooperation is unfolding, but established policy patterns appear to continue with very little changes. This is usefully illustrated by a recent controversy raised by the legal service of the European Commission in relation to the PNR agreement currently negotiated by the services of DG Home with the US. In a letter dated 18 May 2011, the legal service expressed "grave doubts as to [the draft agreement's] compatibility with the fundamental right to data protection" (Commission document SJ.1(2011) 603245). It questioned the scope of the agreement and its inclusion of minor crimes, the retention period (which exceeds the practice established in other such agreements), the absence of possibilities for judicial redress, and the extension of the use of PNR data to include the purpose of guaranteeing US border security. On the issue of retention, the legal service of the Commission points out that "it also represents almost no improvement compared to the current EU-US agreement, which the Parliament refused to approve" (SJ.1(2011) 603245, p. 2). The draft agreement was nonetheless transmitted by DG Home to the Council two days later (Council document 10453/11).

One issue here concerns **transparency and accountability**. It is striking, for one, that such agreements would be negotiated with confidential mandates to the extent that (without envisaging full public disclosure) EU bodies with a stake in the matter are not informed of their content. In the case of the PNR agreements with the US, Canada and Australia, for instance, the Article 29 Working Party has had to rely on a letter forwarded on 11 January 2011 to Commissioner Malmström to provide inputs on the fundamental rights aspects of the issue. Such agreements are notoriously difficult to monitor, as the 'discovery' of the MoU between Canada and the US on transfers of EU PNR data during the November 2008 joint review fully illustrates. The absence of information for concerned bodies and services regarding the mandates of negotiation complicates monitoring further, and can end up undermining the very goals of such agreements. In the case of the EU-US PNR agreement, enhanced transparency and monitoring could also ensure that controversies regarding compliance with the new Treaty-based obligations are avoided, and as such contribute to the support of EU institutions, bodies, offices and agencies by an open, efficient and independent administration (as laid out in Article 298(1) TFEU).

3.3.3.2. The challenge of importing security policies from third countries

Security cooperation with third countries can also lead EU authorities to reconsider the conduct of EU internal security policies. The most explicit case, here, is that of the EU TFTP and EU PNR proposals which are currently being considered. Both initiatives follow

from the requirements of cooperation with the US, which, as demonstrated previously, have themselves fuelled a number of controversies among the EU institutions over questions of privacy and data protection in particular.

The idea of an EU TFTP was initially discussed in the European Parliament resolution of 17 September 2009, which "notes that it may be useful for the Commission to evaluate the necessity of setting up a European TFTP"[243], amidst concerns for the protection of the fundamental freedoms and rights of EU citizens. The EU Counter-Terrorism Coordinator took the notion up a month later, albeit in different terms: concerned with the possibilities "to improve the way in which Member States are feeding information into EUROJUST and EUROPOL", his November 2009 discussion paper to the JHA Council and European Council suggests that the idea of an EU TFTP, together with an EU PNR system, should be pursued. "An added benefit of developing our own European PNR (or even TFTP) models would be the development of a more equal partnership with the US", concludes the paper.[244] Council Decision 2010/412/EU on the conclusion of the EU-US TFTP agreement calls upon the Commission "to submit to the European Parliament and to the Council, no later than one year from the date of entry into force of the Agreement, a legal and technical framework for the extraction of data on EU territory" (Article 2).[245] The legislative roadmap submitted by the European Commission in October 2010 is not particularly detailed, but argues in particular that the rationale for a European TFTP would be for the current system "to be replaced with one where the sending of bulk data can be replaced with more specific, targeted information. For that to be possible, a European system for collecting and analysing the financial messaging data will be required".[246]

Two questions can be raised with regard to these developments. Firstly, **should the EU's internal security policies be driven by considerations of diplomatic competition?** The development of a more equal partnership with the US, which is one of the concerns expressed by the CTC, might be obtained through other means than the replication of U.S. homeland security policies, for example by promoting the EU policies related to the right to data protection and the right to privacy. Secondly, **is it possible to develop additional capacities for the collect and processing of personal data for internal security purposes in the name of the protection of fundamental rights and freedoms?** The European Commission's current roadmap frames the creation of a European TFTP as a protective measure, which would ensure that only custom-tailored information is transferred to the US authorities. **But this 'targeting' will only take place after the "financial messaging data of a large portion of populations both within the Union and abroad" (to cite the Commission's words) is collected and processed**. As it is envisaged that EUROPOL would be put in charge of the European TFTP, such a measure would in addition further reinforce the predominance of this agency, and widen its access to personal data. The fact that the processing will take place on EU territory will certainly provide more legal certainty and guarantees to EU citizens, but there is nonetheless a need to address the various pressing questions that have been raised in this study, including on the issue of oversight and of the 'technological challenge', before considering the establishment of a European TFTP. In the meantime, as one analyst points out, cooperation with the United States has enabled the consideration of an initiative which European internal security agencies, bodies and services would have

[243] European Parliament (2009), Resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism, P7_TA(2009)0016, 17.9.2009.

[244] Council of the European Union (2009), "EU Counter-Terrorism Strategy – discussion paper", 15359/1/09, 26.11.2009, p. 7.

[245] Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purpose of the Terrorist Finance Tracking Programme, OJ L195/3, 27.7.2010.

[246] European Commission (2010), European Terrorist Financing Tracking Programme (European TFTP), 2011/HOME/03 – Version No.2, 10.2010, p. 1.

considered unthinkable a few years ago.[247] This development further highlights the need to extend considerations related to policy assessment and oversight fully to the external dimension of the EU's internal security policies.

[247] A. Amicelle (2011), "The Great (Data) Bank Robbery", op. cit.

CONCLUSION

The key question facing the internal security policies of the European Union following the entry into force of the Lisbon treaty and in the context of the devising of an EU Internal Security strategy is the possibility of change.

Change does not involve so much the tension between national sovereignty, of which security would be a key component, and European integration. It is, rather, about taking stock of the new institutional context and the streamlining of the policies and procedures initially developed in the context of the third pillar into the ordinary process of policy and law-making.

As this study has highlighted, current developments related to the EU-ISS and internal security policies put this capacity for change into question. The issue, as suggested, is not a reluctance to perform the transformations required by the framework of the Treaties, but the actual capacity to alter established courses of action.

Some elements suggest that there is potential for change. The splitting of DG JLS, for one, has sent a strong signal that institutional frameworks originally established in the context of the Schengen cooperation and the Maastricht treaty could be altered. Other developments, for example in the establishment of relations between the FRA and JHA agencies, or in the fact that the views of the European Parliament are increasingly taken into account, constitute similar indications.

This dynamic of change has arguably to be accompanied and nurtured. The old habits of work as it was conducted under the third pillar remain strongly rooted. As in the case of the establishment of COSI and the adoption of the EU “policy cycle” in internal security matters, this persistence can be accompanied by new sets of procedures and institutional mechanisms.

Oversight is a central component for sustaining change.

Accountability and transparency, as a key component of oversight, are not only exceptional demands, or concessions to civil liberties advocates. They can contribute to better assessment of initiatives and policies. A good illustration relates to the concerns over the quality and methodology of the analyses and assessments that have become so important in the conduct of “intelligence-led” security policies. Accountability and transparency, here, can support external and independent evaluations.

By the same token, the constant involvement of those agencies and bodies which are currently included only at the margin of internal security policies, such as the EDPS and Article 29 Working Party, the FRA and the Ombudsman, could bring about significant added value to the policy process itself. Streamlining oversight would allow for policies that are better assessed and routinely examined. Such work requires capabilities, but also demands that these different agencies and bodies operate more closely together.

The European Parliament, together with national parliaments, faces more demands in this regard. This is coherent with the new possibilities that it has obtained under the new Treaty framework. In a number of occasions, particularly on issues such as TFTP and PNR agreements, its involvement has proven critical. The challenge is to turn the results obtained in these specific cases in a regular activity.

RECOMMENDATIONS

The following recommendations take stock of the findings of the study and are all directed towards a greater involvement of the European Parliament at all stages of the policy process in the field of EU internal security.

1. The Involvement of The European Parliament: the Pre-Requisites

The recommendations that follow imply that some pre-requisites are in place, such as an efficient cooperation between the European Parliament and national parliaments and the establishment of inter-parliamentary oversight structures.

On that matter, a permanent inter-parliamentary body/committee should be set up dealing specifically with EU regulatory agencies. This body should be run by the European Parliament's LIBE Committee, with the participation of other relevant committees, and including the representatives of corresponding committees from the national parliaments. The inter-parliamentary body would organise regular meetings and hearings focused on the EU Home Affairs agencies. It could have the possibility to set up 'confidential working groups' assessing the secret/non publicly disclosed operating plans, risks analyses and threat assessments and working arrangements with third countries and other actors constituting the basis of their operations in order to examine their proportionality (including from a budgetary point of view), soundness and added value.

2. The development of an evidence-based EU policy : a condition for budgetary arbitration

Ensuring that the EU's policy in the field of counter-terrorism and organised crime is evidence-based and supported by the best available threat assessments is critical for the European Parliament in order to discuss budget priorities.
The methodology used to develop documents such as threat assessment reports, policy-planning documents should be made publicly available to enable external and independent reviewing and assessment. These documents must receive closer scrutiny and supervision. There exists a significant degree of expertise pooled among the research projects funded under the EU's 6th and 7th Framework Programmes to ensure an external evaluation of the highest quality. Other bodies of the European Union have relied on such external and independent support and review in this area.
The question of knowledge is furthermore not limited to the provision of expertise to internal security agencies, bodies and services, be it external and independent. An evidence-based EU policy in the field of internal security can only benefit from a pluralistic and contradictory debate. There are a number of tools available to the EU institutions to ensure that such a debate takes place. These include the briefing notes and studies that can be requested by the European Parliament, but also the research projects funded under the EU's Framework Programmes. Despite the fact that in recent years, the handling of the latter with regard to security research, and especially of the FP7 Security Theme (FP7-ST), has become a source of concern, the priorities and funding of research in the field of security research constitute areas where the European Parliament has a strong capacity for intervention through its powers as budgetary authority.

As underlined by the LIBE Rapporteur on the Counter-Terrorism Policy, a proper evaluation of ten years of counter-terrorism policies would provide the basis for an evidence-based, needs-driven, coherent and comprehensive EU counter-terrorism

strategy. A panel of independent experts could carry such an in-depth and complete appraisal. Such panel should not only set out clearly the results of the policies in terms of increased security in Europe, but also include a full overview of the accumulated impact of counter-terrorism measures on civil liberties. The European Parliament needs to have a specific budget for independent experts and scholars, in the same way that the US Congress does for instance. Funding selected academic networks or centres of excellence following different policy areas in the domain of security, freedom and mobility and from different disciplinary perspectives would be an efficient way to deliver independent inputs.

The corollary of a broader evidence base and more pluralistic knowledge base in the field of internal security is access to information. All Member State national Parliaments have, to one degree or another, developed mechanisms of oversight for policies involving classified materials, and this should be a priority for the European Parliament as well.

As an addition to this monitoring of the knowledge channels that is required for sound budgetary arbitrations, the clarification of the role of some EU agencies is needed in order to avoid task duplications/overlapping and unnecessary budget expenses. Therefore, the role, tasks, mandates of the EU CTC, OLAF, ENISA, in relation to the ISS need to be reviewed, and if need be clarified. The examination of the role of several components of the Council working structures could also be useful in this regard. The European Parliament could for instance contribute to the assessment of the necessity of CATS and SCIFA, which is supposed to take place from 1 January 2012.

3. Ensuring parliamentary oversight of EU policy process in the field of internal security

Further monitoring of EU council structures, firstly, is highly needed, specifically in relation to COSI. A good reason for this is the exclusion of operational cooperation matters from the ordinary legislative procedure established in Article 87(3) TFEU. This provision weakens the system of checks and balances between the EU institutions, insofar as Parliament is only “consulted” as opposed to ordinary circumstances where it is on equal footing with the Council. The need to further specify mechanisms through which European Parliament and national Parliaments are kept “informed” and how their comments can be taken on board must be a priority for the EP in relation to operational cooperation matters in internal security. Such mechanisms could draw from Article 70 TFEU on impartial evaluation of EU policies, Article 71 TFEU on COSI and Article 6(2) of the COSI Decision.

The right of the EP to request at any time that a representative of EUROPOL to appear before the EP allows members of the European Parliament to ask questions and to stage debates when appropriate. This right should be used more frequently and be extended to the equivalent persons at Eurojust and Frontex.

Furthermore, Article 71 TFEU provides a legal basis for the EP to actively stage hearings. Hearings can be based on Rule 193(2) of the European Parliament’s rules of procedures. Regular hearings could promote the new system of checks and balances introduced by the Lisbon Treaty and contribute to the regular monitoring of activities in the field of internal security. For more prominent cases, there are two possibilities:

a) Rule 184 of the EP’s rules of procedure provides for the creation of special committees, on a proposal from the Conference of Presidents. The term of office of such a committee may not exceed 12 months, unless decided otherwise by Parliament upon its expiry. One possibility would be to set up a special committee

with powers to monitor internal security activities and see that all the agencies, bodies and services involved inform the EP.

b) Temporary committees of inquiry: particular potent tool with a treaty base (Article 226 TFEU, Rule 185 of the EP's rules of procedure). The EP can convene such committees to investigate alleged contraventions or maladministration in the implementation of EU law, except where the alleged facts are already being investigated by a court.

The use of hearings such as the ones held over the past year by the LIBE Committee on EU Counter-terrorism policy or on democratic accountability in the AFSJ organised together with national parliaments establish an additional way of scrutiny on these questions.

4. Ensuring parliamentary oversight of EU security agencies in the field of data protection

The shift towards a more intelligence-driven logic relying on intensive data processing in the work of EUROJUST, EUROPOL and FRONTEX deserves close scrutiny and a stricter framework of oversight.

Any process of personal data should receive full attention from the EP. The modalities through which access to information systems are granted, data is exchanged and stored should be firmly monitored and guaranteed. The LIBE Committee must ensure that the provision that special categories of data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, party or trade union membership, sexual orientation or health shall not be processed and saved unless when this is absolutely necessary and proportionate for the purpose of a specific case and subject to specific safeguards.

Under the changing of circumstances provided by the Lisbon Treaty (co-decision), the European Parliament can now be more involved in data protection issues and should receive reports prepared by the Joint Supervisory Bodies of EUROJUST and EUROPOL. The revision of the EU legal framework for the right to data protection would be a good occasion to raise this question. On that matter, the spirit of the Lisbon Treaty and the 'depillarisation' process should lead to the suppression of Supervisory Bodies per agencies. Supervisory bodies within EU agencies should be at the very least be organised into a network, and a common supervision system under the EDPS should be established. The EP should call for more adequacies of the review mechanisms in place. Likewise, the existence of two legal frameworks in EU data protection law should be reconsidered.

The question of the processing of personal data also calls for further monitoring in the evaluation and assessment of the practical implementation of technological schemes for internal security. For instance, if the idea of a "dialogue" between the public and private sectors on security and technology detailed in this study, involving all the concerned parties, is to be pursued, it should be done from a fully transparent, well-assessed and accountable process.

5. Promoting a "shared culture" of Fundamental Rights in the European internal security agencies and policies

As detailed in the study, there are grounds to include agencies and bodies in charge of fundamental freedoms and rights in the EU policies and strategies in the field of internal security. There are for instance solid grounds for involving bodies such as the FRA or the EDPS in the planning of operational priorities undertaken by COSI. The possibility of legal action over operational activities coordinated by the EU, and the related need to ensure that fundamental freedoms and rights are upheld in these activities gives the freedom agencies more means to intervene in the internal security debate. Furthermore, FRA opinions on JHA matters should become more systematic, and the FRA should include considerations on criminal matters in its annual reports. The FRA should likewise make use of its powers in the post-Lisbon context to assess the ISS from a fundamental rights perspective. The expansion of its activities as regards independent and objective evaluation (not only research activities) of EU policies covering in particular the domains of police cooperation and criminal justice, could be considered. Finally, a more integrated cooperation and coordination between EU (freedom) agencies, such as the European Agency for Fundamental Rights (FRA), the European Data Protection Supervisor (EDPS), the European Ombudsman, should be brought forward.

The strengthening of the links between EU agencies in charge of fundamental rights and freedoms should be accompanied by further efforts to promote joint endeavours with EU JHA agencies. The involvement of the FRA as the fifth JHA agency is an important development. Further links could be envisaged with CEPOL for instance. Human Rights are specifically mentioned as a training priority in the College's strategy for the next five years. A real improvement should be to envisage coordination mechanisms between CEPOL and bodies such as the EDPS and the FRA, which could certainly contribute to the devising of common curricula alongside the work already done on judicial matters with EUROJUST. CEPOL could become a central training place for the role of human rights in juridical and operational matters. Finally, CEPOL could also act as a "prospective" centre investigating trends which are not the ones that Europol and Eurojust focus on, notably on issues related to security policies and human rights.

The new legal framework introduced by the Lisbon Treaty implies that European internal security professionals will regularly have to assess how their activities relate to the Charter of Fundamental Rights and the case-law of the ECJ. This opens interesting paths that could be promoted by the European Parliament in order to build up a "shared culture" of fundamental rights in EU security issues.

REFERENCES

Alegre, S. (2008), "Human Rights concerns relevant to legislation on provocation or incitement to terrorism and related offences", PE 393.283, European Parliament, Brussels.

Alegre, S., D. Bigo and J. Jeandesboz (2009), "External Dimension of the Area of Freedom, Security and Justice", PE 410.688, European Parliament, Brussels.

Alfano, S. (2011), "Report on organised crime in the European Union", PE 454.687v04-00, European Parliament, Brussels.

Amicelle, A. (2011), "The Great (Data) Bank Robbery: Terrorist Financing Tracking Program and the 'SWIFT Affair'", QDR No. 36, CERI, Paris.

Amnesty International and ECRE (2010), Joint Briefing on the Commission proposal to amend Frontex, of September (www.ecre.org/component/downloads/downloads/58.html).

Andoura, S. and P. Timmerman (2008), "Governance of the EU: The Reform Debate on European Agencies Reignited", CEPS, Brussels.

Article 29 Working Party and Working Party on Police and Justice (2009), "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", Working Paper No. 168, 1.12.2009.

Article 29 Working Party (2010), "Report on the second joint enforcement action", 00068/10/EN, WP 172.

Article 29 Working Party (2010), "Opinion 3/2010 on the principle of accountability", 00062/10/EN, WP 173, 13.7.2010.

Article 29 Working Party (2011), "Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", 00664/11/EN, WP 181.

Baldaccini, A. et al. (2008), *Controlling Security*, Paris: L'Harmattan.

Balzacq, T. et al. (2006), "Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats", CEPS Working Document No. 234, CEPS, Brussels.

Balzacq, T. (2008), "Implications of European Neighbourhood Policy in the Context of Border Controls", PE 393.284, European Parliament, Brussels.

Balzacq, T. and S. Carrera (eds) (2005), *Security Versus Freedom? A Challenge for Europe's Future*, London: Ashgate.

Beare, M. (ed.) (2003), *Critical Reflections on Transnational Organized Crime, Money Laundering, and Corruption*, Toronto: Toronto University Press.

Beare, M. and R.T. Naylor (1999), "Major Issues Relating to Organized Crime: Within the Context of Economic Relationships", Law Commission of Canada, Nathanson Centre, Toronto.

Beckett, K. and S. Herbert (2011), *Banished. The New Social Control in Urban America*, Oxford: Oxford University Press.

Berthelet, P. (2011), *Le paysage européen de la sécurité intérieure*, Zurich: Peter Lang.

Bigo, B. et al. (2008), *The Field of the EU Internal Security Agencies*, Paris: l'Harmattan.

Bigo, B. et al. (2008), *Au nom du 11 Septembre. Les démocraties à l'épreuve de l'antiterrorisme*, Paris : La Découverte.

Bigo, D. and A. Tsoukala (eds) (2008), *Terror, Insecurity and Liberty: Illiberal practices of liberal regimes after 9/11*, London: Routledge.

Bigo, D. and J. Jeandesboz (2009), "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'", INEX Policy Brief No. 5, CEPS, Brussels.

Bigo, D., S. Carrera, E. Guild and R.B.J. Walker (eds) (2010), *Europe's 21st Century Challenge: Delivering Liberty*, London: Ashgate.

Bigo, D. et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament", PE 453.216, European Parliament, Brussels.

Brodeur, J.P. (2002), "Crime organisé", in L. Muchielli and P. Robert (eds), *Crime et sécurité. L'Etat des savoirs*, Paris: La Découverte, pp. 242-251.

Brodeur, J.P. and B. Dupont (2004), "Introductory essay: The role of knowledge and networks in policing", in T. Williamson (ed.), *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*, Chichester: John Wiley & Sons Ltd, pp. 9-33.

Brouwer, E. (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System,* Leiden: Martinus Nijhoff.

Bunyan, T. (1993), "Trevi, Europol and the European State, Statewatching the new Europe", Statewatch, London.

Burgess, J.P. and M. Hanssen (2008), "Public Private Dialogue in Security Research", PE 393.286, European Parliament, Brussels.

Carrera, S. and E. Guild (2009), "Towards the Next Phase of the EU's Area of Freedom, Security and Justice: The European Commission's Proposals for the Stockholm Programme", CEPS Policy Brief No. 196, CEPS Brussels.

_____ (2010), "'Joint Operation RABIT 2010' – FRONTEX Assistance to Greece's Border with Turkey: Revealing the Deficiencies of Europe's Dublin Asylum System", CEPS, Brussels.

CFI, T-228/02, Organisation des Modjhahedin du people d'Iran v. Council of the European Union, 12.12.2006.

Commission nationale de l'informatique et des libertés (2009), Conclusions du contrôle du système de traitement des infractions constates (STIC) – Rapport remis au Premier Ministre le 20 janvier 2009, CNIL, Paris.

Council of Europe (2004), *"Apologie du Terrorisme" and "Incitement to terrorism"*, Council of Europe, Strasbourg.

_____ (2005), *Security and social cohesion: Deconstructing fear (of others) by going beyond stereotypes*, Strasbourg: Council of Europe Publishing.

_____ (2005), Human rights and the fight against terrorism –The Council of Europe Guidelines, Council of Europe, Strasbourg.

_____ (2007), Conclusions of the Council of Europe conference "Why terrorism? Addressing the Conditions Conducive to the Spread of Terrorism", Council of Europe, Strasbourg (www.coe.int/t/dlapil/codexter/conf_whyTerrorism_en.asp).

_____ (2007), *The fight against terrorism – Council of Europe standards*, Strasbourg: Council of Europe (4th edition).

_____ (2008), Council of Europe's White Paper on Intercultural Dialogue, Council of Europe, Strasbourg (www.coe.int/t/dg4/intercultural/Source/Pub_White_Paper/White%20Paper_final_revised _EN.pdf).

Council of the European Union (2000), *Decision of 22 December 2000 establishing a European Police College (CEPOL)* (2000/820/JHA), OJ L336/1, 30.12.2000.

_____ (2001), Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II), OJ L 328/1, 13.12.2001

_____ (2001), Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II), OJ L 328/4, 13.12.2001.

_____ (2005), Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation particularly in combating terrorism, cross-border crime and illegal migration, Prüm, Germany*, 27 May 2005*, 10900/05, 7.7.2005.

_____ (2001), Common Position of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP), OJ L344/93, 28.12.2001

_____ (2001), Regulation (EC) No. 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, OJ L344/70, 28.12.2001

_____ (2002), Provisional management solution for the European Police College (CEPOL), 6603/02, 26.2.2002.

_____ (2003), Three-year report on the operation and future of the European Police College, 15722/03, 9.12.2003.

_____ (2003), European Security Strategy, 15895/03, 8.12.2003.

_____ (2003), Three year report on the operation and future of the European Police College, 15722/03, 9.12.2003.

_____ (2004), Three-year report on the operation and the future of the European Police College, 5136/04, 8.1.2004.

_____ (2004), Decision 2004/566/JHA of 26 July 2004 amending Decision 2000/820/JHA establishing a European Police College (CEPOL), OJ L251/19, 27.7.2004.

_____ (2004), Decision 2004/567/JHA of 26 July 2004 amending Decision 2000/820/JHA establishing a European Police College (CEPOL), OJ L251/20, 27.7.2004

_____ (2004), Three year report on the operation and future of the European Police College, 5880/04, 2.2.2004.

_____ (2005), EU SitCen Work Programme, 5244/05, 11.1.2005 (declassified 20.12.2005).

_____ (2004), Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC), OJ L213/5, 15.6.2004.

_____ (2004), Adoption of a proposal for a Council Decision establishing the European Police College (CEPOL), 10534/05, 24.6.2005.

_____ (2004), Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism (OJ L162/29, 30.04.2004).

_____ (2005), Decision on some new functions for the Schengen Information System, including in the fight against terrorism (OJ L68/44, 15.3.2005).

_____ (2005), Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, 9778/2/05, 10.6.2005.

_____ (2005), Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA, OJ L256/63, 1.10.2005.

_____ (2005), A Strategy for the External Dimension of JHA: Global Freedom, Security and Justice, 14366/05, 11.11.2005.

_____ (2005), Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law-enforcement authorities of the Member States of the European Union, OJ L386/15, 25.11.2005

_____ (2006), Two Year Report on the Operation and Future of the European Police College, 5727/06, 7.2.2006.

_____ (2007), Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, OJ L53/1, 22.2.2007.

_____ (2007), Overview of SitCen reports and Political Recommendations, 7261/07, 12.3.2007 (declassified 28.5.2009).
_____ (2008), Report on the Implementation of the European Security Strategy – Providing Security in a Changing World, 17104/08, 10.12.2008.
_____ (2008), Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 30.12.2008.
_____ (2009), Draft Council Conclusions on an Information Management Strategy for EU Internal Security, 16637/09, 25.11.2009.
_____ (2009), EU Counter-Terrorism Strategy – discussion paper, 15359/1/09, 26.11.2009
_____ (2010), CEPOL Strategy, 15068/10, 18.10.2010.
_____ (2010), Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU), OJ L201/30, 3.8.2010.
_____ (2010), Outcome of proceedings of CATS on 11 February 2010, 6557/10, 11.2.2010.
_____ (2010), Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 5842/2/10, 23.2.2010.
_____ (2010), The Stockholm Programme – An open and secure Europe serving the citizen, 5731/10, 3.3.2010.
_____ (2010), Final report on cooperation between JHA Agencies, 8387/10, 9.4.2010.
_____ (2010), Council Conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal migration, 6975/10, 1.3.2010.
_____ (2010), Final report and recommendations of Project Group "Measure 6", 7942/2/11, 6.7.2011.
_____ (2010), Standing committee on operational cooperation in internal security (COSI) – Summary of discussions, 14651/10, 8.10.2010.
_____ (2010), Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purpose of the Terrorist Finance Tracking Programme, OJ L195/3, 27.7.2010.
_____ (2011), CEPOL five-year report, 7764/11, 17.3.2011.
_____ (2011), Report on the cooperation between JHA Agencies in 2010, 5675/11, 25.1.2011.
_____ (2011), "Expansion of the Joint Situation Centre (SitCen)", 5626/11, 24.1.2011.
_____ (2011), Report on the cooperation between JHA Agencies in 2010, 5675/11, 25.1.2011; (2011), Draft Scorecard – Implementation of the JHA Agencies report, 5676/11, 9.4.2010.
_____ (2011), CEPOL five-year report, 7764/11, 17.3.2011.
_____ (2011), Report on cooperation between JHA Agencies in 2010, 5675/11, 25.1.2011.
_____ (2011), JHA agency cooperation – Midterm report January-May 2011 – Activities and Key Findings, 10404/11, 19.5.2011.
_____ (2011), Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies, 10140/11, 18.4.2011.
Crawford, A. (ed.) (2009), *Crime Prevention Policies in Comparative Perspective*, Cullompton: Willan Publishing.
De Hert P. and R. Bellanova (2009), "Data Protection in the area of Freedom, Security and Justice: A system still to be fully developed?", PE 410.692, European Parliament, Brussels.

De Hert, P. and R. Bellanova (2011), "Transatlantic Cooperation on Travellers' Data Processing: From Sorting Countries to Sorting Individuals", Migration Policy Institute, Washington, D.C..

De Vries, K., R. Bellanova and P. De Hert (2010), "Proportionality overrides Unlimited Surveillance: The German Constitutional Court Judgement on Data Retention", CEPS, Brussels.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31, 23.11.1995.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and privacy and electronic communications), OJ L201/37, 31.2.2002.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks and amending Directive 2002/58/EC, OJ L105/54, 13.4.2006.

Dumitriu, E. (2004), "The E.U.'s Definition of Terrorism: The Council Framework Decision on Combating Terrorism", *German Law Journal*, Vol. 5, No 5, pp. 585-602.

Edwards, A. and P. Gill (eds) (2003), *Transnational Organised Crime. Perspectives on global security*, Routledge, London.

European Commission (2004), Proposal for a Council Decision establishing the European Police College (CEPOL) as a body of the European Union, COM(2004) 623 final, 1.10.2004.

_____ (2005), The Hague Programme: 10 priorities for the next five years, COM(2005) 184 final, 10.5.2005.

_____ (2005), A strategy on the external dimension of the area of freedom, security and justice, COM(2005) 491 final, 12.10.2005.

_____ (2005), Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24.11.2005

_____ (2005), Compliance with the Charter of Fundamental Rights in Commission legislative proposals, COM(2005) 172 final, 27.4.2005.

_____ (2006), Implementing the Hague Programme: the way forward, COM(2006) 331 final, 28.6.2006.

_____ (2007), Communication on Public-Private Dialogue in Security Research and Innovation, COM(2007) 511 final, 11.9.2007.

_____ (2007), Proposal for a Council Framework Decision on the use of Passenger Name Records (PNR) for law enforcement purposes, COM(2007) 654, 6.11.2007.

_____ (2008), Annex to the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas – extended impact assessment, SEC(2004) 1628 final, 28.12.2004.

_____ (2008), Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008.

_____ (2008), Preparing the next steps in border management in the European Union, SEC(2008) 153 final, 13.2.2008.

_____ (2009), Communication on an area of freedom, security and justice serving the citizens, COM (2009)262 final, 10.05.2009.

_____ (2009), Moving Europe: EU research on migration and policy needs, DG Research, Brussels.

_____ (2009), Decision determining the first regions for the start of operations of the Visa Information System (VIS) (2010/49/EC), OJ L23/62, 27.1.2010.
_____ (2009), Impact Assessment Guidelines, SEC(2009) 92 final, 15.1.2009.
_____ (2009), Report on progress made in developing the European border surveillance system, SEC(2009) 1265 final, 24.9.2009.
_____ (2009), Consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures, COM(2009) 665 final, 2.12.2009.
_____ (2010), Legislative proposal to set up Entry/Exit System, JHA/2010/004, 8.2010.
_____ (2010), The Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of EUROPOL's activities by the European Parliament, together with national Parliaments (Brussels, 17.12.2010, COM(2010) 776 final).
_____ (2010), European Terrorist Financing Tracking Programme (European TFTP), 2011/HOME/03 – Version No.2, 10.2010.
_____ (2010), Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010), 573 final, 19.10.2010.
_____ (2010), Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, 20.7.2010.
_____ (2010), A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4.11.2010.
_____ (2010), The EU Counter-Terrorism Policy: main achievements and future challenges, COM(2010) 386 final, 20.7.2010.
_____, (2011), Report from the Commission to the EP and the Council on the implementation since 2007 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, COM(2011) 175 final, Brussels, 11.4.2011.
_____ (2011), Evaluation report on the Data Retention Directive (Directive 2006/34/EC), COM(2011) 225 final, 18.4.2011.
_____ (2011), Implementing Decision of 21 September 2011 determining the date from which the Visa Information System (VIS) is to start operations in a first region (2011/636/EU), OJ L249/18, 27.9.2011.
_____ (2011), Determining the technical and operational framework of the European border surveillance system (EUROSUR) and the actions to be taken for its establishment, SEC(2011) 145 final, 28.1.2011.
_____ (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 2.2.2011.
_____ (2011), Accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SEC(2011) 133 final, 2.2.2011.
_____ (2011), Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purpose of the Terrorist Finance Tracking Program, SEC(2011) 438 final, 17.2.2011.
_____ (2011), A European terrorist finance tracking system: available options, COM(2011) 429 final, 13.7.2011.
_____ (2011), Smart borders – options and the way ahead, COM(2011) 680 final, 25.10.2011.

European Court of Auditors (2008), Report on the annual accounts of the European Police College for the financial year 2007 together with the College's replies, OJ C311/136, 5.12.2008.

_____ (2009), Report on the annual accounts of the European Police College for the financial year 2008 together with the College's replies, OJ C304/124, 15.12.2009.

European Data Protection Authorities (2008), Declaration on three communications from the Commission on border management, Rome, 18 April.

EDPS (2008), Preliminary comments of the European Data Protection Supervisor on three communications from the Commission on border management COM(2008) 69 final, COM(2008) 68 final, COM(2008) 67 final, 3 March 2008.

_____ (2011), Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May.

_____ (2011), Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 25.3.2011.

_____ (2011), Opinion on the Communication from the Commission "A comprehensive approach on personal data protection in the European Union", EDPS, Brussels, 14.1.2011.

European Digital Rights (2011), Shadow evaluation of the Data Retention Directive (2006/24/EC), EDRI, Brussels, 17 April.

European Parliament (2001), "Transparency and intelligence", intervention of the Counter-Terrorism Coordinator Gilles de Kerchove, Brussels, Hearing on the Right to access to EU documents: implementation and future of Regulation (EC) No 1049/2001.

_____ (2006), Security Research: European Parliament resolution on Security Research – The Next Steps (2004/2171(INI)), OJ C133/135, 8.6.2006.

_____ (2008), Resolution of 20 November 2008 on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, P6_TA(2008)0561, 20.11.2008.

_____ (2009), European Parliament recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)), OJ C184/119, 8.7.2010.

_____ (2009), Resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism, P7_TA(2009)0016, 17.9.2009.

_____ (2010), Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year 2008 (2010/556/EU), OJ L 252/232, 25.9.2010.

_____ (2010), Resolution of the European Parliament of 5 May 2010 with observations forming an integral part of its Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year 2008, OJ L252/233, 25.9.2010.

_____ (2010), Legislative resolution on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purpose of the Terrorist Finance Tracking Program, P7_TA(2010)0279.

_____ (2011), Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year 2009 (2011/619/EU), OJ L250/268, 27.9.2011.

_____ (2011), Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year 2009 (C7-0241/2010 – 2010/2181(DEC), pending publication in the Official Journal, 25.10.2011.

_____ (2011), European Parliament resolution of 25 October 2011 with observations forming an integral part of its Decision on discharge in respect of the implementation of the budget of the European Police College for the financial year2009 (C7-0241/2010 – 2010/2181(DEC)), A7-0330/2011, 25.10.2011.

_____ (2011), European Parliament resolution of 8 June 2011 on the mid-term review of the Seventh Framework Programme of the European Union for research, technological development and demonstration activities (2011/2043(INI)), P7_TA-PROV(2011)0256, 8.6.2011, §.27.

_____ (2011), Report on a comprehensive approach on personal data protection in the European Union, Brussels, A7-0244/2011, 22.6.2011.

European Policy Evaluation Consortium (2004), "Study for the extended impact assessment of the Visa Information System", EPEC, Brussels, 12.2004.

European Ombudsman Annual Report, 2010.

European Organisation for Security (2009), "White Paper: A European Approach to Border Management", EOS, Brussels.

European Union Agency for Fundamental Rights (2011), Opinion on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final), 1/2011.

Favarel-Garrigues, G. (2001), « Concurrence et confusion des discours sur le crime organisé en Russie », *Cultures & Conflits*, No 42, pp. 9-46.

Fijnaut C. et al. (1998), *Organized Crime in the Netherlands*, The Hague: Kluwer.

Frattini, F. (2005), Intervention at conference on "The Hague Programme: A partnership for the European Renewal in the Field of Freedom, Security and Justice", organised by the Centre for European Policy Studies (CEPS), Brussels 14 July.

Geyer, F. (2007), "Fruit of the Poisonous Tree: Member States' Indirect Use of Extraordinary Rendition and the EU Counter-Terrorism Strategy", CEPS Working Document No.263, CEPS, Brussels.

_____. (2008), "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", CHALLENGE Research Paper No. 9, CEPS, Brussels.

Guild, E. (2010), "EU Counter-terrorism Action: A fault line between law and politics?", CEPS, Brussels.

Guild, E. and F. Geyer (eds) (2008), *Security Versus Justice? Police and Judicial Cooperation in the European Union*, London: Ashgate.

Guild, E. and S. Carrera (2011), "Towards an Internal (In)security Strategy for the EU?", CEPS, Brussels.

Guittet, E.-P. (2008), "Miscarriages of Justice and Exceptional Procedures in the War against Terrorism", CEPS, Brussels.

Gonzalez Fuster, G. et al. (2010), "Profiling in the European Union: A High Risk Practice", INEX Policy Brief No. 10, CEPS, Brussels.

Hailbronner, K. (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to the United States of America", PE 348.589, European Parliament, Brussels.

Hayes, B. (2006), *Arming Big Brother: The EU's Security Research Programme*, Statewatch/TNI, Amsterdam/London.

Hayes, B. (2009), *Neoconopticon: The EU Security-Industrial Complex*, Statewatch/TNI, Amsterdam/London.

Helmbrecht, U. (2011), *ENISA today and in the future*, Committee on Industry, Research and Energy, Mini-Hearing on ENISA, European Parliament, Brussels.

Hempel, L. et al. (2009), *Exchange of information and data between law-enforcement authorities within the European Union*, PE 419.590, European Parliament, Brussels.

House of Lords (2004), Select Committee on European Union Fourth Report: Letter from Caroline Flint MP to the Chairman, London, 15 December.

_____ (2004), "Judicial Cooperation in the EU: the role of Eurojust", The Stationery Office, London.

_____ (2005), European Union Committee 5th Report of Session 2004-05 - After Madrid: the EU's response to terrorism - Report with evidence,; House of Lords (2011), European Union Committee 17th Report of Session 2010-12 – The EU Internal Security Strategy, The Stationery Office, London.

_____ (2007), "Schengen Information System II: Report with Evidence", The Stationery Office, London.

_____ (2008), "European Union Committee, 9th Report of Session 2007-2008: Minutes of Evidence", House of Lords, London, 5 March.

_____ (2011), "The EU Internal Security Strategy", The Stationery Office, London.

Hughes G. and A. Edwards (eds) (2002), *Crime Control and Community: The new politics of public safety,* Cullompton: Willan Publishing.

Hustinx, P. (2009), *Data Protection and the need for an EU Information Management Strategy*, Council Ad Hoc Working Group on Information Exchange, Reception by the Swedish Presidency, Brussels, 6.7.2009.

Int'Veld, S. (2011), "Report on the EU Counter-Terrorism Policy: main achievements and future challenges", PE 460.953v02-00, European Parliament, Brussels.

International Commission of Jurists (2008), "Briefing Paper: Amendment to the Framework Decision on Combating Terrorism – Provocation to Commit a Terrorist Offence" (www.un.org/en/sc/ctc/ specialmeetings/2011/docs/icj/icj-2008-fd2007-650.pdf).

Jeandesboz, J. and F. Ragazzi (2010), "Review of security measures in the Research Framework Programme", PE 432.740, European Parliament, Brussels.

Jones, F. (2007), "Agencies: origins of tasks, local conditions and staffing", PE 381.092, European Parliament, Brussels, 17.10.2007.

Lavenex, S. and N. Wichmann (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to the Countries covered by the European Neighbourhood Policy (ENP)", PE 348.596, European Parliament, Brussels.

Levi, M. and M. Maguire (2004), "Reducing and Preventing Organised crime: An Evidence-Based Critique", *Crime, Law and Social Change*, Vol. 41, pp. 397-469.

de Lobkowicz, W. (2002), *L'Europe de la sécurité intérieure: une élaboration par étapes,* Paris : La Documentation Française.

Luif, P. and H. Riegler (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to the Western Balkan Countries", PE 348.588, European Parliament, Brussels.

Maguire, M. (2004), "The Crime Reduction Programme: Reflections on the Vision and the Reality", *Criminal Justice*, Vol. 4, No 3, pp. 213-238.

Menkiszak, M., M. Jaroszewicz and M. Falkowski (2006), "The External Dimension of the Area of Freedom, Security and Justice in Relation to Russia", PE 348.594, European Parliament, Brussels.

Mitsilegas, V. (2001), "Defining Organised Crime in the European Union: the Limits of European Criminal Law in an Area of Freedom, Security and Justice", *European Law Review*, vol.26, pp. 565-581.

Mitsilegas, V. (2009), *EU Criminal Law*, Oxford: Hart Publishing.

Mitsilegas, V. (2011), "The Council Framework Decision on the Fight against Organised Crime: What can be Done to Strengthen EU Legislation in the Field?", PE 453.195, European Parliament, Brussels.

Monar, J. (ed.) (2010), *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice,* Brussels: Peter Lang.

Müller-Wille, B. (2004), "For our eyes only? Shaping an intelligence community within the EU", *Cahiers de Chaillot Occasional Papers*, No. 50.

Neal, A. (2009), *Exceptionalism and the Politics of Counter-terrorism: Liberty, Security and the War on Terror*, London: Routledge.

Parkin, J. (2011), "The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law", CEPS, Brussels.

Peers, S. (2004), *Annotations on The "Hague Programme" final version,* Statewatch, London.

_____ (2007), "Salvation out of the Church: Judicial Protection in the Third Pillar after the *Pupino* and *Segi* judgements", *Common Market Law Review*, Vol. 44, pp. 883-929.

_____ (2008), "Key Legislative Developments on Migration in the European Union", *European Journal of Migration and Law*, Vol. 10, pp. 77-104.

Ramboll-Euréval-Matrix (2009), *Evaluation of the EU decentralised agencies in 2009 – Final Report Volume III: Agency level findings*, Brussels.

Reding, V. (2010) Opening remarks at the European Parliament Hearing in the Committee on Civil Liberties, Justice an d Home Affairs (LIBE), European Parliament Hearing, 11 January 2010.

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4, 28.12.2006.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L218/60, 13.8.2008.

Rijken, C. (2006), "Lessons learnt from the first efforts to establish a JIT", *Utrecht Law Review*, Vol. 2, Issue 2, (www.utrechtlawreview.org/).

Scherrer, A., A. Mégie and V. Mitsilegas (2009), "The EU role in fighting transnational organised crime", PE 410.678, European Parliament, Brussels.

Scott Marcus, J. et al. (2011), "The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally", PE464.432, European Parliament, Brussels.

Surveillance Studies Network (2006), *A Report on the Surveillance Society*, London, Report for the Information Commissioner, September.

United Nations World Tourism Organisation (2011), *UNWTO Tourism Highlights*, Madrid: UNWTO.

Van Buuren, J. (2009), *Secret Truth: The EU Joint Situation Centre*, Eurowatch, Amsterdam.

Van Duyne, P. and T. Vander Beken (2009), "The incantations of the EU organised crime policy making*", Crime, Law and Social Change*, Vol. 51, No 2, pp. 261-281.

Wacquant, L. (2007), *Urban Outcasts: A Comparative Sociology of Advanced Marginality*, Cambridge: Polity Press.

Wills, A. et al. (2011), "Parliamentary Oversight of Security and Intelligence Agencies in the EU", PE 453.207, European Parliament, Brussels.

ANNEX

CONTENT:

FIGURES:

FIGURE 1: THE EU POLICY CYCLE IN INTERNAL SECURITY AS FORESEEN BY THE HARMONY PROJECT 133

FIGURE 2: TOTAL RECORDS ON PERSONS AND TOTAL RECORDS ON UNWANTED ALIENS IN THE SIS DATABASE, WITH ARTICLE 96 RECORDS COMPONENT (2004-2010) 134

FIGURE 3: TOTAL VISA APPLICATIONS (CATEGORIES A, B, C) TO SCHENGEN AND NON-SCHENGEN STATES, 2005-2009 134

FIGURE 4: TOTAL VISAS ISSUED (CATEGORIES A, B, C, VTL, D, D+C) BY SCHENGEN AND NON-SCHENGEN STATES, 2005-2009 135

FIGURE 5: PRE-LISBON TREATY INSTITUTIONAL AND EFFECTIVE RELATIONS BETWEEN EU AGENCIES, BODIES AND SERVICES IN CHARGE OF INTERNAL SECURITY 136

TABLES:

TABLE 1: CHANGES TO COUNCIL JHA STRUCTURES AFTER LISBON 138

TABLE 2: OVERVIEW OF COUNCIL PREPARATORY BODIES IN JHA MATTERS (E. BODIES) 140

TABLE 3: COSI INITIAL 12-MONTH WORK PROGRAMME AND CURRENT 18-MONTH WORK PROGRAMME 141

TABLE 4: SUMMARY OF FORMAL BILATERAL RELATIONS BETWEEN EU “JHA AGENCIES” (2011) 141

TABLE 5: CATEGORIES OF INFORMATION INCLUDED UNDER ARTICLE 2 THE EUROPOL/FRONTEX STRATEGIC AGREEMENT OF MARCH 2008 (NON LIMITATIVE) 142

TABLE 6: LIST OF CRIMINAL OFFENCES FALLING WITHIN THE SCOPE OF THE STRATEGIC AGREEMENT BETWEEN EUROPOL AND FRONTEX (AS OF MARCH 2008) 142

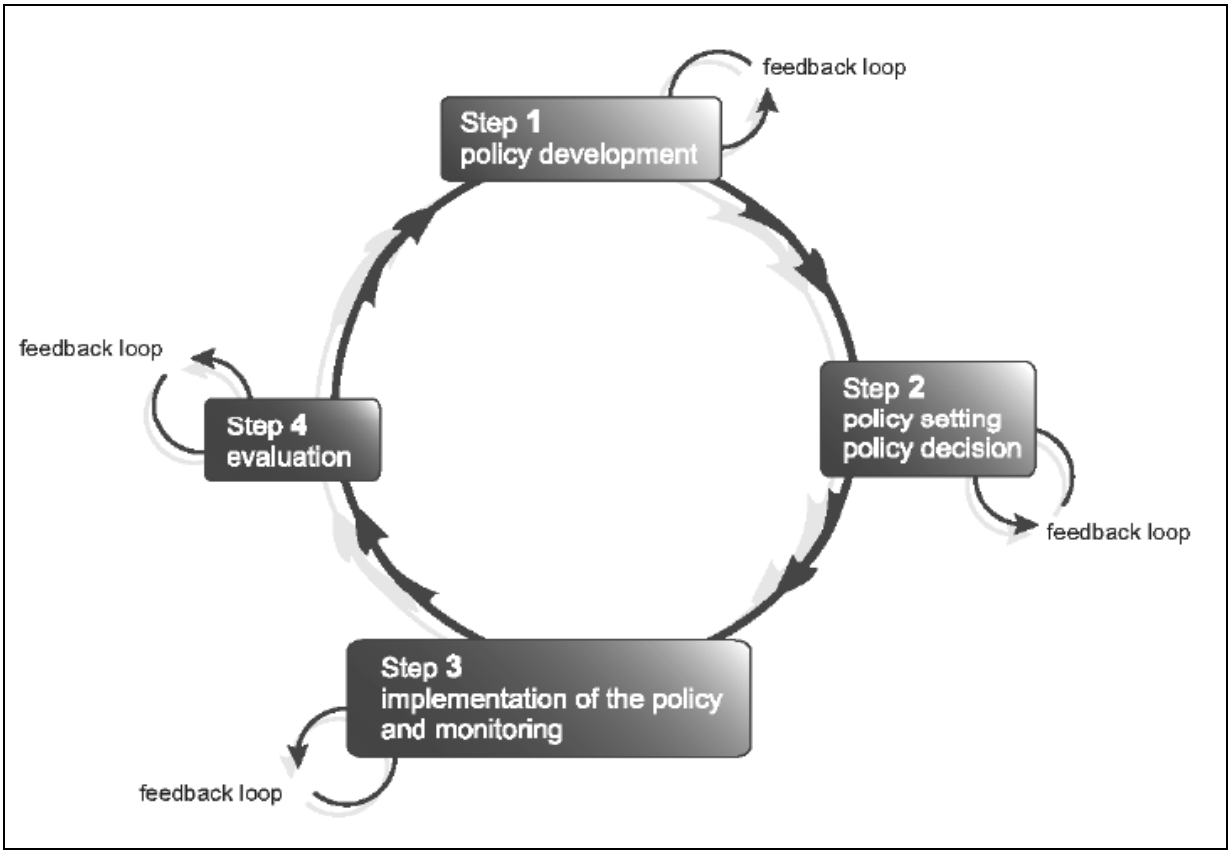
TABLE 7: THE SHIFT TOWARDS MASS DATA PROCESSING: COMPARING ESTIMATES OF THE NUMBER OF RECORDS ON PERSONS IN SIS, VIS, EES AND EU-PNR 143

METHODOLOGICAL NOTE ON TIMELINE 146

LIST OF INTERVIEWS 147

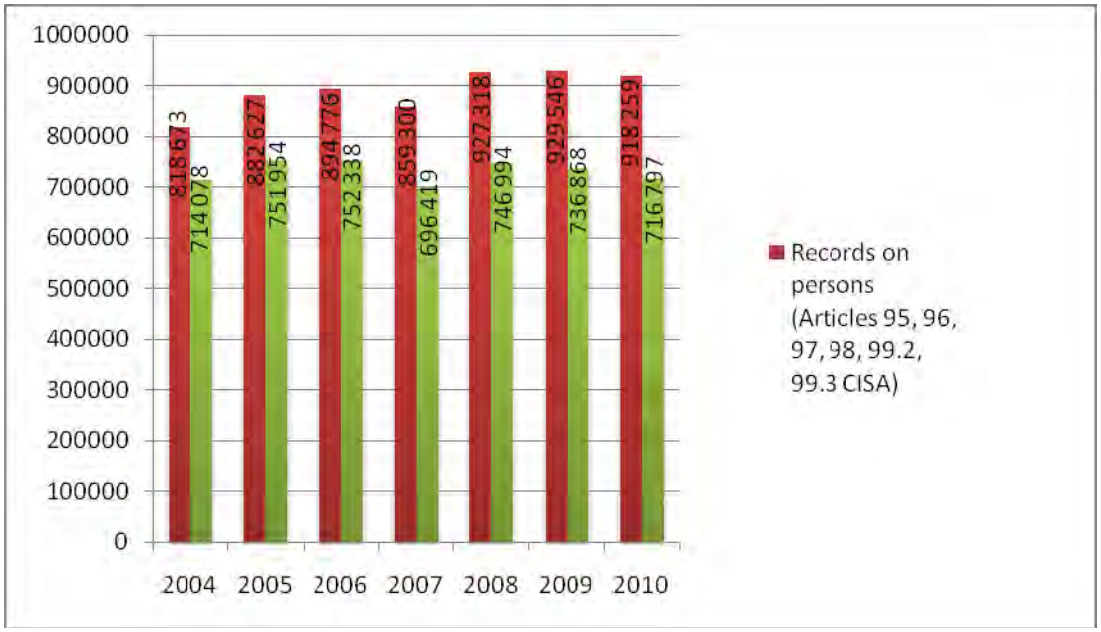
Figures

Figure 1: The EU policy cycle in internal security as foreseen by the Harmony project



Source: Council document 14581/10, p. 16.

Figure 2: Total records on persons and total records on unwanted aliens in the SIS database, with Article 96 records component (2004-2010)



Source: Council documents 8621/05, 5239/06, 6178/07, 5441/08, 5764/09 and 6434/2/11 Rev.2.

Figure 3: Total visa applications (categories A, B, C) to Schengen and non-Schengen states, 2005-2009

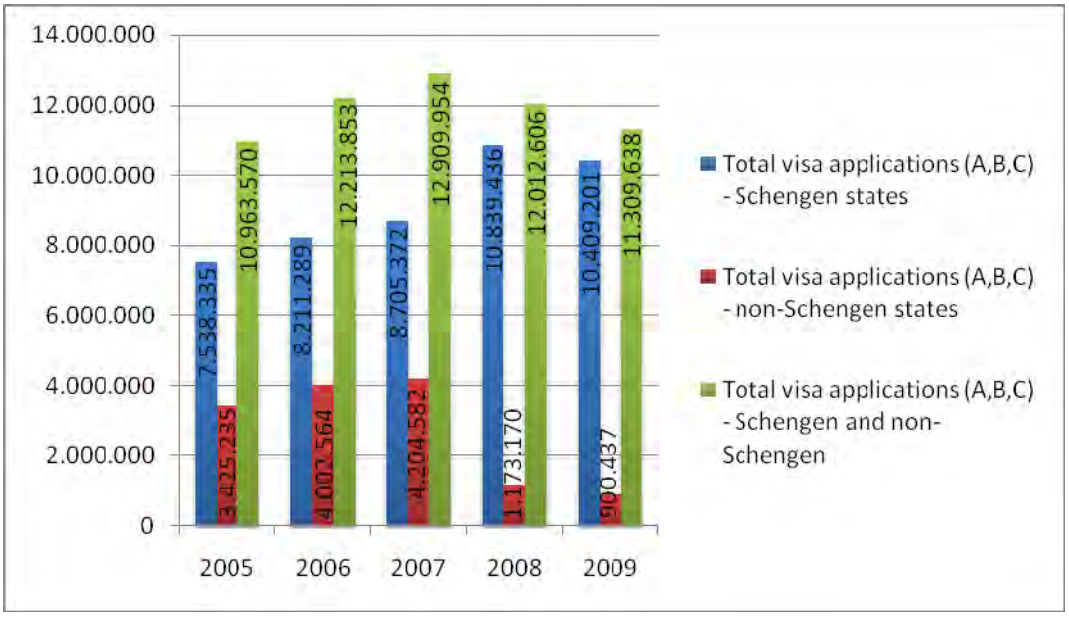


Figure 4: Total visas issued (categories A, B, C, VTL, D, D+C) by Schengen and non-Schengen states, 2005-2009

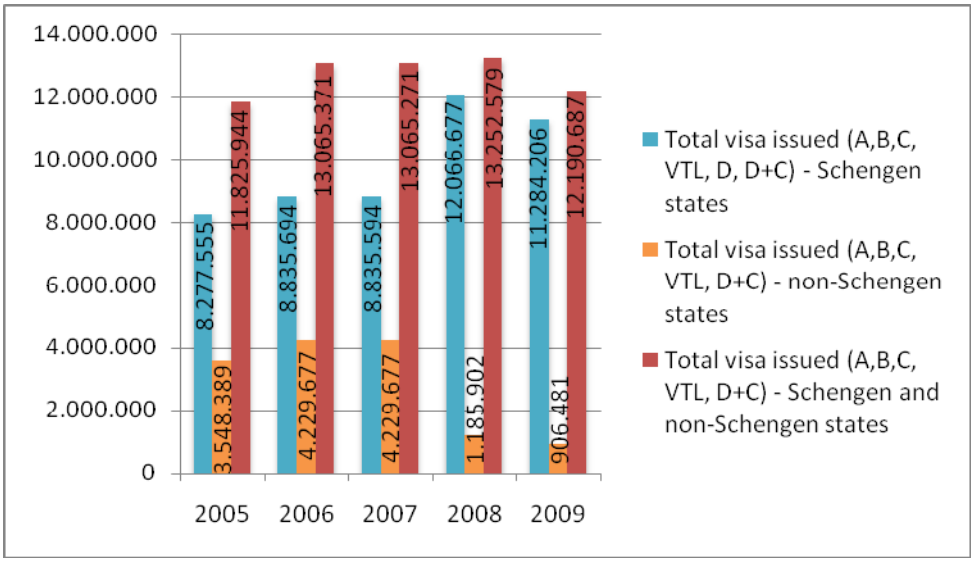
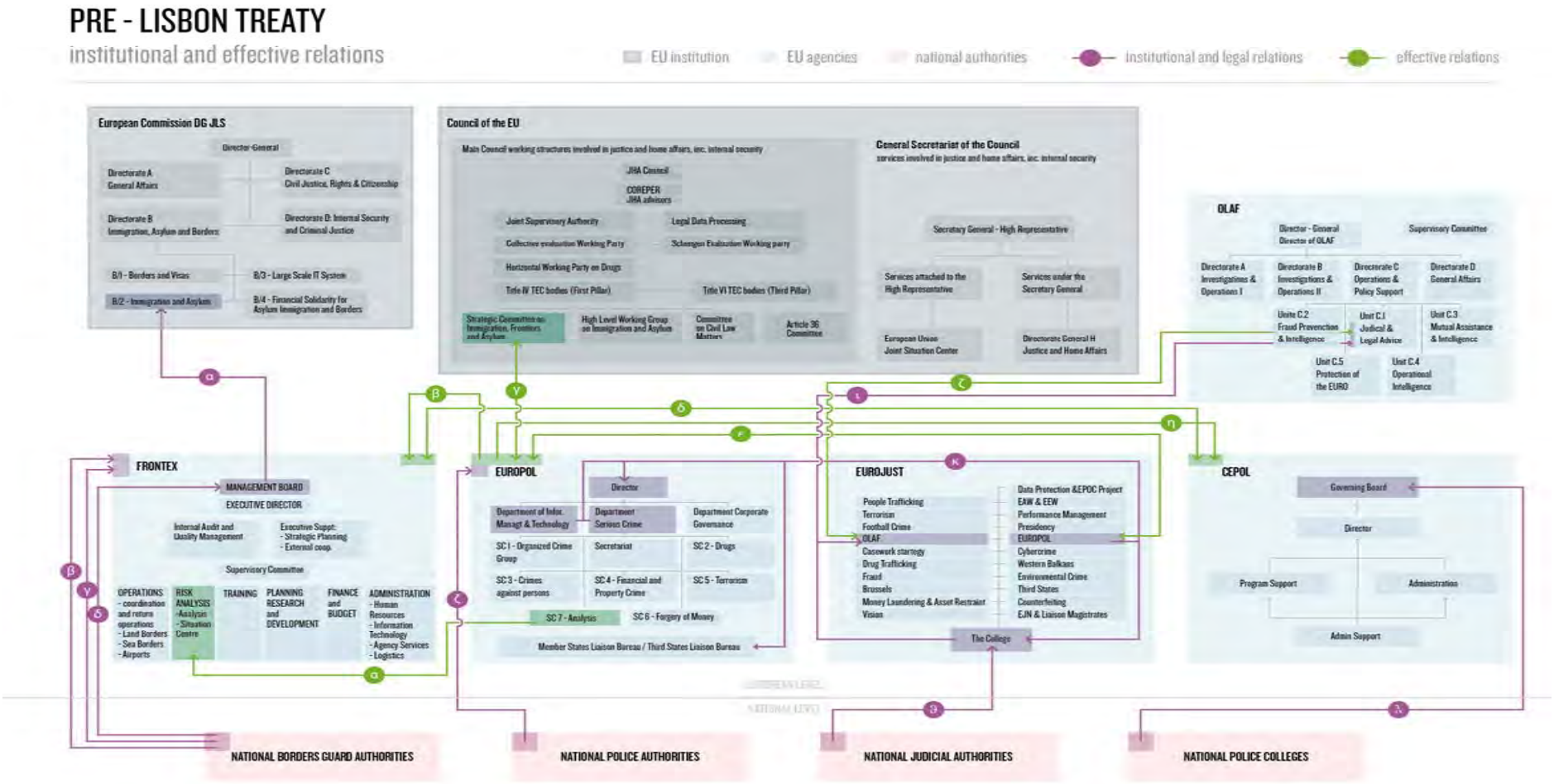


Figure 5: Pre-Lisbon treaty institutional and effective relations between EU agencies, bodies and services in charge of internal security




PRE - LISBON TREATY
labels
α
FRONTEX > EUROPEAN COMMISSION
Council Regulation (EC) No 2007/2004 establishing a European agency for the management of operational cooperation at the external borders of the Member States of the European Union (Article 20)
β
NATIONAL BORDER GUARD AUTHORITIES > FRONTEX
Council Regulation (EC) No 2007/2004 on the provision of operational coordination, support for joint return operations, provision of training ;
Regulation (EC) No 863/2007 (RABITs)
γ
NATIONAL BORDER GUARD AUTHORITIES > FRONTEX
FRONTEX Management Board Decision of 21.9.2006 Laying Down Rules on the Secondment of National Experts (SNE's) to the Agency
δ
NATIONAL BORDER GUARD AUTHORITIES > FRONTEX, MANAGEMENT BOARD
Council Regulation (EC) 2007/2004 on Appointment of FRONTEX board members (Article 21)
ζ
NATIONAL POLICE AUTHORITIES > EUROPOL
Council Decision of 6 April 2009 establishing the European Police Office (2009/371/JHA)
θ
NATIONAL JUDICIAL AUTHORITIES > EUROJUST, THE COLLEGE
Institutional Relation
ι
EUROJUST, THE COLLEGE > OLAF, UNIT C.1
Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, esp. Art. 26(3) and (4), MoU between EUROJUST and OLAF (14.4.2003)
κ
EUROJUST / EUROPOL RELATIONS
Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime;
λ
NATIONAL POLICE COLLEGES > CEPOL
Relation with CEPOL Governing Board
α
EUROPOL > FRONTEX
Contribution to Risk Analyses & Exchange of Information
β
EUROPOL > FRONTEX
Strategic Agreement (entered into force 20.3.2008)
η
EUROPOL > CEPOL
Strategic Agreement (entered into force 1.6.2007)
...
REMAINING RELATIONS
Exchange of Information

Tables

Table 1: Changes to Council JHA Structures After Lisbon

(B = General Affairs preparatory bodies; C = External Relations/Security and Defence/Development preparatory bodies: E = JHA preparatory bodies)

Designation (Pre-Lisbon)	Name	Status
E.0	CATS (Article 36 Committtee)	Meetings will continue until 1 January 2012. Will focus on strategic issues where COSI would not be able to contribute and meet as necessary by convening of the Presidency (Doc. 16070/09 and 16072/09)
E.1	Strategic Committee on Immigration, Frontiers and Asylum (SCIFA)	Same as CATS
E.2	Working Party on Migration and Expulsion	Renamed as Working Party on Integration, Migration and Expulsion. The WP will meet in different formations depending on the agenda
E.3	Visa Working Party	Continues
E.4	Asylum Working Party	Continues
E.5	CIREFI	Abolished. CIREFI and its functions are transferred to FRONTEX, which shall report to the Council on statistical matters previously conferred on CIREFI
E.6	Working Party on Frontiers	Continues. Will be called on discussing issues dealt with in CIREFI previously
E.7	Working Party on Civil Law Matters	Continues
E.8	SIS/SIRENE Working Party	Merged with E.17 and E.18 in E.27 Working Party for Schengen Matters
E.9	SIS TECH Working Party	Same as E.8
E.10	Police Cooperation Working Party	Merged in E.26 Law Enforcement Working Party
E.11	Europol Working Party	Same as E.10
E.12	Working Party on Terrorism	Continues. Will meet with C.19 (COTER) when dealing with horizontal/cross-cutting issues
E.13	Customs Cooperation Working Party	Continues
E.14	Working Party on Cooperation in Criminal Matters	Continues
E.15	Working Party on Substantive Criminal Law	Continues
E.16	Working Party on Collective Evaluation	Discontinued
E.17	Working Party on Schengen Evaluation	Merged in E.27 Working Party for Schengen Matters together with E.8 SIS/SIRENE Working Party and SIS-TECH Working Party

E.18	Working Party on the Schengen Acquis	Merged in E.27 Working Party for Schengen Matters together with E.8 SIS/SIRENE Working Party and SIS-TECH Working Party
E.19	Multidisciplinary Group on Organised Crime	Becomes E.28 Working Party on General Matters including Evaluation. Deals with matters relating to organised crime and prevention, excluding terrorism, that are not covered by COSI or other working parties and all evaluation mechanisms that will be set up under Article 70 TFEY except Schengen evaluation (which are dealt with in E.27 WP for Schengen Matters)
E.20		No longer exist (abolished with Council Decision setting up the European Judicial Network)
E.21	Working Party on Civil Protection	Continues
E.22	Ad Hoc Working Party on Fundamental Rights and Citizenship	Renamed as Working Party on Fundamental Rights, Citizens Rights and Free Movement of Persons, made permanent and tasked with all matters related to FR and citizens rights. Remit includes follow-up to accession of the Union to ECHR, follow-up of reports from the EU-FRA
E.23	Ad Hoc Group on Information Exchange	Renamed Working Party on Information Exchange and Data Protection, made permanent. Merged with G.9 Working Party on Data Protection (Art.29 WP)
E.24	JAI-RELEX Ad Hoc Support Group	Made permanent and renamed JAI-RELEX Working Party
B.3	High-Level Working Group on Asylum and Migration	Continues
B.4	Horizontal Working Party on Drugs	Continues
B.10	Working Party on Legal Data Processing (E-justice and E-law)	Renamed as Working Party on E-Law with mandate to implement the action plan on e-justice. Legal data processing issues should be transferred to the European Commission and include discussions on integrated system for access to Community and Union Law and CELEX
C.19	COTER	Continues
C.38	Working Party on the application of specific measures to combat terrorism (CP 931 WP, see Doc. 10826/1/07)	Continues

Source: Council documents 17653/09 and 5688/1/11

Table 2: Overview of Council preparatory bodies in JHA matters (E. bodies)

Designation (Pre-Lisbon)	Name
E.1	Strategic Committee on Immigration, Frontiers and Asylum (SCIFA)
E.2	Working Party on Integration, Migration and Expulsion
E.3	Visa Working Party
E.4	Asylum Working Party
E.5	*CIREFI - Discontinued*
E.6	Working Party on Frontiers
E.7	Working Party on Civil Law Matters
E.8	*SIS/SIRENE Working Party - Merged with E.9, E.17 and E.18 in E.27*
E.9	*SIS-TECH Working Party - Merged with E.8, E.17 and E.18 in E.27*
E.10	*Police Cooperation Working Party - Discontinued, tasks transferred to E.26*
E.11	*Europol Working Party - Discontinued, tasks transferred to E.26*
E.12	Working Party on Terrorism
E.13	Customs Cooperation Working Party
E.14	Working Party on Cooperation in Criminal Matters
E.15	Working Party on Substantive Criminal Law
E.16	*Working Party on Collective Evaluation - Discontinued, evaluation transferred to E.28*
E.17	*Working Party on Schengen Evaluation - Merged with E.8, E.9 and E.18 in E.27*
E.18	*Working Party on the Schengen Acquis - Merged with E.8, E.9 and E.17 in E.27*
E.19	*Multidisciplinary Group on Organised Crime - Merged in E.28*
E.20	*Abolished*
E.21	Working Party on Civil Protection
E.22	Working Party on Fundamental Rights, Citizens' Rights and Free Movement of Persons
E.23	Working Group on Information Exchange and Data Protection
E.24	JAI-RELEX Working Party
E.25	CATS
E.26	Law Enforcement Working Party (formerly E.10 and E.11)
E.27	Working Party for Schengen matters (formerly E.8, E.9, E.17 and E.18)
E.28	Working Party on General Matters including Evaluation (formerly E.16 and E.19)

Source: Council Document 5688/1/11.

Table 3: COSI initial 12-month work programme and current 18-month work programme

2010-2011 12-month work programme (Council Document 13871/10)	2011-2012 18-month work programme (Council Document 12363/11)
EU Policy Cycle (Harmony Project)	Implementation of EU Policy Cycle
Internal Security Strategy	Monitoring support and coordination of the development and implementation of the Internal Security Strategy, consistent with the EU Policy Cycle
Cooperation to address organised crime	Interaction between external and internal EU security (PSC/COSI)
COSPOL Projects (results, organisation, subjects)	Co-odination mechanism for joint operations
European Pact to combat international drug trafficking	Co-ordination between EU JHA Agencies
Coordination mechanisms for joint operations	Reinforcing the protection of external borders and combating illegal migration
Fight against arms trafficking	European Pact to Combat International Drug Trafficking
Action Papers on PKK	European Pact on Synthetic Drugs
Financing of operational cooperation/Internal Security Fund	Fight against arms trafficking
Coordination between agencies	Solidarity clause
Reinforcing the protection of external borders and combating illegal immigration	
Solidarity clause	
Interaction between internal and external security	
Conclusions of the 1st Heads of NCBs Conference	

Table 4: Summary of formal bilateral relations between EU "JHA Agencies" (2011)

	CEPOL	EUROJUST	EUROPOL	FRONTEX
CEPOL		MoU (1.1.2010)	Agreement (20.10.2007)	Cooperation agreement (25.6.2009)
EUROJUST	MoU (1.1.2010)		Revised Agreement (1.10.2009)	Negotiations under way, formal agreement expected in 2011
EUROPOL	Agreement (20.10.2007)	Revised agreement (1.10.2009)		Agreement (29.3.2008) and Cooperation Plan (1.10.2009)
FRONTEX	Cooperation agreement (25.6.2009)	Negotiations under way, formal agreement expected in 2011	Agreement (29.3.2008) and Cooperation Plan (1.10.2009)	

Source: Council documents 5816/10 (p. 3), 5675/11, 5676/11.

Table 5: Categories of information included under Article 2 the EUROPOL/FRONTEX Strategic Agreement of March 2008 (non limitative)

"Strategic information"	"Technical Information"
Enforcement actions that might be useful to suppress offences and improve the integrated border management of the Member States of the European Union	Means of strengthening administrative and enforcement structures in the fields covered by this agreement
New methods used in committing offences, in particular those threatening the security of external borders or facilitating illegal immigration	Police working methods as well as investigative procedures and results
Trends and developments in the methods used to commit offences	Methods of training the officials concerned
Observations and findings resulting from the successful application of new enforcement aids and techniques	Criminal intelligence analytical methods
Routes and changes in routes used by smugglers, illegal immigrants or those involved in illicit trafficking offences covered by this agreement	Identification of law enforcement expertise
Prevention strategies and methods for management to select law enforcement priorities	
Threat assessments, risk analysis and crime situation reports	

Table 6: List of criminal offences falling within the scope of the Strategic Agreement between EUROPOL and FRONTEX (as of March 2008)

Annex 1 list of criminal offences – EUROPOL/FRONTEX Strategic agreement 2008	
"Unlawful drug trafficking" offences - criminal offences listed in Article 3(1) of the United Nations Convention of 20 December 1988 against Illicit Traffic in Narcotic Drugs and Psychotropic substances, and amending and replacing acts	"Motor vehicle crimes" - the theft or misappropriation of motor vehicles, lorries, semi-trailers, the loads of lorries or semi-trailers, buses, motorcycles, caravans and agricultural vehicles, works vehicles, and the spare parts for such vehicles, and the receiving and concealing of such objects
"Crime connected with nuclear and radioactive substances" – criminal offences listed in Article 7(1) of the Convention on the Physical Protection of Nuclear Material of 3 March 1980, and relating to the nuclear and/or radioactive materials defined in Article 197 of the Euratom Treaty and Directive 80/836 Euratom of 15 July 1980	"Forgery of money and means of payment" – the acts defined by Article 3 of the Geneva Convention of 20 April 1929 on the suppression of counterfeiting currency, which applies to both cash and other means of payment
"Illegal immigrant smuggling" – activities deliberately intended to facilitate, for financial gain, the entry into, residence or employment in the territory of the Member States of the European Union, contrary to the rules and conditions applicable in the Member States	"Illegal money laundering activities" – criminal offences listed in Article 6(1) to (3) of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 8 November 1990
"Trafficking in human beings" – subjection of a person to the real and illegal sway of other persons by using violence or menaces or by abuse of authority or intrigue, especially with a view to the exploitation of prostitution, forms of sexual exploitation and assault of minors or trade in abandoned children. These forms of exploitation also include the production, sale or distribution of child-pornography material.	

Table 7: The shift towards mass data processing: comparing estimates of the number of records on persons in SIS, VIS, EES and EU-PNR

Data Processing Scheme	Estimates of number of records on persons	Categories of persons concerned
SIS (for comparison purposes)	Under 1 million yearly over the past 7 years	Chiefly third country nationals (records on the basis of Article 96 CISA)
VIS (in process of becoming operational, starting October 2011)	Around 60 million in any given 5-year period	Persons who fall under visa obligations to enter the territory of the Member States of the European Union and EU citizens or residents acting as hosts
EES (envisaged legislative proposal)	Should policy option of recording entries and exits of all third country nationals be pursued, more than 350 million (based on figures of international tourist arrivals in EU-27)	Depending on policy option, either same persons that would be registered in VIS or in addition, persons not required to obtain a Schengen visa to travel to the EU
EU-PNR (2011 Commission proposal for a European Parliament and Council Directive)	500 million records (figure provided by air carriers)	All passengers using air transportation to cross the external borders of the Member States of the EU

Methodological note on timelines

In order to provide additional information and evidence, this study relies on visual supports. Figure 5 available in the Annex presents the institutional and effective relations between EU agencies, bodies and services in charge of internal security in the pre-Lisbon context. Four timelines presenting the evolution of European internal security policies since the 1960s can additionally be accessed online, at the following URL: http://jiminy.medialab.sciences-po.fr/deviss/timeline/. The Justice and Home Affairs Programme at the Centre for European Policy Studies (CEPS) assisted on the collection, selection and archiving of data. The methodology followed by CEPS for the collection of this data foresaw a specific timeline (between 1999 and 2011) and focused on the assessment and selection of all available documents on the websites of the JHA agencies and bodies demonstrating the evolution and framing of threats in the areas of organized crime, terrorism and border control. It focused as well on the agencies, actors and networks in the JHA policy sphere (giving special attention to SitCen, Frontex, Europol, COSI, Eurojust, CEPOL, the CTC and ENISA).

The “timeline on European security” visualisation maps the history of European cooperation and policies in the field of internal security. Based on available historiographies, it distinguishes between four processes: the history of informal clubs and working group structures (particularly in the field of police and judicial cooperation) , the history of Community related developments in internal security, the history of the establishment and roll-out of systems for the exchange and processing of information, and the history of international agreements with third countries in the area of internal security.
The visualisation presents these four processes in a time-oriented matrix. Each column represents a time period of a year, from 1967 to 2011, and each row the events that occurred across all four processes for a given year. Events pertaining to the same process are grouped together, and organised by order of occurrence.
In order to improve readability, grouped rows are coloured according to their belonging topic and connected by a light coloured line: 'Police Cooperation', 'Community developments', 'databases and information network' and 'external dimension'.

List of Interviews

Baines, Victoria, Strategic Analyst, EUROPOL, May 2011

Banfi, Ferenc, Director, CEPOL, June 2011

Collon, Michael, Clerk, EU Sub-Committee F - Home Affairs, House of Lords, March 2011

Coninsx, Michèle, Vice President, EUROJUST, May 2011

Cuadrat-Grzybowska, Katarzyna, Legal Advisor, European Data Protection Supervisor, July 2011

Ellerman, Jan, Data Protection Officer, EUROPOL, May 2011

Hijsmans, Hielke, Head of Unit, Policy and Consultations, European Data Protection Supervisor, July 2011

Jancewicz, Tatiana, Senior Legal Officer, EUROJUST, May 2011

Nogala, Detlef, Research and Knowledge Management Officer, CEPOL, June 2011

Shapcott, William, Director, DG A, Council of the European Union, former director of SitCen, May 2011

Torrance, Michael, EU Policy Analyst, House of Lords, March 2011

Van Renterghem, Pierre, Business demand & products - Capabilities Department, EUROPOL, May 2011

Verhaag, Alinde, Head of Case Management, EUROJUST, May 2011

Wainwright, Rob, Director, EUROPOL, May 2011

Wewer, Gregor, Governance Department, EUROPOL, May 2011

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

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

Policy Areas

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

Documents

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

ISBN