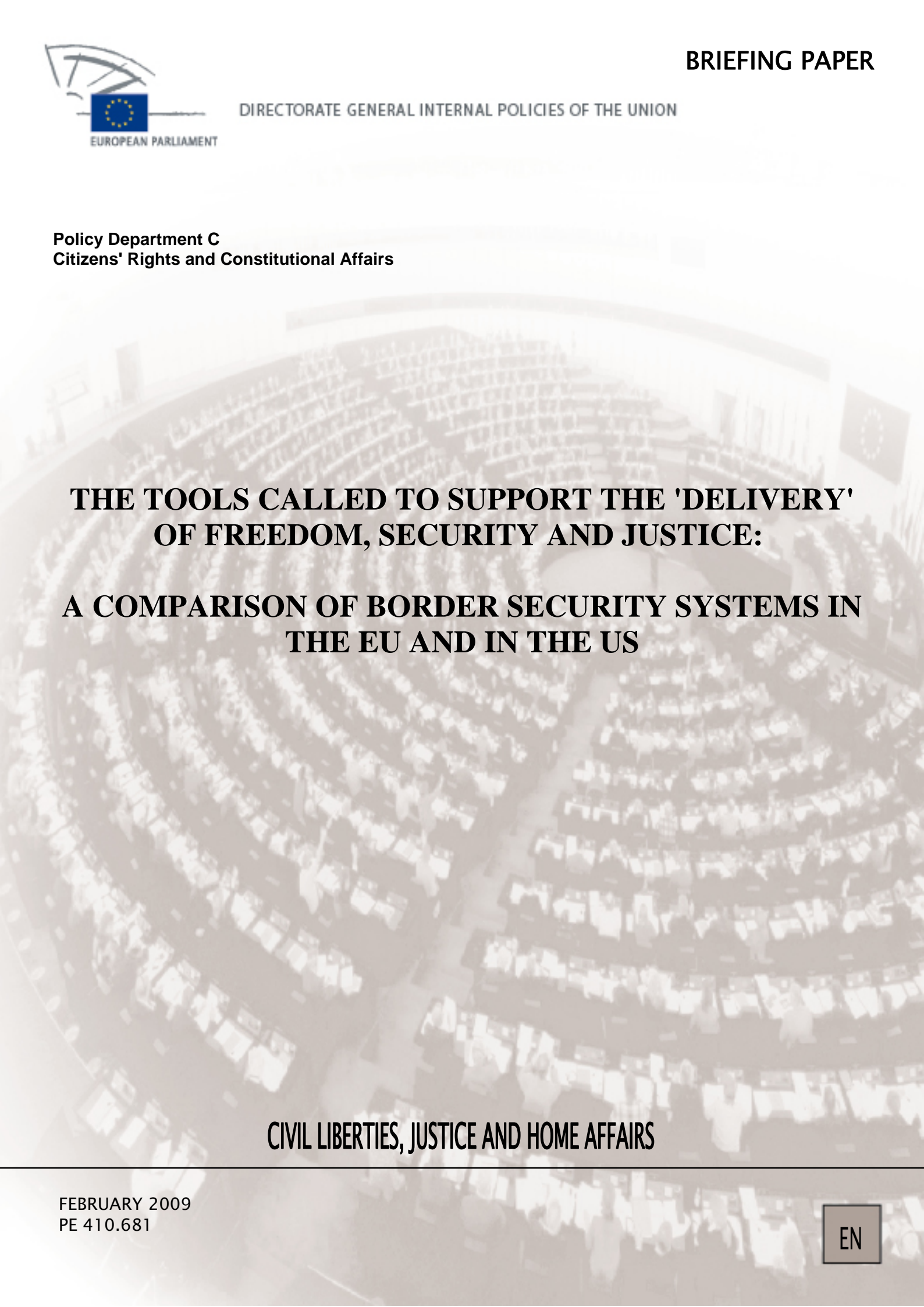


Policy Department C  
Citizens' Rights and Constitutional Affairs



**THE TOOLS CALLED TO SUPPORT THE 'DELIVERY'  
OF FREEDOM, SECURITY AND JUSTICE:  
A COMPARISON OF BORDER SECURITY SYSTEMS IN  
THE EU AND IN THE US**

**CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS**





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

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

## **THE TOOLS CALLED TO SUPPORT THE 'DELIVERY' OF FREEDOM, SECURITY AND JUSTICE:**

### **A COMPARISON OF BORDER SECURITY SYSTEMS IN THE EU AND IN THE US**

#### **AD HOC BRIEFING PAPER**

**Abstract:**

While the European Union is about to take far-reaching decisions on the best way to ensure the security of its external border, there is a strong tendency to take guidance from the United States, the world's undisputed forerunner in employing advanced technology and strict control procedures. Besides highlighting the weaknesses of the current EU approach against the background of the almost accomplished US system, the briefing undertakes to analyse to what extent exclusive transatlantic inspiration is the right way to follow for European policy-makers. It carefully examines US experience gained since the late 1990s in setting up a watertight entry-exit system, in particular the reasons why, despite all efforts made and resources spent, the project did not yet yield a completely satisfactory outcome. It also argues that even such advanced models can never be considered "one size fit all"-solutions, transferable to other regions with paying attention to their political, geographic and other specificities – and, above all, one should not overestimate technology as a problem-solver. Besides taking inspiration from outside, the European Union should also consider alternative mechanisms adapted to the domestic situation such as controls carried out inside the territory.

**PE 410.681**

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

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

Authors: **Dr Peter Hobbing, CEPS, Brussels**  
**Professor Dr Rey Koslowski, Transatlantic Academy, Washington D.C.**  
**and University at Albany, State University at New York (SUNY)<sup>1</sup>.**

*Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS)*

Manuscript completed in February 2009

Copies can be obtained through:

Dr. Joanna Apap

Tel: +32 2 2832105

Fax: +32 2 2832365

E-mail: [joanna.apap@europarl.europa.eu](mailto:joanna.apap@europarl.europa.eu)

Informations on DG Ipol publications:

<http://www.europarl.europa.eu/activities/committees/studies.do>

Brussels, European Parliament

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

---

<sup>1</sup> Acknowledgements: Rey Koslowski thanks the Transatlantic Academy as well as the Migration Policy Institute, the Woodrow Wilson International Center for Scholars and the MacArthur Foundation for research support that contributed to this paper

# THE TOOLS CALLED TO SUPPORT THE 'DELIVERY' OF FREEDOM, SECURITY AND JUSTICE:

## A COMPARISON OF BORDER SECURITY SYSTEMS IN THE EU AND IN THE US

### Contents

<b>1. Introduction .....</b>	<b>4</b>
<b>2. Status quo: a snapshot of the current transatlantic divide in border security .....</b>	<b>4</b>
<b>2.1 Fragmentary coverage of cross-border flows in the EU .....</b>	<b>5</b>
<b>2.1.1 EU concept of Integrated Border Management .....</b>	<b>6</b>
<b>2.1.2 The Schengen Information System II (SIS II).....</b>	<b>8</b>
<b>2.1.3 The Visa Information System (VIS).....</b>	<b>9</b>
<b>2.1.4 Eurodac .....</b>	<b>11</b>
<b>2.1.5 FRONTEX and its involvement in operative action.....</b>	<b>12</b>
<b>2.1.6. “Second-line” controls within the territory .....</b>	<b>14</b>
<b>2.1.7 Missing links.....</b>	<b>14</b>
<b>2.1.7.1 The EU-PNR system still not in place .....</b>	<b>15</b>
<b>2.1.7.2 ETA/ESTA scheme .....</b>	<b>15</b>
<b>2.2 US Border Security Systems: More but Incomplete.....</b>	<b>16</b>
<b>2.2.1 Entry-Exit: US-VISIT and supporting mechanisms.....</b>	<b>16</b>
<b>2.2.2 Secure Border Initiative (SBI) - Coverage of green/blue borders.....</b>	<b>22</b>
<b>2.2.3 Visa Waiver Program Reform and ESTA .....</b>	<b>25</b>
<b>3. Convergence ahead? Tendencies of transatlantic approximation .....</b>	<b>26</b>
<b>3.1 Closing the gap: The EU’s vision of an integrated border management in the 21st century .....</b>	<b>26</b>
<b>3.1.1 The Future Group’s report of 30 June 2008.....</b>	<b>27</b>
<b>3.1.2 The Commission border package of February 2008.....</b>	<b>29</b>
<b>3.1.2.1 The next steps in border management.....</b>	<b>29</b>
<b>(1) Facilitation for “bona fide” travelers.....</b>	<b>30</b>
<b>(2) Entry/exit system .....</b>	<b>31</b>
<b>(3) Electronic System of Travel Authorisation (ESTA) .....</b>	<b>32</b>
<b>3.1.2.2 Future development of FRONTEX.....</b>	<b>32</b>
<b>3.1.2.3 European Border Surveillance System EUROSUR .....</b>	<b>32</b>
<b>3.1.2.4 European PNR System on the use of air passenger data (PNR) for law enforcement purposes .....</b>	<b>33</b>
<b>3.2 US strategies to counter remaining weaknesses/loopholes.....</b>	<b>34</b>
<b>3.2.1. Western Hemisphere Travel Initiative (WHTI) .....</b>	<b>34</b>
<b>3.2.2. Building border crossing infrastructure .....</b>	<b>35</b>
<b>3.2.3. Radio Frequency Identification (RFID) .....</b>	<b>36</b>
<b>3.2.4 Requiring airlines to collect biometric exit data.....</b>	<b>38</b>
<b>4. Conclusions .....</b>	<b>39</b>
<b>5. Recommendations .....</b>	<b>40</b>
<b>Annex “EU/US systems of border security: table of correspondence”.....</b>	<b>42</b>
<b>Bibliography .....</b>	<b>43</b>
<b>Legislation .....</b>	<b>49</b>
<b>Abbreviations.....</b>	<b>50</b>

## 1. INTRODUCTION

Recent transatlantic clashes over vital issues of external and internal security have undermined the faith in finding easy solutions satisfying the needs and convictions of both parties. Be it the question of going to war or not on Iraq, Afghanistan or even Iran, the way of tackling terrorism while respecting rights of travellers, bank customers or citizens in general, each time surprisingly different preferences/sensitivities surface on both sides of the Atlantic. Although there is mostly agreement on the problem as such as well as the necessity of tackling it **jointly**, the proposed solutions are quite likely meet with the opposition of one party.

Tackling international terrorists with military or police power, protecting the homeland against the risk of violent attacks with due respect for civil liberties or considering this sensitive area exempt from the strict application of such „old-fashioned“ notions, these are some of the dividing lines between the two continents. The division extends to basic control strategies whether these are confined to the moment of entering the homeland or include both border checks and internal controls via ID cards and checks on the labour market<sup>1</sup> And even where the mutual acceptance of concepts appears attractive to policy-makers, this may be in contradiction with the historic or geographical realities.

If the European Parliament has decided to commit such comparative study, this has also to be seen in the light of yet another turn in EU-US security relations, i.e. the current change of direction undertaken by Brussels to more or less directly align with major US border-related policies. When consulting the options sketched out by the Commission in its “border package” of February 2008 as well as the Future Group report of June 2008, one feels shifted into a genuinely US environment characterised by concepts/tools such as “ESTA” (Electronic System of Travel Authorisation), “Entry/Exit System”, “Automated border checks” which have so far not been part of the EU border vocabulary. Even associations of the “virtual fence”, as employed with mixed success at the US – Mexican border, may be evoked by the newly developed concept of a „European Border Surveillance System – EUROSUR“ based on surveillance tools and sensors such as „satellites, unmanned aerial vehicles etc“ recommended for difficult stretches of the external border. On top of this, the creation of an „Euro-Atlantic area of cooperation in the field of Freedom, Security and Justice“ as considered by the Future Group would mean another surprising move forward.

In view of this rather confusing situation of foreignness and yet proximity, it is obviously wise to once again explore the current state of border approaches and determine how they relate to their respective bases in terms of legal and factual foundations. This includes issues of legal acceptability as well as practical feasibility, especially in the sense that formulas without a due promise of factual efficiency would in any case fail the test.

Even if the transatlantic divide implies that things are sometimes incomparable or incompatible, one may draw at least certain conclusion out of the study: if things don’t work in the US even under the much favourable conditions, how can they be successful in Europe under much less favourable conditions

The main part of the paper is divided in three sections: we will (2) examine the current state of border security on the basis of the achievements and problems emerged on both sides, then (3) highlight the progress envisaged under an increasingly converging agenda, and finally (4) evaluate to what extent the planned efforts appear effective and appropriate in view of the perfect degree of security targeted for.

## 2. STATUS QUO: A SNAPSHOT OF THE CURRENT TRANSATLANTIC DIVIDE IN BORDER SECURITY

Individual findings strongly confirm the large gap between the situations on both sides.

---

<sup>1</sup> For a detailed description of the “transatlantic divide” regarding ID cards and internal controls, see Hobbing (2008), p. 25f

While the US based on its established status of a sovereign nation state and a set of fixed and clear borders (Meyers/Koslowski/Ginsburg 2007, p.5) has been able to adapt its concepts rather rapidly to changing global challenges including those of post-9/11, the EU still finds itself hampered by institutional inconsistencies when trying to react to such situations.

It is true that also the US had to struggle with administrative landslides when performing the fusion of various border-related agencies into the new Bureau of Customs and Border Protection (CBP) under the auspices of DHS, equally a newcomer within the established family of US departments. Yet difficulties were relatively minor in comparison to the EU scenario marked by seemingly “limitless political, legal and bureaucratic nuances of institutions, rules, national cultures and, not least, reigning personalities” (Meyers/Koslowski/Ginsburg, *ibid*).

It is no surprise that clashes occurred in the often feverish attempt to translate transatlantic solidarity into concrete action. In contradiction with (and partially unaware of) actual EU competencies, the US side launched new initiatives such as the Container Security Initiative (CSI) and Passenger Name Record (PNR) submission requirements by solely involving individual Member States capitals. What had appeared practical/pragmatic at first sight, produced each time a complete deadlock of negotiations which could be resolved only by the due involvement of Brussels and extension of the initiative to include the Union as such.

If, from this point on the lesson of competencies seemed understood, this did not impede the US in early 2008, to again propose negotiations on combined visa waiver/airline security issues to selected capitals only: however, instead of a misunderstanding this represented a well-calculated move taking advantage of blurred competence situations as well as frustrated governments willing to take the risk of a major quarrel with Brussels as they blamed their continued exclusion from the Visa Waiver Program (VWP) on irresolute negotiation strategies by the institutions.

Another European disadvantage lies in geography: instead of just two long-standing neighbours, the enlarging EU had to adapt to rapidly changing sets of new neighbours along its eastern confines and there is no end in sight. Currently there are nine neighbours, each exposed to specific migratory pressure along established transit routes from CIS and Asia (IOM 2008). The same is true for a large part of the southern maritime borders which equally experience dramatic migration flows from Africa. Should Turkey as a longstanding accession candidate become EU member, the external border would considerably expand in length, involve fourteen neighbours and adjoin to international hotspots such as Iraq, Iran and the Caucasus region (Hobbing, 2003). According to assumptions by the UK House of Lords (2008: s.11) „the migratory pressure on Europe’s borders will grow because there are a growing number of failed states where a combination of economic incompetence, uncertainty of property rights, corruption, internal conflicts, political anarchy and repressive regimes has created intolerable conditions for the local population.“

## **2.1 Fragmentary coverage of cross-border flows in the EU**

In contrast to the rather uniform concepts available in the US in terms of security philosophy, organisational and equipment structures, Europe still presents a scattered image of individual state and administrative traditions. Neither do the treaties foresee any harmonisation of public administration in the Member States, nor does Brussels possess means to enforce its own legislation, apart from very narrow exceptions such as competition law. Moreover border security with its strong ties to sovereignty and criminal justice<sup>2</sup> remains a difficult terrain for implementing supranational concepts (Carrera 2007; UK HoL 2008, s.9). Thus, despite a far-reaching EU influence on the rules governing its borderless internal area and the crossing the external border, the actual handling of border matters remains a prerogative of the Member States.

---

<sup>2</sup> for a very detailed and convincing plea in favour of a supranational European criminal law see U. Sieber (2009)

This situation had provoked serious concern already during the post-9/11 overhaul of European security devices; the Laeken Summit of December 2001 criticised the increasing imbalance in bearing the financial burden of the external border. While until then, the burden had been shared rather equally between practically all Member States and in particular involving the big ones France and Germany, the gradual enlargement of the Schengen zone implied a shift towards the new - less experienced and less well-off - partners, in particular the Baltic states, Poland, Slovakia, Hungary and later Romania and Bulgaria (Hobbing 2003, p. 6). Although at that stage, time was not yet ripe for considering radical solutions such as the “European Corps of Border Guards”<sup>3</sup> which would assume the full responsibility of controlling the border and thus relocate the responsibility from national to Union level, a profound reflection started on how the burden on individual Member States could be relieved and at the same time a greater Union influence be ensured.

While formally reconfirming the principle that the “responsibility for the control and surveillance of external borders lies with the Member States”<sup>4</sup>, the institutions employed a policy of small steps to make the gradual EU involvement palatable to national capitals. In particular, the creation of the FRONTEX agency in 2004 represented an excellent example for such soft approach: building upon incentives rather than constraint, Member States were “encouraged” to make optional use of FRONTEX’s services. Among the services offered prevailed those of a rather technical nature (risk analysis, training, research, equipment) while any implication in operational activities remained embedded in multiple safeguards, notably the authorisation/request of the Member State(s) concerned, to avoid the impression that the EU might try to overrule national autonomy. The outcome lived up largely to expectations: Member States took advantage of the services proposed under such favourable conditions and FRONTEX acquired indeed some considerable influence on the practical realities of the border.

Also in other areas EU input remained selective and in strict compliance with the principle of subsidiarity; major measures which shaped the European border reality decisively concern (1) the set-up of a European concept of integrated border management (EU-IBM), various large-scale IT systems such as (2) the Schengen Information System (SIS and SIS2), (3) the Visa Information System (VIS), (4) Eurodac and (5) FRONTEX and its joint operations.

### 2.1.1 EU concept of Integrated Border Management

As the act of border-crossing actuates multiple state controls for security, tax, health and other purposes there is a clear coordination need to avoid that interventions block each other and frustrate the efficiency of clearance procedures. These overlapping competences include both the risk of creating crucial loopholes in the security set-up as well as wasting resources by duplication of efforts.

In recent years, concepts of integrated border management have been developed to tackle this neuralgic point in border mechanisms in the perspective of reconciling facilitation and security needs, both vital for the functioning of modern societies. In accordance with its specific needs, the EU established its own IBM concept which pays particular tribute to the incomplete state of the Union and the multitude of “competent authorities” involved at national and EU level<sup>5</sup>. As adopted by the JHA Council of 4-5 December 2006, the formula comprises the following elements<sup>6</sup>:

- (a) Border control (checks and surveillance) as defined in the Schengen Borders Code including risk analysis and crime intelligence
- (b) Detection and investigation of cross border crime in coordination with all competent law enforcement authorities

---

<sup>3</sup> as tentatively considered by the Commission in May 2002 in direct response to the questions raised by the Laeken Summit (Commission 2002, p. 12).

<sup>4</sup> as explicitly posted in Article 2(1) of the FRONTEX Regulation (EC) 2007/2004

<sup>5</sup> >> multitude .... Hobbing (2003),

<sup>6</sup> EU Council (2006), p. 27



- (c) The four-tier access control model (measures in third countries of origin or transit, cooperation with neighbouring countries, border control at the external borders, control measures within the common area of free movement, including return);
- (d) Inter-agency cooperation for border management (border guards, customs, police, national security and other relevant authorities) and international cooperation
- (e) Coordination and coherence of the activities of Member States and Institutions and other bodies of the Community and the Union.

The regulatory value of the EU IBM-concept was reinforced by the fact that it built upon established tools such as the Schengen Borders Code<sup>7</sup> (referred to under (a) above) with its detailed description of control measures to be conducted at the borders as well as the 2002 Schengen Catalogue and its four-fold filter-methodology to thoroughly control access to the EU (see (c) above). Its EU/Schengen-wide implementation was furthermore enhanced by a very practical tool, i.e. the Practical Handbook for Border Guards (Schengen Handbook) as established by a Commission recommendation of 6 November 2006<sup>8</sup>,

The EU-IBM approach was successfully exported even far beyond its limits by introducing it to the countries of the Western Balkans (Guidelines for Integrated Border Management in the Western Balkans of January 2007) and Central Asia (Handbook for implementation of the EU IBM concept in Central Asia of December 2006): international organisations such as UN and ICMPD actively assisted the implementation of this “advanced modernization tool” for trade and travel control purposes, while NATO and OSCE welcomed the reforms as contribution to the demilitarisation of border services formerly part of armed forces under the Soviet regime<sup>9</sup>. In the same perspective, EU-IBM standards have been part of CESS training courses on “Democratic Governance in the Security Sector” provided to the Black Sea and Southern Caucasus countries in 2006 and 2007<sup>10</sup>.

Despite this impressive record, one should not ignore the difficulties the IBM concept faces in establishing a coherent border approach for the European Union as a whole. While EU-IBM clearly exercises a positive influence in gradually approximating the standards applied at the various segments of the external border, there is no automatism implied. Beyond “encouraging” the Member States e.g. to use the before-mentioned handbook<sup>11</sup> for training purposes and “recommending” its transmission to the relevant border services, there is little authority Brussels can add to ensure its application at the local level. On the contrary, frequent statements that - despite a recognized need to ensure a uniform implementation of common rules – such handbooks and guidelines are “not intended to create any legally binding obligations upon Member States”<sup>12</sup> reconfirm national supremacy in practical border matters rather than the will to definitely change the situation.

A similar signal comes from the basic EU-IBM document itself: rather than being adopted as a formal legal instrument, its statements were presented as part of the conclusions of a JHA minister meeting – void of any legal effect.

All this confirms that despite positive tendencies in view of a more coherent, EU-driven management of the external borders, the main deficiencies/weaknesses continue to exist, i.e. that /due to the absence of a unique central body, the handling of border matters is still extensively exposed to diverging interests of individual countries (Members States and Schengen associate countries) and a multitude of half-ways coordinated authorities.

---

<sup>7</sup> EU Council (2006a)

<sup>8</sup> Commission (2006)

<sup>9</sup> see NATO (2003) nad OSCE Ministerial Conference, Border security and management concept. Ljubljana 2005 [http://www.osce.org/documents/mcs/2005/12/17436\\_en.pdf](http://www.osce.org/documents/mcs/2005/12/17436_en.pdf)

<sup>10</sup> see <http://www.cess.org/programmes/current/view/?id=8>

<sup>11</sup> "Practical Handbook for Border Guards (Schengen Handbook)", see EU Commission (2006)

<sup>12</sup> Commission (2006), p. 6

## 2.1.2 The Schengen Information System II (SIS II)

The original Schengen Information System (SIS) was designed as one of the compensatory measures<sup>13</sup> foreseen in the Schengen Agreement of 1985 to allow the lifting of controls at the internal borders. The principal purpose of border controls being to “keep the unwanted out and prevent the wanted from leaving”<sup>14</sup>, the need arose that all the information on wanted/unwanted individuals and objects be pooled and made available to control staff at common external border (instead of national borders as before).

SIS which became operational by 26 March 1995 works on the basis of alerts flagging wanted/unwanted individuals and objects according to the following criteria.

Regarding **wanted** persons/objects, one distinguishes between persons (a) wanted for extradition to another Schengen state (Art. 95 SCH 90), (b) missing (Art. 97), (c) wanted as witnesses, for prosecution or enforcement of judgments (Art. 98), (d) wanted for serious offences (Art. 99(2)) as well as objects such as motor vehicles, fire arms, identity papers etc which have been stolen, misappropriated or lost (Art. 100). The category of **unwanted** persons (Art. 96) concerns third-country nationals considered to present a threat to public policy, public security or national security of one of the Member States.

So far SIS stores only **alphanumeric data** (letters and numbers) regarding individuals<sup>15</sup>:

- names, including aliases;
- sex and "objective physical characteristics";
- date and place of birth;
- nationality;
- whether the persons are armed or violent;
- the reason for the alert; and
- the action to be taken

With its two-fold database structure (central CSIS and national NSIS/SIRENE), the system had to master a rapidly increasing data volume reaching 8.6 million records by 1998 and 22 million in 2007 (1.1 million of which related to persons)<sup>16</sup>. Also in other respects it was evident that the original SIS, designed for a maximum of 18 parties, would soon have to go beyond its predetermined limits. In 2001, in view of the forthcoming eastern/southern enlargement with 10 more Member States plus the Schengen accession of Norway, Iceland and lastly Switzerland, the EU commissioned the **new SIS II** which will be able to handle at least 31 parties (participating countries plus institutional users such as Europol)

The general system overhaul also presented the opportunity of equipping SIS II with some up-to-date technical and legal features: the new system as based on Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA allows to go beyond the alphanumeric limitations and store **biometric data** (for the time being fingerprint and facial image, but possibly at a later stage also DNA profiles and

---

<sup>13</sup> together with the following other complementary measures according to the Schengen Convention of 1990:

- reinforcement of external border controls on the basis of common standards (see 1.1.1 above and 1.1.4 below)
- common visa policy (see 1.1.3 below)
- enhanced police and judicial cooperation

<sup>14</sup> according to the concise formula used by the EU Committee of the UK House of Lords in its SIS II Report (UK House of Lords 2007)

<sup>15</sup> as well as corresponding details in the case of objects

<sup>16</sup> European Parliament (2008), p. 7

retina scans). The digital fingerprints may currently be used for the confirmation of identity only („one-to-one“ search) as opposed to an identification by means of a „one-to-many“ search“: the latter would require additional evidence of its reliability to be examined i.a. by the European Parliament<sup>17</sup>. It was furthermore recognized that SIS II would serve to a **dual purpose**, i.e. not only as a compensatory measure to ensure the free movement within the Schengen zone, but also – as is en vogue after 9/11 – to facilitate crime control, notably fight against terrorism and serious crime<sup>18</sup>.

In terms of comments, most criticism refers to the repeated delay in rendering SIS II fully operational: not only did this extensively strain the new Member States' patience in becoming part of the Schengen zone, it also upset the confidence in the Commission's long-term strategic planning of the project (UK House of Lords 2007, s. 27). Now in early January 2009, another postponement of the passage from SISone 4all to SIS II is in sight, probably for a date some time in 2010<sup>19</sup>. Technical problems to be expected during the very act of migration from one system to the other should not be underestimated (European Parliament 2008, p. 9ff).

While further concerns target various details of the project such as the yet unresolved discrepancy between the 1st and the 3rd Pillar part of SIS II<sup>20</sup>, observers are also troubled by the meagre hopes for a relatively uniform application of the system: too divergent were national practices in the past, notably with regard to classification of failed asylum seekers which in certain Member States were routinely considered “illegal aliens” and thus flagged in the system under Art. 96<sup>21</sup>. There is fear that similarly uncoordinated practices will develop as regards the collection of biometric data; so far, each country has its “own standards and ways of enrolling people into a system”<sup>22</sup> which heavily increases the risk of mismatches in identification procedures. Beyond this, current criticism addresses the overall technical performance of the system and even takes into consideration that the entire upgrade might be abandoned.<sup>23</sup>

Last but not least SIS II, as perfect as it may become implemented and developed over the time, sharply diverges in its very concept/philosophy from modern border concepts: conceived as a compensatory measure to address specific security/public policy threats within the Schengen zone, it focuses its attention on these threats, i.e. the persons/objects flagged, while ignoring the remaining instances of border-crossing. On top of this, neither SIS nor SIS II foresee recording the entry/exit movements of travellers, not even those flagged as wanted or unwanted by SIS alert<sup>24</sup>.

SIS II as it is currently envisaged does clearly not contribute anything to closing the gap in the sense of a European entry/exit system.

### 2.1.3 The Visa Information System (VIS)

Already by its name, VIS is often seen as direct counterpart to the US-VISIT representing the prototype of all entry-exit systems but in reality, things are quite different<sup>25</sup>. As with the Schengen Information System (SIS II), the VIS has its origins in the toolset developed to compensate possible security deficits arising from the abolition of internal border controls. Its primary purpose is to support

---

<sup>17</sup> Art. 22(c) Regulation (EC) 1987/2006 and Art. 22(c) Council Decision 2007/533/JHA

<sup>18</sup> Art. 1 (2) Regulation (EC) 1987/2006 and Art. 1 (2) Council Decision 2007/533/JHA. This allows – under certain conditions – to grant SIS II access to enforcement/criminal justice authorities such as Europol and Eurojust (Art. 41,42 of the Council Decision)

<sup>19</sup> Brunsdén, J. „Schengen data-sharing faces further delay“, *EuropeanVoice*, 8.1.2009. Retrieved from <http://www.europeanvoice.com/article/imported/schengen-data-sharing-system-faces-further-delay/63544.aspx>

<sup>20</sup> Notably with regard to the touchy issue of privacy/data protection: as long as the Framework Decision has not been adopted and implemented, it would not appropriate to implement SIS II (see UK HoL 2007, s. 124)

<sup>21</sup> Hobbing (2006), p. 4

<sup>22</sup> UK HoL (2007), s. 58

<sup>23</sup> according to statements by the Czech presidency of 15 January 2009. See EUobserver of 16.1.09 retrieved from <http://euobserver.com/22/27420>

<sup>24</sup> Meyers, Koslowski and Ginsburg (2007), p. 19

<sup>25</sup> Hobbing (2007), p. 5

the **common visa policy** which represents an important prerequisite for the functioning of the Schengen area.

Already in the late 1990s it became obvious that the common visa system was increasingly exposed to so-called “**visa-shopping**”, i.e. multiple or chain requests lodged by the same person to the visa authorities of various Member States. This implied the risk of not only overloading the system but also that the applicants took advantage of diverging practices in the granting of visa. In order to allow for greater transparency in the issuance procedures, the development of VIS began in 2001<sup>26</sup>, with the relevant legal bases being adopted in 2008<sup>27</sup> and its full operation including roll-out at consulates and border crossing points in 2012<sup>28</sup>.

Based on its “capacity to connect at least 27 Member States, 12 000 VIS users and 3,500 consular posts worldwide”<sup>29</sup>, the VIS will allow the Schengen Member States to exchange data on short-stay and transit visas.

As a result of prolonged debates, in particular with the European Parliament and the data protection authorities, the VIS package finally adopted in 2008 is based on several safeguards ensuring a far-reaching protection of civil liberties notably in the field of data protection<sup>30</sup>.

In terms of legislative purposes, visa and asylum-related issues (fight against fraud, facilitation of issuing procedures and border checks) definitely dominate, while the “prevention of threats to internal security” plays a secondary role, appears only as the last among seven items (Art. 2 (g) Regulation (EC) No 767/2008). There is a clear limitation of the data to be recorded under the following categories (Art. 5):

- **alphanumeric** data on the applicant<sup>31</sup> and on visas<sup>32</sup> requested, issued, refused, annulled, revoked or extended
- **biometric data** of the applicant in terms of (1) a digital photograph in compliance with Regulation (EC) 1683/95 and thus ICAO standards and (2) digital fingerprints in accordance with the Common Consular Instructions (CCI), whereby the **ten-finger** requirement is part of still a pending proposal for amending the CCI21<sup>33</sup>

VIS being primarily a tool of visa policy, access by other government branches remains a closely supervised exception: a three-tier system of access rights distinguishes between visa authorities as the normal “stakeholders”, border and other authorities competent to carry out identity checks and finally, with the strictest conditions imposed, authorities, including Europol, competent for the prevention, detection and investigation of terrorist offences and serious crime (Art. 3)<sup>34</sup>

As regards system architecture, VIS although sharing the same technical platform with the SIS II database, has been designed as an entirely separate system without interface to any other large scale IT-system at EU-level such as SIS II and Eurodac. Although in the framework of post-9/11 discussions concepts of synergy and interoperability were examined (EU Commission 2005), privacy considerations finally prevailed to keep VIS entirely apart.

---

<sup>26</sup> Decision 2004/512/EC

<sup>27</sup> Regulation (EC) No 767/2008 and Decision 2008/633/JHA

<sup>28</sup> EU Commission, Rapid news MEMO/08/85 of 13 February 2008, retrieved from [europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/85&format=DOC&aged=1&language=EN&guiLanguage=en](http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/85&format=DOC&aged=1&language=EN&guiLanguage=en)

<sup>29</sup> EU Commission (2003)

<sup>30</sup> see Hobbing (2007), p. 5f

<sup>31</sup> in particular: name, sex, date and place of birth, nationality, residence, employer, ...

<sup>32</sup> in particular: place and date of the application; type of visa requested; details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, main destination and duration of the intended stay; purpose of travel; intended date of arrival and departure; intended border of first entry or transit route

<sup>33</sup> „ten fingerprints taken flat and digitally captured“; cf. COM(2006)269 final,

<sup>34</sup> for details see Hobbing (2007), p. 8

The only issue currently pending concerns the frequency with which border checks have to be carried out not only on the basis of the visa sticker number but also involving the verification of fingerprints: the European Parliament in principle agrees with the Commission approach that such checks of biometric identifiers should be routinely employed in order to prevent visa fraud (COM 2008), but insists that in view of avoiding excessive waiting times at the border, exemptions from the checking requirement should be foreseen (European Parliament 2008a).

Another legislative initiative promises the development of greater coherence in the management of the external EU border: according to the proposed amendment of the Common Consular Instructions (CCI), Member States could in the future opt to represent each other in the reception of visa application and the enrolment of biometric identifiers (EU Commission 2006a). This proposal which has been endorsed by the EP<sup>35</sup> would even allow for the creation of **common biometric enrolment centres** run jointly by the consular services in question.

In the context of VIS, one should by no means not forget the recent project of a **Biometric Matching System (BMS)** designed to become the „central biometric component of a collection of European Union identity programs for the protection of citizens and Schengen borders“<sup>36</sup>. BMS represents a powerful search engine that can match biometric data from visa applications etc with biometric data stored at central level<sup>37</sup>. Currently BMS is foreseen to exclusively serve the VIS but extensions are planned for the future to cover further biometry-based systems such as Eurodac and SIS II<sup>38</sup>.

From an overall point of view, however, the same is true as was said about the two previous items EU-IBM and SIS II: all these systems originally established as Schengen compensatory measures hardly qualify for implementing the more recent border concepts in the sense of watertight entry-exit systems. As they are all built around a specific compensatory purpose (common border management, common prevention of specific threats, common visa policy) they do neither per se cover global entry-exit solutions nor are they susceptible for easy transformation into such a mechanism.

Such transformation into an entry-exit has actually been considered in the context of the discussion of enhanced synergy and interoperability of EU databases (EU Commission 2005) but was not pursued any further due to reasons of data protection and practicability.

#### 2.1.4 Eurodac

Eurodac represents a EU-wide system for the identification of **asylum-seekers**, based on electronic comparison of fingerprints. Created in the context of the Dublin Convention of 1997<sup>39</sup>, Eurodac<sup>40</sup> was assigned a decisive role in the fight against asylum shopping. If the responsibility of examining asylum applications was routinely incumbent on the Member State first entered by the asylum-seeker, it often turned out to be difficult to identify this Member State of first entry – all the more as the examination was mostly considered a rather unwelcome burden.

Fingerprints to be taken of each asylum-seeker/illegal immigrant and their immediate transmission to the Eurodac central unit appeared the only way to ensure the identification of the Member States in question<sup>41</sup>.

---

<sup>35</sup> European Parliament (2008b)

<sup>36</sup> see press release of 20 October 2008 by Accenture/Sagem on the development contract awarded to them by the Commission [http://newsroom.accenture.com/article\\_display.cfm?article\\_id=4762](http://newsroom.accenture.com/article_display.cfm?article_id=4762)

<sup>37</sup> The BMS database will be able to store the fingerprints of up to 70 million people and process more than 100,000 verification and identification requests per day. The system will perform one-to-one comparisons for biometric verifications and one-to-many searches for biometric identifications (ibid).

<sup>38</sup> Paul, F. (2007)

<sup>39</sup> later replaced by the “Dublin II” Regulation (EC) 343/2003

<sup>40</sup> on the basis of Regulation (EC) 2725/2000

<sup>41</sup> Art. 4, 8 Regulation (EC) 2725/2000

Eurodac, being operational as the first European AFIS (Automated fingerprint identification system) since 15 January 2003, relies on a fully automated central database which - besides details on the asylum application – only contains biometric fingerprint data (ten fingers – rolled impression) as the most accurate method of identification. The record does not include the name of the asylum seeker<sup>42</sup>.

From a technical point of view, Eurodac has worked almost faultlessly ever since and at a reasonable expenditure<sup>43</sup>. Problems concern, however, the consistent use of the system by Member States authorities: due to imprecise language in the regulation, finger print data are transmitted to the central unit too late (or never) which puts at risk the smooth working of the system.<sup>44</sup>

A major change is in sight for Eurodac, once the **Biometric Matching System (BMS)** will be in place and has been accepted as the central storage facility for biometric data: in this case Eurodac would be integrated into the BMS framework<sup>45</sup>

### 2.1.5 FRONTEX and its involvement in operative action

Despite its before-mentioned limitations in terms of competence (see Section 2.1 above), FRONTEX as combined with financial incentives has exercised quite a positive influence on the practical cooperation between Member States in the management of the external border.

Within three years after its set-up in 2005, FRONTEX has become a widely known actor on the European stage – making the headlines probably more often than any other of the 36 EU agencies. Despite this publicity, mainly due to its involvement in the spectacular maritime operations around Malta and the Canary Islands, one may note that FRONTEX still is “a baby” in full development and need for support and guidance by its parents<sup>46</sup>.

FRONTEX has developed rapidly in terms of staff (2005: 44; 2008: 189) and resources (2006: €19m; 2008: 70m) and to a certain extent also as regards competences.

As we pointed out above, the remit given to FRONTEX was based on the strict acceptance of the traditional role of Member States as “guardians” of the external border and its integrity. The only way to exercise EU influence in this field was by offering assistance to Member States requesting so. It would now be appropriate to examine to what extent this soft approach has helped to pave the way for a more formal involvement in operational border activities.

Besides the more secluded functions which according to Art. 2(1) Regulation (EC) 2007/2004 cover letters (b) assistance to border guard training, (c) carrying out risk analyses, (d) follow-up on relevant research development, it is mainly the operational issues which deserve special attention.

Given that according to the Director of FRONTEX, General Laitinen, item (f) assisting with joint return operations was also “not at the top of the priorities”<sup>47</sup>, the agency’s main focus has evidently been on Art. 2(1)(a), i.e. **coordination of operational cooperation between Member States**. The

---

<sup>42</sup> *ibid.* Art. 5

<sup>43</sup> see RAPID Press release „EU’s biometric database continues to ensure effective management of the Common European Asylum System „, of 18.9.2007 retrieved from <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1347&format=HTML&aged=0&language=EN&guiLanguage=en>

<sup>44</sup> an amendment has recently been proposed by the Commission (see doc. COM (2008) 825 final of 3.12.2008. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0825:FIN:EN:PDF>

<sup>45</sup> Eurodac annual report CNS/1999/0116 of 11/09/2007 <http://www.europarl.europa.eu/oeil/resume.jsp?id=172842&eventId=1007046&backToCaller=NO&language=en>

<sup>46</sup> MEP Javier Moreno Sanchez in his statement before the UK House of Lords European Committee on 16 October 2007 (UK HoL 2008, s. 3)

<sup>47</sup> *ibid.* s.64



agency has indeed spent far more than half of its budget on operational activities<sup>48</sup>, 80% of which went into maritime operations<sup>49</sup>.

With names borrowed mainly from Greek-Roman mythology (from „Ariadne“ to „Minerva“), well beyond 40 operations have been conducted between 2006 and 2008, including 9 maritime, 12 land and 5 mixed operations as well as 10 pilot projects<sup>50</sup>; 26 of these operations are described in detail on the FRONTEX website<sup>51</sup>. Between 5 and 12 Member States participated in each event supported by appropriate operational resources such as vessels/aircraft. In terms of results, the FRONTEX evaluation report points to „more than 53,000 persons, for 2006 and 2007 together, [who] have been apprehended or denied entry at the border during these operations. More than 2 900 false or falsified travel documents have been detected and 58 facilitators of illegal migration arrested.”<sup>52</sup>

Even if these “achievements” have equally provoked critical comments in terms of “human rights violations”<sup>53</sup> during the so-called search and rescue operations (SAR) in the Mediterranean, it is generally recognised that FRONTEX has made great progress in short time<sup>54</sup>. **Human rights** issues especially in the context of the disembarkation of intercepted persons deserved close attention, but required guidance from a higher level forum rather than ad-hoc decision-making within individual FRONTEX missions<sup>55</sup>.

Further problems exist with regard to the commitment of some Member States actually to make available the resources they have promised in the framework of **CRATE** (Central Register of Available Technical Equipment): a striking example was cited by MEP Bussutil according to whom not one of the 32 patrol vessels pledged by Italy took part in Operation NAUTILUS in July 2007<sup>56</sup>.

This may indicate that Member States still take the much strained national autonomy in border management too literal. In fact, it seems common sense for a coordinator to expect that “there is something to coordinate”<sup>57</sup>.

Also the newly adopted **RABITs Regulation (EC) 863/2007** did not essentially change the situation: RABITs operations – foreseen for emergency situations of an unexpected nature<sup>58</sup> - are based on a novel concept called “compulsory solidarity”, which means that Member States are in principle obliged to participate. However, the regulation itself leaves loopholes: besides duly repeating that “the responsibility for the control and surveillance of external borders lies with the Member States”<sup>59</sup>, it also exempts Member States “faced with an exceptional situation substantially affecting the discharge of national tasks” (Art. 4(3)).

RABITs officers (as well as officers participating in other FRONTEX operations!) enjoy important new powers which in a way represent a quantum leap in European enforcement cooperation: not only are they entitled to “carry service **weapons**, ammunition and equipment as authorised according to the home Member State’s national law” (Art. 6 (5)), they also have the **legal capacity** to carry out active

---

<sup>48</sup> Jeandesboz, J. (2008), p. 12

<sup>49</sup> UK HoL, s.92

<sup>50</sup> EU Commission (2008a), s.6

<sup>51</sup> [http://www.frontex.europa.eu/examples\\_of\\_accomplished\\_operati](http://www.frontex.europa.eu/examples_of_accomplished_operati)

<sup>52</sup> EU Commission (2008a), s.9

<sup>53</sup> Georgi, F. (2008); Jeandesboz, J. (2008), p. 17; Carrera (2007), p. 26

<sup>54</sup> UK HoL (2008), s. 185

<sup>55</sup> *ibid.* S. 112f: According to MEP Gérard Deprez it should not be the responsibility of the Master of the vessel which rescues persons to decide where they should be disembarked; much rather this must be addressed by the working group developing general guidelines about the law of the sea as it relates to EU States and illegal migration.

<sup>56</sup> *Ibid.*, s. 105

<sup>57</sup> *ibid.*, s. 106

<sup>58</sup> contrary to **foreseeable** situations identified by means of risk analysis, as covered by Art. 2(1) (a) of the FRONTEX regulation.

<sup>59</sup> Regulation (EC) 863/2007, whereas-clause 5

border guard activities, i.e. to perform all tasks and exercise all powers for border checks or border surveillance in accordance with Regulation (EC) No 562/2006. Up to then such transfer of public authority to foreign officers was possible only in certain European countries<sup>60</sup>

The RAPID Staff Pool was in the meantime established and currently comprises 629 border policemen from all EU Member States including Iceland and Norway (with the exception of Ireland and UK). Three RABITs training exercises have been successfully conducted (Portugal 2007, Slovenia and Romania 2008)<sup>61</sup>, but so far the capacity not actually been used.

At this stage, one might note the “FRONTEX-experiment” with its soft entry into a domain of traditional national predominance has brought unexpected progress under a few important aspects:

- The 40+ operations held so far on a voluntary basis have allowed Member States to get acquainted with the method (and learn to appreciate the multilateral cooperation)
- Practical experience gained and problems jointly encountered have evidently reduced traditional reticence against the presence of foreign officials and the exercise of public authority by them.

These features have in contrast not brought about a revolution in public perception towards a new European approach in border and other. Traditions continue to exist. National borders continue to be “hugely symbolic” and there has so far been no “spill-over effect” in the sense that the positive FRONTEX experience would overcome centuries-old prejudices.

#### 2.1.6 “Second-line” controls within the territory

Although not formally part of the border surveillance scheme, most EU Member States heavily rely on an internal control scheme composed of (1) the requirement for immigrants (as well as EU citizens) to register with the police at their new address<sup>62</sup> and (2) controls of the labour market to detect illegal employment which in most cases coincides with cases of illegal immigration<sup>63</sup>. In addition, Member States make use of the spot check option to control ID cards anywhere in the territory as granted by Article 2 (3) of the 1990 Schengen Convention<sup>64</sup>. Even the UK recognises that due to the „difficulty of policing long land frontiers“, continental Europe has a much greater dependence on internal controls, such as identity checks<sup>65</sup>.

#### 2.1.7 Missing links

Beyond the mechanisms so far described, the EU stands out by the absence of certain devices which have become routine for many of the partners in the transatlantic framework and elsewhere.

Such unusual “white spots” in EU border security arrangements concern in particular the control/monitoring of air traffic, notably by means of Passenger Name Records (PNR) and systems of electronic travel authorization (ETA/ESTA).

---

<sup>60</sup> Hobbing (2003), p. 22

<sup>61</sup> see FRONTEX news <http://www.frontex.europa.eu/search/go:szukaj/>

<sup>62</sup> see Article 22 Schengen Convention 1990

<sup>63</sup> e.g., in Germany this task is carried out by the Customs administration which undertakes large scale operations to tackle illegal employment, [http://www.zoll.de/english\\_version/f0\\_aentg/index.html](http://www.zoll.de/english_version/f0_aentg/index.html), [http://www.zoll.de/d0\\_zoll\\_im\\_einsatz/b0\\_finanzkontrolle/i0\\_aufgaben/index.html](http://www.zoll.de/d0_zoll_im_einsatz/b0_finanzkontrolle/i0_aufgaben/index.html); at the EU level, the Commission proposal on “sanctions against employers of illegally staying third-country nationals” (EU Commission 2007a) is about to be approved by European Parliament, see EUobserver of 4 February 2009, <http://euobserver.com/9/27527/?rk=1>

<sup>64</sup> see Hobbing (2005), p. 16

<sup>65</sup> UK HoL (2008), s. 43



### *2.1.7.1 The EU-PNR system still not in place*

Although the EU has duly served other countries in facilitating the transmission of passenger data by concluding formal agreements with the US (2004,2007), Canada (2005) and Australia (2008)<sup>66</sup>, it has so far renounced on establishing its own mechanism. This is not to say that no attempt was made (see 2007 Commission proposal for a “Council Framework Decision on the use of Passenger Name Record for law enforcement purposes”<sup>67</sup>) but a number of complications have up to now impeded the adoption of a sound instrument.

There have been burdens from the past in the context of the US agreements which left their scars and inhibited a positive climate of interaction between the legislative players. Parliament<sup>68</sup> and privacy authorities feeling routinely excluded by the Council, the unexpected outcome of the procedure before the European Court of Justice, the Commission allegedly accepting lower privacy standards when negotiating the second US agreement, all this added to an atmosphere of mutual mistrust<sup>69</sup>.

This and further issues of disagreement arisen in 2008, not only between the institutions, but also between groups of Member States, make it highly unlikely that a solution be found on the basis of the current proposal<sup>70</sup>. It would therefore appear appropriate to deal with this issue rather in the context of part 3.1. covering future developments.

### *2.1.7.2 ETA/ESTA scheme*

Considerations regarding the introduction of ETA/ESTA have so far been entirely absent from formal discussions at EU level; possibly due to the minor percentage of travellers arriving in the EU by air, the subject has up to now not been considered of a vital importance for European needs. However, it is now addressed by the Commission as a possible “tool of the future” it is necessary to allow for more flexible solutions in border management and thus include internal control mechanisms (EU Commission 2008c).

## **Intermediary conclusions on 2.1**

Our snapshot of the current situation of EU borders confirms the (still) very fragmentary character of protection devices: national structures still dominate the picture and there are relatively few elements which bear a clear European Union mark. Neither is there a definitely established border line nor a central authority which would oversee the loosely coordinated cluster of national border segments, let alone command a common corps of border guards. Existing database systems cover certain border-related aspects but are far from providing a seamless recording of all cross-border movements. The newly created FRONTEX agency owed its successful entry into the domain of operational border security to the clear acceptance of a secondary role as a support service.

This illustrates how far the EU at this stage is still away from the US situation characterised by a centuries-old state and border structure as well as a federal border administration which understands its duty as “It’s law enforcement on a nationwide scale... from coast to coast, border to border”<sup>71</sup>.

---

<sup>66</sup> significantly enough for the overall situation, this instrument is still exposed to the pending EP decision on whether to challenge the agreement before the ECJ (EP Press release „Legitimacy of PNR challenged again” of 14.10.08 <http://www.libertysecurity.org/article2265.html>

<sup>67</sup> COM(2007) 654 final of 27.11.07

<sup>68</sup> see as a most recent example the session report of 20 October 2008 on PNR matters <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20081020+ITEM-015+DOC+XML+V0//EN>

<sup>69</sup> for a detailed description see Hobbing (2008), p. 11f, 48ff

<sup>70</sup> see Statewatch News Online (2008) according to which the Commission proposal is „being rewritten from scratch“

<sup>71</sup> US Customs recruitment message

## 2.2 US Border Security Systems: More but Incomplete

In the wake of the September 11, 2001 al Qaeda attacks on the United States, the Bush Administration endeavoured to create a “smart border,” which “must integrate actions abroad to screen goods and people prior to their arrival in sovereign U.S. territory, ... allow extensive prescreening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic, [and] use ... advanced technology to track the movement of cargo and the entry and exit of individuals (White House 2005).” In a dramatic illustration of the administration’s agenda, Richard Falkenrath, former deputy assistant to the president and deputy Homeland Security advisor, drew an analogy likening the revolution in military affairs of the 1990s to the “revolution in border security” that is taking place now.<sup>72</sup>

The “smart borders” concept was incorporated into the U.S. National Homeland Security Strategy, which advocates “pushing borders out” beyond U.S. territorial boundaries by stationing Customs and Border Protection (CBP) officers in seaports and airports abroad and by requiring electronic submission of passenger and cargo manifests in advance of departure to the United States. As expanding e-government and private sector submission of electronic data enables the preclearance of passengers and cargo, thereby removing the necessity of inspection at territorial boundaries, the objective is for borders to increasingly exist *de facto* in cyberspace, i.e., become “virtual borders.”

This strategy of employing technology as a “force multiplier” that shifts borders outward clearly has had consequences for all those who travel to the US and for those states sharing a land border with the US. The growing impact of the US changing border security strategy has become evident as the US government deployed a series of systems and programs, most notably the automated biometric entry-exit system US-VISIT and the Secure Border Initiative (SBI) as well as reforms of the Visa Waiver Program (VWP) and deployment of the related Electronic System for Travel Authorization (ESTA). These multimillion dollar initiatives have increased the number of tools available to border control authorities, however, their implementation has been far from complete and whether they can meet policymaker expectations in terms of both counter-terrorism and immigration law enforcement mission is yet to be seen.

### 2.2.1 Entry-Exit: US-VISIT and supporting mechanisms

The basics of entry systems in the US are rather straightforward and similar to processes in many other countries. In the primary inspection process that occurs when a traveler first encounters an officer at a port of entry, the officer inputs a traveler’s data, usually through swiping the machine readable zone of the traveler’s passport, into a system that can query a database with a watch list of individual names, passport numbers etc. that may generate a “hit,” which is then further investigated in secondary inspection.

US immigration inspectors began using the National Automated Immigration Lookout System (NAIIS) in 1983 and by 1988 it became available at 44 of the then 610 ports of entry (GAO 1988). In the 1990s, the former U.S. Immigration and Naturalization Service (INS) updated and supplemented this basic entry system.

In 1996, the US Congress passed the *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*. This law included section 110.a.1, “Automated Entry-Exit Control System,” which mandated the development of an automated entry-exit control system that would “collect a record of every alien departing the United States and match the records of departure with the record of the alien’s arrival in the United States.”<sup>73</sup> US business groups, states, and localities bordering Canada and Mexico argued

---

<sup>72</sup> Response to Rey Koslowki’s question at “Transatlantic Homeland Security? European Approaches to ‘Total Defense,’ ‘Societal Security’ and Their Implications for the U.S.,” Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, February 19, 2004.

<sup>73</sup> *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, section 110.a.1, “Automated Entry-Exit Control System,” U.S. Congressional Record—House (September 28, 1996): H11787.

against the new entry-exit data collection requirements noting that registering every person who crosses into the US from Canada or Mexico, even using then-existing smart card technology, would still require enough processing time to back up traffic at the border for hours, especially at the US-Canadian border crossing between Detroit, Michigan and Windsor, Ontario, impair international movement of goods and people, thereby costing billions of dollars in lost trade and tourism receipts to the US (Senate 1998).

In response to this lobbying, Congress pushed back the impending deadline for implementation of the law in 1998 (Cohn 1999) and then in 2000, pushed back the deadline once again. The Data Management Improvement Act (DMIA) of 2000 amended Section 110, mandating the development of an entry-exit system to be put in place at all air and seaports by the end of 2003, at the fifty most highly trafficked land ports of entry by the end of 2004, and at all ports of entry by the end of 2005. In practical terms, however, the DMIA deflected the creation of a full-fledged entry-exit system with a complete database since it limited data collection to that which was already being collected by the INS by existing authorities of law and disallowed collection of any new entry-exit data.<sup>74</sup>

The resulting entry-exit tracking system primarily covered passengers arriving by air and consisted of a paper I-94 arrival/departure form stamped at the port-of-entry, which was supposed to be collected by the airline upon departure, given to immigration authorities and entered into a database. Due to lost forms, incomplete or inaccurate data entry, exit by land border, and incomplete deployment of the system, missing exit data corrupted the database, leaving immigration inspectors with no effective way of knowing if individuals had overstayed their visas (Bromwich 1999). This was the case with several of the September 11 hijackers.

In response to the September 11 attacks and the failures of government information systems that they exposed, Congress passed and President Bush signed into law entry-exit system provisions in the USA PATRIOT Act<sup>75</sup> and in the Enhanced Border Security and Visa Entry Reform Act of 2002.<sup>76</sup> Both pieces of legislation reiterated the DMIA mandate for implementation of an entry-exit system. The USA PATRIOT Act mandated that the entry-exit system should utilize biometric technology and tamper-resistant, machine-readable documents and that the system should be able to interface with other law enforcement databases. The Enhanced Border Security and Visa Entry Reform Act, passed in the Senate by a margin of 97 to 0 and in the House 411 to 0, specifically required the development of a database for arrival and departure data from machine-readable travel documents, the establishment of standards for biometrics for visas and other travel documents, and the installation of equipment at all ports of entry to enable collection, comparison, and authentication of biometric data. In order to address the loopholes that allowed some members of Al Qaeda to enter on U.S. visas, Congress mandated that all U.S. visas incorporate a biometric identifier by October 26, 2004, and a combination of facial recognition and electronic fingerprint scanning was selected as “the most effective and least intrusive (Jacobs 2003).”

Subsequently, the Intelligence Reform and Terrorism Prevention Act of 2004 called for an acceleration of the full implementation of an automated biometric entry-exit data system; collection of biometric exit data from all those required to provide biometrics upon entry; integration of all databases that contain information on aliens and interoperability with the entry-exit system; policies and procedures to maintain accuracy and integrity of entry-exit data, frontline personnel training, and a registered traveler program that is integrated into the automated biometric entry-exit system.<sup>77</sup>

---

<sup>74</sup> See *Data Management Improvement Act of 2000*, Public Law 106-215.

<sup>75</sup> *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Public Law 107-56, section 414 (October 26, 2001).

<sup>76</sup> *Enhanced Border Security and Visa Entry Reform Act of 2002*, Public Law 107-173, section 302 (May 14, 2002).

<sup>77</sup> *The Intelligence Reform and Terrorism Prevention Act of 2004*, House Report 108-796, Section 7208.

In accordance with congressional mandates, US-VISIT is being implemented incrementally and the requirements of the first three of four increments are being met by extending, enhancing, and building interfaces between some (and potentially all) of the following legacy systems:

Arrival Departure Information System/Visa Waiver Permanent Program Act Support System (ADIS/VWPASS)  
Advance Passenger Information System (APIS)  
Biometric Verification System (BVS)  
Consolidated Consular Database (CCD)  
Central Index System (CIS)  
Computer-Linked Application Information Management System (CLAIMS)  
Consular Lookout and Support System (CLASS)  
Global Enrollment System (GES)  
Integrated Automated Fingerprint Information System (IAFIS)  
Interagency Border Inspection System (IBIS)  
INS Automated Biometric Identification System (IDENT)  
Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS)  
National Automated Immigration Lookout System (NAILS II)  
NEXUS  
Nonimmigrant Information System (NIIS)  
Outlying Area Reporting Station (OARS)  
Portable Automated Lookout System (PALS)  
Secure Electronic Network for Travelers Rapid Inspection (SENTRI)  
Student Exchange and Visitor Information System (SEVIS)

By interfacing many of the above existing legacy INS and U.S. Customs systems, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is developing the mandated automated biometric entry-exit system, which is currently serving as the entry system used by inspectors at ports of entry. US-VISIT collects biographical and biometric data (digital photo of face and finger scans) from certain foreign nationals when they apply for visas at U.S. consulates abroad<sup>78</sup> as well as when they enter the United States. Watch list checks are run on the data collected in order to help inspectors at ports of entry keep out potential terrorists and criminals as well as determine whether those who enter the United States leave in accordance with the terms of their visas. The US-VISIT contract solicitation outlined a more comprehensive vision to develop US-VISIT into a “virtual border” (DHS 2003) and this contract was won by an Accenture-led team of companies in May 2004. The US-VISIT program has cost close to \$2 billion through Fiscal Year (FY) 2009 and its projected cost through FY 2014 is between \$7.2 billion and \$14 billion (Hite 2004).

US-VISIT was first deployed at airports on January 1, 2004 and by the end of 2005 it was in place at all 284 air, land and sea ports of entry (DHS 2005). In the four years since the initial deployment of US-VISIT at the beginning of 2004 to March 2008, biometrics have been collected from 113 million individuals entering the US and run against watchlist databases (Chertoff 2008). More than 1,800 criminals or immigration violators have been stopped from entering the United States with the help of US-VISIT (Barth 2007). Although US-VISIT is fast becoming the world’s largest biometric database, it is still very much a work in progress. For example, exit data beyond that received from airline and ship manifests are not yet collected, therefore, US-VISIT is not yet a fully functioning entry-exit system.

The system works as follows: The pre-entry process begins at U.S. consulates abroad. Nonimmigrant visa applicants provide biographic data on the visa application and submit a digital photograph and fingerprint scans at U.S. embassies and consulates. These data are checked against the Consular Lookout and Support System (CLASS) watch list, which includes data from the Justice Department’s National Crime Information Center (NCIC) system, a computerized index of criminal justice information (criminal records, fugitives, terrorist lookouts, missing persons, etc.) as well as other

---

<sup>78</sup> In cooperation with the State Department’s BioVisa program.

Interagency Border Inspection System (IBIS) watch lists. A record is then generated within IBIS. IBIS is a system shared by twenty law enforcement and border control agencies that resides on the Treasury Enforcement Communication System (TECS) at the CBP Data Center. After watch list checks are run, the visa application is either approved or denied. When those who have received a visa board a U.S.-bound airplane or ship, the airlines and sea carriers are required to electronically transmit passenger manifests using the Advance Passenger Information System (APIS). Passenger data on these manifests are then checked against watch lists in advance of arrival at U.S. ports of entry.

The entry process at ports of entry begins when a foreign national arrives at the primary inspection site and presents his or her travel documents to the CBP officer. The CBP officer scans the machine-readable documents (or enters data manually if documents are not machine readable) into IBIS. The Inspector Field Manual requires that in primary inspections, inspectors must run queries of IBIS using the foreign national's last name, first name, date of birth, and passport number (DHS-OIG 2004, 15). IBIS and APIS queries generate any existing biographical lookout hits and existing records based on manifest data. IBIS also indicates if there are any existing fingerprints in the IDENT database that were submitted during the visa application process. Once a biographical record is generated from the Consolidated Consular Database (CCD) or from passenger manifest data, the inspector switches to the IDENT screen, takes the person's photograph, and scans his or her fingers. These biometrics are checked against the IDENT database. If there are no fingerprints in the database, the person is enrolled in US-VISIT; if there are fingerprints that were submitted during the visa application process, a one-to-one match with data from the initial enrollment abroad verifies the individual's identity. If there is a watch list hit or a biometric mismatch, the person goes to secondary inspection for additional screening (GAO 2004).

An automated entry-exit system can be a very powerful tool to identify visa-overstayers, as Australian experience amply demonstrates. Australian inspectors electronically record the entry of everyone entering Australia (whether a foreigner or Australian citizen), usually with an automated passport reader. Inspectors similarly capture passport data from everyone leaving and the system matches exit records with corresponding entry records. If the system determines that someone has overstayed his or her visa, he or she will be referred to secondary inspection for an interview. If the overstay is more than 28 days, the person is informed that he or she will not be granted a temporary visa to travel to Australia for three years. The Australian border officials have been collecting entry and exit data since 1981 and, due to improvements in data collection, such as automated passport readers at entry and exit, they can now easily determine the number of people who have overstayed their visas, e.g. 47,500 in 2005 (DIMA 2005, p. 77 ).

The situation in the U.S. has been quite different. There are no exit controls at land border crossing points and therefore no systematic collection of I-94 forms. Lost forms, incomplete or inaccurate data entry and exit by land border have meant that the missing exit data corrupted the database. US-VISIT can become a powerful immigration law enforcement tool; however, the database must be accurate enough to ensure that the lack of an exit record truly meant that the person in question actually had not left the country. If there were to be repeated errors in the exit data that could be corroborated by other evidence (e.g., an entry stamp in the individual's passport from another country before the individual's U.S. visa expired, combined with boarding passes, home videos documenting the individual's homecoming, etc.), then the entry-exit system could be considered unreliable as a whole and the data it generated not useful for the prosecution of individual cases. If one individual could register an exit of another without being detected by the entry-exit system, it could be susceptible to fraud. Once identified, it is unlikely that a visa overstayer would remain at the address originally given upon arrival, and even if he or she did, there are a limited number of Immigration and Customs Enforcement (ICE) officers available to find, apprehend, and deport millions of visa overstayers (see e.g. Senate 1998, pp. 14-16).

Although it is clear that an automated entry-exit system cannot also automatically enforce visa time limitations, such a system constrains the options open to visa overstayers that may, in turn, modify their behavior. Most importantly, individuals may be able to overstay their visas once (not be found and remain in the United States), but it would be very difficult for them to leave the United States,

apply for another visa, and overstay again. Without a credible entry-exit system, it has been possible for visa overstayers to not only stay in the United States, but also to travel back and forth. If nothing else, US-VISIT could reduce the total number of visa overstayers in the United States simply by stopping those who have overstayed from returning again.

Alternatively, if deployment of US-VISIT is not paired with increased enforcement of laws prohibiting employment of illegal migrant workers, visa overstayers who are gainfully employed in the U.S. underground economy may simply opt to remain in the United States and not return home so as to not risk being denied entry. Those who obtain a visa in order to enter the United States and work illegally may opt to stay as well. It may have the same effect that increased enforcement at the U.S.-Mexican border has had—turning temporary illegal migrant workers into permanent illegal migrant workers who opt to have their families smuggled into the United States once rather than paying multiple smuggler’s fees and repeatedly risking assault, theft, injury, or apprehension on trips back and forth themselves.

Moreover, with the addition of its biometric capabilities, US-VISIT differs fundamentally from the previous, incomplete automated entry-exit system, which was more susceptible to fraud. With the addition of biometrics, the system has been useful in stopping those with records of criminal or immigration violations from entering the United States, some of whom had previously entered the United States repeatedly using aliases and fraudulent documents but whose fingerprints collected upon entry produced watch list hits in IDENT. Moreover, since US-VISIT’s biometric capabilities make it more difficult to commit visa fraud; it will most likely deter foreign nationals from attempting it.

With respect to counterterrorism, the DHS has yet to announce the apprehension of a single suspected terrorist with data gathered by US-VISIT (although visa applications have been denied by the State Department due to security watch list checks supported by biometrics). Of course, one can never know how many potential terrorists were deterred. The nearly completed upgrade in biometric collection from two index fingerprints to full 10 fingerprint scans may specifically deter the entry of terrorists who may have left their fingerprints in terrorist training camps and safe houses captured by the US military or may have their fingerprints in law enforcement databases of countries that are cooperating with the US. Even if US-VISIT did collect data used to identify a terrorism suspect, law enforcement and intelligence agencies may opt not to make it public, so as not to compromise ongoing investigations.

Terrorists may simply circumvent US-VISIT by crossing borders between points of entry. One stakeholder in the Detroit-Windsor area noted that while CBP is collecting fingerprints from legitimate travelers crossing the Ambassador Bridge, a terrorist could easily take a boat across the Detroit River into the United States undetected just a few miles up- or downstream, mixing in with the thousands of Michigan’s recreational boaters. Terrorists could be smuggled into the United States between ports of entry, just as hundreds of thousands of illegal migrants are every year. In Congressional testimony, former Deputy Secretary of Homeland Security James Loy noted that “several Al Qaeda leaders believe operatives can pay their way into the country through Mexico (Loy 2005).”

Frontline border control officers often compare their task to squeezing a balloon: If you squeeze one end, it expands at the other. Clamping down at one part of the border diverts smugglers and illegal migrants to attempt to cross elsewhere. If one stiffens controls at some ports of entry or eliminates one form of visa and document fraud, smugglers will try others and put new pressures on other systems. US-VISIT will increase the risks for terrorists attempting to enter the United States undetected through ports of entry. Should they not be deterred and persist in their attempts, US-VISIT may divert them into means of entry that pose higher risks of apprehension and/or other harm that disables them and disrupts their plot.

Essentially, US-VISIT is an additional obstacle to foreign terrorists wishing to enter the United States, however, even when fully deployed, it is unlikely itself to catch many terrorists trying to enter the United States. It is unlikely that “established terrorists” who suspect that they may have been under surveillance will willingly provide the biographical and biometric data that may lead to their apprehension. It is unlikely that the data given by “potential terrorists” who have no criminal record

and minimal contacts with terrorist organizations will generate a hit on the watch lists that are checked by US-VISIT. Undeterred, “established terrorists” are more likely to try to circumvent US-VISIT, either by fraud using stolen or fraudulent U.S. or Canadian travel documents or fraudulent Mexican border crossing cards, or by crossing between ports of entry.

Much depends on the intelligence, experience, and training of the terrorists. As some of the mistakes and risky behavior of some of the 9/11 hijackers indicate, terrorists, much like other criminals, are not always that smart. US-VISIT may succeed in catching a few of the less competent, but there are still simply too many ways to circumvent or deceive the system for it to be much more than a small part of border control authorities’ response to international terrorism.

The US-VISIT program completed its rollout at land borders at the end of 2005 and without any appreciable disruptions of traffic flows. It is important to keep in mind, however, that at land borders, enrollment in US-VISIT can be performed in secondary inspection because it is only mandatory for a relatively small percentage of those crossing land borders. Enrollment in US-VISIT is only required of those traveling on a regular visa, those entering under the Visa Waiver Program and, as of January 2009, legal permanent residents and several other categories of aliens. Enrollment in US-VISIT is not required of U.S. citizens, visa-exempt Canadian nationals,<sup>79</sup> or the seven million plus Mexicans with border crossing cards. In order to limit the impact on traffic flows, CBP officers at land border crossings will have discretion as to which permanent residents will be referred to secondary inspection and enrollment in US-VISIT (*Federal Register* 2006, pp. 42605-42611).

	Air	Sea	Land	Totals
U.S. Citizens	33.0	7.4	120.7	161.1
Legal Permanent Residents	4.4	0.2	75.0	79.6
Visa Waiver	13.0	0.3	1.8	15.1
Visa Exempt (Canadians)			52.2	52.2
Regular Visa	19.3	4.5	4.5	28.3
Mexican Border Crossing Card			104.1	104.1
Totals	67.9	12.4	358.3	440.4

If current entry rates follow recent historical patterns (see Table 1), a relatively small percent of those people entering the United States over land borders are being enrolled in US-VISIT.

Given exemptions from US-VISIT, it becomes very important to make sure that the Americans, Canadians and Mexicans who are exempted from US-VISIT are in fact who they say they are. In the past, U.S. citizens could simply make an oral declaration of citizenship to enter at land borders (this practice was ended in January 2008 by implementation of the Western Hemisphere Travel Initiative, see below). The inspector, using his or her judgment, could then allow the person to enter if satisfied with the totality of information available or ask to see a passport or other proof of citizenship, such as a birth certificate. For example, in 2004, I entered the U.S. from Canada as an automobile passenger. The driver told the inspector that we were U.S. citizens and I never spoke. The inspector did not ask the driver or me for proof of citizenship. Similarly, a daring English-speaking illegal migrant (or foreign terrorist) could declare U.S. citizenship to avoid biometric enrollment in US-VISIT and hope not to be asked for proof of citizenship. In 2004, there were 12,404 individuals making false claims to

<sup>79</sup> Canadian nationals entering the United States for short stays are exempt from most visa requirements and also from US-VISIT; however, those who are entering the United States on a visa are required to be enrolled in US-VISIT.

<sup>80</sup> Source: DHS 2003, p. 12.

U.S. citizenship who were intercepted by inspectors when their claims were challenged.<sup>81</sup> There are no available statistics for those, like the driver and myself, who entered with a declaration of U.S. citizenship that went unchallenged.

Another problem is posed by the 811,000 U.S. passports that have been reported to INTERPOL as lost or stolen (INTERPOL 2006). A somewhat less daring English-speaking foreigner could have acquired one of these U.S. passports and have his picture inserted then show the passport's outside cover while declaring U.S. citizenship at the border. If demanded by the inspector to verify identity and citizenship, the passport may, or may not, be detected as fraudulent. Although there were 12,599 fraudulent U.S. passports intercepted at ports of entry in 2004,<sup>82</sup> the DHS Inspector General concluded that those attempting to enter the United States with stolen passports are usually admitted, that reports of stolen passports on lookout systems made little difference, and that several blocks of stolen passports have been linked to Al Qaeda (DHS-OIG 2004).

Those who smuggle migrants through ports of entry conduct their own surveillance and know the realities of the inspection processes extremely well. If certain visa fraud schemes and the use of fraudulent foreign passports are foiled by the biometric screening of US-VISIT, travel documents that enable individuals to pose as U.S., Canadian, and Mexican citizens exempt from US-VISIT become much more useful and valuable to smugglers and terrorists. Passports with film photographs laminated onto the inside cover are easier to alter with substitute photos than current passports with digital photographs and are therefore much more valuable to smugglers. These older passports were issued until April 2002 and are valid for ten years. Tens of thousands of people attempt to enter the United States with fraudulent U.S. passports each year.

Although biometric data are collected at entry, there was no clear requirement for the collection of biometric exit data until the Intelligence Reform and Terrorism Prevention Act of 2004. According to the new law, "The entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data, regardless of the port of entry where such categories of individuals entered the United States."<sup>83</sup> This means that biometric exit data will need to be collected from not only the approximately thirty-seven million people who enter by air and sea with nonimmigrant visas, or under the Visa Waiver Program, but also those people who enter over land borders. It also means that those who submit biometrics to US-VISIT when entering by air or sea must also be able to submit their biometrics at land border exits. The Intelligence Reform and Terrorism Prevention Act of 2004 also requires that the DHS report to Congress on progress in developing a biometric exit process, the first of which was to be provided by June 2005. A December 2006 GAO report (GAO 2006) explained in detail that this progress report has yet to be made and that a viable plan for a biometric exit process is not yet in sight.

In sum, the deployment of US-VISIT has basically added collection of biometric data to the existing entry process and entry systems used. This has largely been accomplished by building interfaces between the legacy IDENT biometric system and Interagency Border Inspection System as well as the Consolidated Consular Database. Biometric data collection provides an additional obstacle to entry by impostors, increases the accuracy of watchlist checks and, especially with 10 fingerprint scans, may deter the entry of terrorists. Deployment of US-VISIT is limited to entry and enrollment is required of a relatively small percentage of all those who enter the US. Therefore, US-VISIT is far from the entry-exit system that was initially envisioned by Congress.

## 2.2.2 Secure Border Initiative (SBI) - Coverage of green/blue borders

The use of surveillance technologies for border security goes back to the 1970s and 1980s when the former Immigration and Naturalization Service (INS) began using low-light video cameras and portable electronic intrusion-detection ground sensors deployed at the border. In 1997, the INS developed the "Integrated Surveillance Intelligence System" (ISIS) which deployed motion, infrared,

---

<sup>81</sup> Source: INS Form G-22.1.

<sup>82</sup> Source: INS Form G-22.1.

<sup>83</sup> *The Intelligence Reform and Terrorism Prevention Act of 2004*, House Report 108-796, Section 7208 (d).



seismic and magnetic sensors and some 13,000 ground sensors were deployed by 2000. The seismic and infrared sensors can detect motion and heat within a 50-foot radius and the metal sensors have a 250-foot range. When combined with remotely controlled video cameras that have a five mile radius, border patrol agents can detect clandestine entries, train cameras on the illegal migrants and smugglers, determine their numbers and whether they are carrying weapons and then dispatch the appropriate patrols (Daté 2000). Nevertheless, the Integrated Surveillance Intelligence System was only deployed along 4% of the border with 10,500 sensors operative in October 2005 (GAO 2006a), many of the sensors have proved difficult to maintain in a variety of weather conditions and do not have an ability to differentiate animals from humans. If responded to by patrols, false alerts triggered by animals, end up diverting manpower. Alternatively, sensors may end up just counting illegal migrants and animals if Border Patrol staffing does not include a night shift, as was the case in certain sectors along the U.S.-Canadian border before September 11, 2001.

In August 2004, the Department of Homeland Security (DHS) established the America's Shield Initiative, which was to maintain and modernize ISIS and "integrate new, state of the market surveillance technologies (Aguilar 2005)." Internal negative evaluations of the initiative by DHS information technology staff and external Congressional criticism eventually led the then Secretary of Homeland Security, Michael Chertoff, to announce an overhaul of the short-lived America's Shield Initiative a year later arguing that DHS should not deploy "gadgets" along the border to detect illegal entrants but rather develop new technologies and strategies (Dizard and Lipowicz 2005). At the same time, bills in Congress called for an Integrated and Automated Surveillance Program "to establish a security perimeter known as a 'virtual fence' along such international borders to provide a barrier to illegal immigration."<sup>84</sup> Despite the fact that comprehensive immigration reform legislation failed to be enacted, the Secure Fence Act of 2006 mandated the building of 670 miles of additional physical barriers and "systematic surveillance of the international land and maritime borders of the United States through more effective use of personnel and technology, such as unmanned aerial vehicles, ground-based sensors, satellites, radar coverage, and cameras."<sup>85</sup>

The DHS replaced America's Shield with the "Secure Border Initiative" (SBI), a comprehensive multi-year plan which, among other things, involves: "a comprehensive and systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of UAVs, and next-generation detection technology (DHS 2005a)." In support of the initiative, U.S. Customs and Border Protection (CBP) launched a solicitation for the Secure Border Initiative Network (or "SBInet") contract, estimated at \$2.5 billion. After interested firms coalesced into teams, five teams headed by Raytheon, Lockheed Martin, Boeing, Ericsson and Northrop Grumman were invited to submit proposals from which the CBP selected the Boeing team in September 2006.

Although proponents maintain SBInet will reduce illegal migration, a virtual fence can be circumvented, bypassed or countered with decoys. The US Border Patrol apprehends 1 million illegal border crossers annually, on average over five years (DHS 2006, Table 36) but for each illegal crosser that Border Patrol Agents catch they say two or three get away (King 2006, p. H5027). Those who successfully enter the US, often after having been apprehended and returned several times, join the estimated 12 million illegal migrants, most of whom evaded Border Patrol Agents and are predominantly Mexican (Pew 2006).

Mexicans, however, can circumvent a fence on the US-Mexican border through Canada because Canada does not require visas of Mexican nationals. Mexicans can fly visa-free from Mexico City to Vancouver (\$500 roundtrip), get to the US-Canadian border and walk across. Mexicans who work illegally picking apples in Washington State have done this for many years. Fifty-five percent of the illegal border crossers apprehended at the US-Canadian border in 2005 were Mexicans (DHS 2006a). Once completed at an estimated cost of \$7.6 billion (Stana 2008, p. 7), the fence along the 1,989-mile southern border may not be very effective until DHS builds another fence on the much longer 5,525-

---

<sup>84</sup> *Comprehensive Immigration Reform Act of 2006*, S. 2611, section 754.

<sup>85</sup> *Secure Fence Act of 2006*, Public Law 109-367, Government Printing Office.

mile US-Canadian border or persuade the Canadian government to end visa-free travel from its NAFTA partner, Mexico.

If a virtual fence is erected along both southern and northern borders, it can be bypassed through the ports of entry. According to the DHS, *SBI* will drive illegal border crossers to ports of entry where Customs and Border Protection (CBP) officers “have the greatest tactical advantage (CBP 2006).” In 2006, CBP officers turned back 200,000 people but many migrants are still smuggled through ports of entry using fraudulent documents or hidden in vehicles (GAO 2007). Migrants pay smugglers additional fees of up to \$2,000 for such “express service” instead of crossing dangerous deserts and mountains (Dermota 2007). If the virtual fence drives current illegal border crossers to ports of entry, it will greatly increase inspections of travelers and vehicles. According to the Government Accountability Office, CBP officers already waive vehicles though without inspection and several thousand additional officers are needed to properly handle current flows (GAO 2007, p. 7). Smugglers know the weaknesses in CBP’s inspection procedures and train to take advantage of them. Unless staffing and infrastructure at ports of entry keeps up with increasing smuggling attempts, wait times will increase, as will pressure to move traffic through without thorough inspection and, thereby, enable smugglers to bypass *SBI*.

Even if *SBI* is fully deployed along all US land borders and CBP sufficiently staffs ports of entry to match increased smuggling, smugglers can counter the virtual fence with decoys. Much as the Soviet Union could build and deploy many more decoy nuclear warheads than the Strategic Defense Initiative (SDI) could ever completely shoot down, smugglers can hire Mexican nationals to cross the border, be detected by *SBI* and then tie up a sufficient number of the Border Patrol Agents dispatched to catch them so that others can be safely led across the border. Drug smugglers already use illegal migrants as decoys to divert Border Patrol Agents from the path of drug shipments (AP 2007). If illegal migrants are willing to pay an additional \$2,000 to be smuggled through ports of entry, they would pay for decoys to increase their chances of a successful crossing.

*SBI* deployment will increase smuggling fees, currently around \$2,000 - \$3,000 for crossing the US-Mexican border (Lee 2006). As long as illegal migrants can earn money in the US, higher fees may only marginally decrease migrants’ demand for smugglers’ services. Chinese nationals pay up to \$60,000 to be smuggled from China to the US, usually with a \$1,500 down payment and the balance paid back by working 80 hour weeks for several years and loan repayment backed up by enforcers’ threats of bodily harm (Chin 2001). A virtual fence will not significantly reduce illegal migration as long as those who manage to get past the fence can still finance smugglers’ fees and find jobs working illegally in the US.

The Secure Border Initiative has come close to achieving the Congressional mandate of building the 670 miles of new physical border fencing by the end of 2008 but legal proceedings and increased costs have slowed building. Likewise, the deployment of the virtual fence has been behind schedule and the systems deployed have not worked as expected. Given that Barak Obama voted for the Secure Fence Act, it is unlikely that either physical or border fence building will be immediately halted. Nevertheless, the program may be reconsidered given new budgetary priorities in light of the global financial crisis. In any event, even if billions of dollars continue to be appropriated to build the border fence, it is not clear that the fencing will work as intended.

Illegal migration may very well decrease in the coming years but this may have more to do with a collapse in the US construction industry, a long deep recession and increased enforcement of employer sanctions on the hiring of illegal migrants. Although it is beyond the scope of this report, it is important to note that DHS issued a rule requiring all federal contractors to use E-Verify for all new employees. E-Verify is an electronic employment verification system that supports internal enforcement of immigration laws by enabling employers to submit an employee’s data over the internet in order to receive confirmation of that person’s authorization to work in the US. In her confirmation hearings, incoming Secretary of Homeland Security Janet Napolitano emphasized that the Obama administration will refocus its efforts in combating illegal migration by prosecuting those employers who hire illegal migrant workers.

### 2.2.3 Visa Waiver Program Reform and ESTA

As international travel increased in the post-WWII era, many states eliminated visa requirements for nationals of other states on a bilateral reciprocal basis. For example, the US Visa Waiver Program (VWP) began as pilot program with UK and Japan in 1988 (and became permanent in 2000). The VWP permits travel to the US for purposes of business or pleasure for up to 90 days without a visa by nationals of states that similarly permit visa-free travel by US nationals, meet other program requirements and successfully apply to join the program. In 2007, 13 million nationals of 27 countries entered the US under the VWP.

After British national Richard Reid boarded a transatlantic flight in 2001 with only his passport and then tried to detonate a bomb in his shoes, members of Congress called for the elimination of the VWP. This it did not happen; partly because the building consulate facilities and hiring sufficient staff necessary to re-impose a universal visa requirement on the nationals of all states would be prohibitively costly and take a long time. In 2002, Congress opted to only change the program to require that nationals of member countries have biometric e-passports to enter the US.

The VWP came into the spotlight again in 2006 when UK officials uncovered a plot of over 20 British nationals of Pakistani origin, who planned to board US-bound flights and blow them up with liquid explosives. In 2007, the Director of National Intelligence testified that Al Qaeda is recruiting Europeans because they could travel to the US with just a passport. In response, members of Congress introduced legislation in 2007 to eliminate the VWP but then in August passed legislation to reform it.

Political pressure for reforms increased as US-EU visa policy asymmetries that grew through EU enlargement threatened visa-free transatlantic travel. Before the 2004 enlargement, the VWP included all EU member states except Greece. Member states could evoke a solidarity clause in the common EU visa policy, through which one country (e.g. Greece) could have treated US nationals on a reciprocal basis and required visas of them, thereby leading the entire EU to require visas of US citizens and bringing transatlantic visa-free travel to an end.

After the 2004 enlargement, only one of the new member states (Slovenia) was accepted into the VWP. US citizens enjoyed visa-free travel to all EU member states under its common visa policy but after the 2004 and 2007 enlargements, nationals of 14 EU member states did not enjoy visa-free travel to the US. EU officials argued that the US should allow visa-free travel to all EU citizens and the European Commission regularly reports on the lack of progress in attaining visa reciprocity. Nevertheless, the US resisted such arguments from Brussels and persisted in bilateral arrangements that bypass the EU's common visa policy.

Several Central and Eastern European states put US visa policy at the top of their bilateral foreign policy agendas with the United States. In response, President Bush conceded that Poland, the Czech Republic, Slovakia, Hungary, Romania, Estonia, Latvia and Lithuania should be allowed into the VWP because they joined the US in the "coalition of the willing" to fight the "war on terrorism" in Iraq and Afghanistan. Instead of eliminating the VWP or adding new states to the existing program, the Congress and President Bush agreed to reform it.

The VWP had required that the rate of refusal of the visa applications of VWP member state nationals must be less than 3%. The 2007 VWP reform legislation allows the DHS to consider applications to join the VWP of those countries with refusal rates of between 3-10% if these countries meet certain conditions such as: "actively cooperating with the US to prevent terrorist travel including sharing counterterrorism and law enforcement information."<sup>86</sup> On October 17, 2008, President Bush announced the expansion of the VWP to include the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Slovakia and South Korea effective on Nov. 17, 2008. The DHS then designated Malta VWP country effective on Dec. 30, 2008. The remaining "visa waiver road map" countries with

---

<sup>86</sup> *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law 109-367.

which the US is working to help qualify for the VWP include: Bulgaria, Cyprus, Greece, Poland, and Romania.

While relaxing the visa refusal rate criteria for membership enables expansion of the program, expansion was linked to two security measures: The DHS must certify “an air exit system is in place that can verify the departure of not less than 97 percent of foreign nationals who exit through airports of the United States and the electronic travel authorization system required under subsection (h)(3) is fully operational.”<sup>87</sup> In order for DHS to maintain authority to admit new countries into the VWP, must incorporate biometric capabilities in air exit system by June 30, 2009.

Electronic travel authorization systems such as that being developed to implement the VWP reforms were first pioneered by Australia in mid-1990s. Australia maintains a *de facto* universal visa regime whereby those travelers for whom a visa is not required must apply for and receive an Electronic Travel Authority. To receive an Electronic Travel Authority, those intending to travel to Australia electronically submit the biographical data on their passports either through travel agents or by themselves through a web portal. Automated watch list checks are executed and usually within minutes an Electronic Travel Authority is issued for travel to Australia or the applicant is referred to apply for a visa at an Australian consulate.

The US Electronic System for Travel Authorization (ESTA) system requires passengers or travel agents to provide biographical data of travelers (name, date of birth, passport number, etc.) at least 72 hours in advance of departure. The ESTA was launched August 1, 2008 after which one could enter biographical passport data on a voluntary basis on English language website. Starting Oct 15, 2008, it became available in additional languages. All VWP travelers have been required to use ESTA since January 12, 2009.

## **Intermediary conclusions on 2**

The “generation gap” between the Atlantic partners is clearly illustrated by the category of problems yet unresolved: while the EU still struggles for border basics, all the US seems to need in its far more accomplished situation is a slightly better fine-tuning of existing control mechanisms. It remains to see, within Part 3 of the report, to what extent the EU is ready and willing to perform the “great leap forward” to achieve a far-reaching convergence with the standards adopted by the US.

### **3. CONVERGENCE AHEAD? TENDENCIES OF TRANSATLANTIC APPROXIMATION**

The EU’s view going westward in order to catch up with the leader or at least reduce the gap, one should in the heat of the moment not forget that situations and solutions may not be altogether comparable. This would not only concern the legal prerequisites in terms of governmental structures which might indeed be incompatible or hardly compatible. Attention should also be paid to features such as geography which might have been decisive for the success of border tools currently in fashion such as the entry-exit concept born in Australia and therefore not necessarily fit for reproduction in less island-dominated situations.

#### **3.1 Closing the gap: The EU’s vision of an integrated border management in the 21st century.**

As we have noted in Part 2 above, the EU is on the move as well. Gone are the days when changes relating to border security had to be justified by compensatory necessities for Schengen. At the latest since the Amsterdam Treaty, the smooth working of the Area of freedom, security and justice was upgraded to represent a motive as such for adopting legislation, but for quite some time no real use was made of these new functions.

---

<sup>87</sup> Ibid.

While most of the existing measures as described in the "status-quo" part above (Section 2.1) still seem rooted in the former Schengen philosophy, newer initiatives such as the Commission "border package" of February 2008 clearly embodies the new approach. Whether one can agree with the proposals as such and their often security/LE-based visions is yet another question, but there is no doubt that they aim for comprehensive rather than fragmentary solutions. The paradigm shift is directly linked to the discussions of the "Future Group"<sup>88</sup>, which since early 2007 was busy preparing a new roadmap in EU home affairs matters to succeed the Tampere Conclusions (valid for the period 1999-2004) and the Hague Programme (2004-2009)<sup>89</sup>. Regarding border security, the ideas (and often the language) of the Future Group report presented in June 2008 are practically identical with those of the three Commission communications. The EP has so far not formally reacted on the content but pointed to the comprehensive Commission report expected for spring 2009 and to serve as the "basis for the following Parliamentary and Council deliberations"<sup>90</sup>. However, at this stage it already reminded one of the new legislative rules to be respected once the Lisbon Treaty enters into force<sup>91</sup>.

### 3.1.1 The Future Group's report of 30 June 2008

The Future Group has been criticised for imposing an exclusive "home affairs' vision" for a subject which would rather have deserved a multidisciplinary approach duly combining security and civil liberties aspects<sup>92</sup>. Such criticism seems confirmed by the controversial character of quite a few of the measures proposed as well as the outdated composition of the group based on a pre-Amsterdam perception of JHA matters. Besides eight representatives from Member States ministries, Council Secretariat and Commission, the Chairman of the EP LIBE Committee<sup>93</sup> was admitted just as an observer, certainly not a good basis for a balanced debate of subjects which, for a considerable part, fall under the remit of the 1<sup>st</sup> Pillar!

Although some of the major "buzzwords" cited<sup>94</sup> seem to have been dropped on the way from the discussion to the report stage, quite a number of highly controversial issues such as the proposed "Euro-Atlantic area of cooperation in the field of freedom, security and justice with the United States" or the "convergence principle" do remain and will certainly give rise to some intense debates in the time to come. In view of the complex subjects each time concerned, it is strongly regretted that the predominantly 3<sup>rd</sup> Pillar-oriented procedure chosen for the preparation of the 2009-2014 successor to Tampere and The Hague will exclude important players such as the European Parliament and the data protection authorities from a due involvement in the formal decision-making process. This once again shows how urgent it is to achieve the entry into force of the Lisbon Treaty!

In terms of border security, the FG report attracts attention under various headers.

As we have regretted the current lack of **coherence between the various national sectors** of the external border, some of the FG proposals relating to a closer interaction of national services would offer interesting perspectives<sup>95</sup>. Whether it is the closer cooperation between police and customs, the interlinking of national enforcement services e.g. by creating a common "corporate identity", joint ventures such as the Police and Customs Cooperation Centres (PCCCs) and joint investigation teams, the pooling of resources by joining forces in training matters, research, development and the purchase

---

<sup>88</sup> Informal High Level Advisory Group on the Future of European Home Affairs Policy, created on the initiative of the German presidency in January 2007

<sup>89</sup> It is expected that the new programme be formally adopted under Swedish presidency in the second half of 2009, see Carrera, S. and E. Guild (2008)

<sup>90</sup> see LIBE Opinion of 30.6.08 (European Parliament 2008d)

<sup>91</sup> *ibid*

<sup>92</sup> Bunyan (2008)

<sup>93</sup> until January 2008 MEP Jean-Marie CAVADA, since then MEP Gérard DEPPEZ

<sup>94</sup> such as the upgrading of Europol to a "real European criminal police", "Interior Ministries giving themselves an EU internal security policy", "permanent European Reinforcement Teams to be stationed in Libya/Chad", system of pre-border checks", see Bunyan (2008), p.8, 10

<sup>95</sup> Future Group (2008), Chapters I,II,III

of equipment, all this would definitely strengthen the coherence and help to eliminate frictions and particularistic tendencies between the many services/administrations involved at the national as well as European level. Another aspect is the proposed codification of the relevant EU legislation which will not only provide greater transparency in favour of citizens but also facilitate implementation by authorities at the national and local level<sup>96</sup>.

Such promotion of a “federal” tendency in the management of the external border is of course exposed to questions and criticism, notably under the aspect of traditional primacy of Member States in this field. However, as we have seen above, positions are slowly shifting towards a more pragmatic approach. As has been pointed out elsewhere in more detail, it is not easily comprehensible why many core policy areas such as monetary matters and higher education have been to such a large extent been “re-organised/revolutionised” by EU involvement while police and border matters should remain an absolute taboo for the Union<sup>97</sup>.

An entirely different aspect lies in the “enforcement-driven” character of the initiative as currently proposed. Greater coherence does not necessarily mean arbitrary police interaction in the sense of an uncontrolled information exchange (“principle of availability”) or other forms of cooperation which could indeed prove counterproductive. The decisive factor lies in the democratic control which is currently lacking in those areas still under the aegis of the 3<sup>rd</sup> Pillar. This means that help is not so far away; once Lisbon enters into force, most of the subject areas concerned will become subject to the mainstream decision-making and thus due democratic control by Parliament, Court of Justice and data protection authorities. In anticipation of this event, the EP already requests that all legislative proposals be postponed which are non-accomplished by 1 January 2009 and fall under the co-decision regime<sup>98</sup>. Prominent examples of such postponement should first all be the proposed framework decisions on (1) the use of Passenger Name Record (PNR) for law enforcement purposes and (2) the protection of personal data in the framework of police and judicial cooperation in criminal matters<sup>99</sup>.

Another group of issues suggested by the Future Group under the header of “**New technologies and information networks**”<sup>100</sup> needs to be considered with great care. This subject situated between the citizens’ fear of what is called „the digital tsunami“ and the need of law enforcement agencies („public security organisations“) to operate a sufficiently yielding information exchange to successfully counter crime risks.

Mastering the „tsunami“ in the interest of citizens is indeed a highly important and laudable undertaking<sup>101</sup>, but also a task so complex that law enforcement authorities alone appear clearly overburdened by it. Especially as they want to tackle the “tsunami” in a double, even contradictory sense, ie combat it in favour of society and, at the same time, exploit it for purposes of crime control. Technical as well as legal devices such as the “EU JLS Law Enforcement Information Management Strategy (EU IMS)” proposed to master this delicate situation in combination with the “principle of availability”<sup>102</sup> may represent valid solutions, however, this hard to judge from just a summary description. The same applies to other suggested mechanisms such as PETs (privacy-enhancing technologies) or “privacy by design”<sup>103</sup>, the Common Requirements Vision (CRV) to be contributed by the Police Chiefs Task Force and the “European Security Tool Pool”, apparently for testing purposes. All this is very confusing already from a linguistic-technical point of view.

---

<sup>96</sup> although part of the “Better regulation” strategy agreed between the EU institutions as early as 2003, this reminder is welcome as the process tends to get stalled due to the volume of legislation, number of languages etc (see „Codification and recasting” [http://ec.europa.eu/governance/better\\_regulation/codif\\_recast\\_en.htm#\\_issue](http://ec.europa.eu/governance/better_regulation/codif_recast_en.htm#_issue))

<sup>97</sup> see Hobbing (2008a), pp. 253ff

<sup>98</sup> EP (2008d), p.6

<sup>99</sup> *ibid.*

<sup>100</sup> Future Group (2008), Chapter V, p. 43

<sup>101</sup> Guild, E., K. Groenendijk and S. Carrera (2008)

<sup>102</sup> Future Group, p. 45

<sup>103</sup> Aside the specific FG problematic, the development of PET and privacy by design as such are seen as a highly positive venture, see Guild, E., K. Groenendijk and S. Carrera (2008), s. 8

According to lessons learned elsewhere last but not least in the US, we know that, especially in the security sector, the risk of vital errors increases with the number of co-existing and mutually interlinked IT, database and management systems involved<sup>104</sup>. This is all the more true where “machines” do not just “automated monitoring and analysis”, but take autonomous decisions without human input in terms of a final review by an inspector. This should be taken as an urgent advice to avoid any legislative decision-making without due consultation of data protection experts who would at the same time examine the necessity, effectiveness and proportionality of the measures proposed. As well as the added value of any interoperability/synergy solutions. Their expertise should, in particular, be consulted for the still pending proposal for a Framework Decision on data protection.

Last but not least the FG proposes some measures of far-reaching impact for the **external dimension of Home Affairs Policy**<sup>105</sup>. This concerns three subjects in particular. There is first of all the phenomenon of an “increasing blurriness of internal and external security”<sup>106</sup> requiring closer cooperation between home affairs, external relations and also the military, secondly the objective for FRONTEX to conduct search and rescue patrols also in the territorial waters of third countries<sup>107</sup>, and finally the very ambitious plans for closer cooperation with the US under auspices of a „**Euro-Atlantic area of cooperation with the United States in the field of Freedom, Security and Justice**“<sup>108</sup> and a „common transatlantic space with more sharing of relevant information and at the same time greater protection of personal data“<sup>109</sup>. All these items are of a highly delicate character and certainly require a well-balanced approach between all interests involved, in particular as regards human rights.

Although the FG report does not expose the objectives in question in sufficient detail to engage in a substantive discussion, it seems worth to recall already at this stage the disillusioning negotiations recently led with the US in PNR matters. These have abruptly highlighted the enormous differences in approach when tackling clashes between security and civil liberties issues<sup>110</sup>. The lessons learned at that occasion make it difficult to believe, that one can reasonably expect to bridge the existing gaps and achieve such an “area of cooperation” which can exist only on the basis of a consensus on the fundamental values.

In view of the still uncertain significance of the FG report for concrete EU policy-making, we shall not further expand on the remaining elements of the FG report; some of them relating to FRONTEX, Eurosur and the global revision of the border systems will be dealt with in the following section under header of the Commission border package where they have been exposed in more detail.

### 3.1.2 The Commission border package of February 2008

Although the “Border Package” contains concepts elaborated in more detail than those proposed by the Future Group, one has to be aware that these, too, are nothing more than visions of the future not yet underpinned by any legislative basis or even firm political commitment. Some of the commentators have therefore abstained from a profound discussion of the more hypothetical passages, especially those in the FRONTEX and Eurosur communications<sup>111</sup>. We will proceed in a similar manner and mainly concentrate on the items more fully developed.

---

<sup>104</sup> this applies in particular to the US-experience gathered by DHS with a rapidly changing sequence of database and profiling systems employed between 2001 and 2007 (Hobbing, 2008, pp. 13-15)

<sup>105</sup> Future Group (2008), Chapter VI, p. 48

<sup>106</sup> *ibid* paras 1,75

<sup>107</sup> *ibid* para 118

<sup>108</sup> *ibid* paras 50,71

<sup>109</sup> *ibid* para 168

<sup>110</sup> Hobbing (2008), pp. 40-49

<sup>111</sup> EDPS (2008)

NB. For easier comparison, it is noted that, with the border package, the Commission moves into a terrain which in the US is covered by the programmes US-VISIT (entry-exit system), ESTA (Electronic travel authorisation) and SBInet (surveillance of green/blue border).

### 3.1.2.1 “The next steps in border management” (EU Commission 2008c)

If Commission communications are sometimes compared to non-operational “trial balloons” to test whether the time is ripe for launching certain initiatives, the “next steps” text has certainly fulfilled its purpose. Reactions were numerous, although it seems the majority of them were hesitant if not critical of the objectives pursued and measures proposed.

The communication is future-oriented, not only because its time-frame for implementation is not yet determined (possibly post-2012?) but also because it addresses new horizons in technical and organisational terms.

The Commission argument is built around a psychologically forceful combination of undisputable security needs and (allegedly) attractive facilitation incentives. Well-known/serious border threats stemming from terrorism, organised crime, illegal migration etc leave no choice but to scrupulously apply the Schengen Border Code<sup>112</sup> with all its painstaking formalities. Although regrettable, the interests of tourists and an economically important travel industry must thus stay behind, unless – and here come the good news ... - one takes advantage of the benefits of modern technology which would allow to miraculously reconcile both concerns.<sup>113</sup>

The approach builds on three features: (1) facilitation measures for “bona fide” travellers, (2) introduction of an entry/exit system and (3) introduction of an Electronic System of Travel Authorisation (ESTA).

#### **(1) Facilitation for “bona fide” travellers**

The proposed benefits would include (a) simplified checking methods for the traveller concerned by means of biometric identifiers and automated gates, and (b) increased cost-effectiveness for the border authorities involved as more passengers could be processed by less staff. But the benefits also have their price for (a) the travellers by means of extensive pre-screening procedures including the collection of biometric identifiers (facial image and fingerprints) - just as for visa holders, and (b) the border authorities in terms of “considerable purchase and maintenance costs”<sup>114</sup> for installing the necessary equipment at border crossings etc. Beyond 3<sup>rd</sup> country travellers subject or not to visa requirements, the “bona fide” approach would also be open to EU citizens<sup>115</sup>. thus building upon national “Registered/Trusted Traveller” programmes existing at numerous European airports (e.g. Amsterdam-Schiphol, London, Frankfurt).

From a critical point of view, comments point to the doubtful benefits of the “bona fide” treatment as rarely would encounter obstacles<sup>116</sup> and moreover the disadvantage that the new measure would require the collection, processing and storage of considerable amounts of personal data, involving all the extensively known risks for privacy<sup>117</sup> which should by all means be duly examined before system is installed.

It should also be noted, however, that bona fide programmes seem to enjoy quite some popularity on both sides of the Atlantic as recent surveys show: average time gains in terms of 2 instead of 15

---

<sup>112</sup> Regulation (EC) No 562/2006

<sup>113</sup> EU Commission (2008c), p. 5

<sup>114</sup> Carrera, S., F. Geyer and E. Guild (2008),

<sup>115</sup> EU Commission (2008c), p. 7

<sup>116</sup> *ibid*

<sup>117</sup> EDPS (2008), p.2



minutes waiting time<sup>118</sup> seem a sufficient reason for travellers not only for submitting their personal data but also pay accession fees of up to 150 Euro per year<sup>119</sup>.

## (2) Entry/exit system

Starting from the concept/technology envisaged for the “bona fide” programme, the Commission could also think of establishing by 2015 a register recording all entry or exit movements of 3<sup>rd</sup> country nationals admitted for a short stay (up to 3 months): this is seen as a handy tool to (a) identify visa-overstayers, (b) deter potential overstayers and (c) provide operational data on patterns of overstaying, migration flows and overstayers for visa purposes. There are indications that the proposed system should also serve the purposes of the fight against terrorism and serious crime<sup>120</sup>.

A smoothly working entry-exit system certainly represents an attractive vision, allowing the authorities in charge to closely monitor “who is in and who is out”, just like a “hotel manager” who wants be sure about the guests checked in at his place<sup>121</sup>. Actual overstayers could be flagged via an “alert” issued to national authorities automatically after expiry of the visa.

However, ambitious projects of such a dimension also have to face a number of pertinent questions, all the more when they essentially rely on the mass processing of personal data. Question number one would by all means relate to the **feasibility of the new system** and the results it is likely to produce. An EU entry-exit system is impossible to implement with current entry data retention policies of several states. For example Germany, Austria and Slovenia do not retain entry data after a watch list check is completed.<sup>122</sup> Therefore, there is no entry record against which an exit record can be matched. Every EU (Schengen) member state would have to retain entry data to match with exit data that might be collected upon exit from that state any other EU (Schengen) member state. Moreover, data protection authorities would in first place enquire into the necessity and expected effectiveness of such privacy-invading measure<sup>123</sup>.

In view of the enormous costs expected, especially for (a) the additional enrolment of 3<sup>rd</sup> country nationals not subject to a visa requirement, (b) creation of an appropriate database (part of VIS or separate system?) for storing entry-exit data, (c) roll-out of the system and its equipment to every single border crossing point (BCP), critical remarks concern the following aspects:

- Lack of a masterplan to reasonably structure the various initiatives taken on the surveillance of individuals. The acceleration of proposals in this field make it difficult to have a full overview.
- Lack of reliable evidence supporting the need/efficiency of the system. So far arguments are just based on estimates/samples or “bold statements” (EDPS 2008: 3), also there seems to be no immediate consequence for overstayers, once the “alert” is activated (Guild, Carrera and Geyer, 2008: 3)
- No exploitation of comparative experience gained in other parts of the world (in particular Australia and USA). As can be seen from parts 2.2 and 3.2 of this report, the US entry-exit system is far from being complete despite intense efforts and strong budgetary input for many years<sup>124</sup>.

---

<sup>118</sup> see Travel news <http://www.thetransnational.travel/news.php?cid=international-registered-traveler.Apr-08.24>

<sup>119</sup> price for a Privium Plus membership at Schiphol Airport in the Netherlands  
<https://www.schiphol.nl/web/show/id=67508/langid=42>

<sup>120</sup> EU Commission (2008d)

<sup>121</sup> According to the statement of a senior official at the European Commission

<sup>122</sup> Rey Koslowski’s interviews with German, Austrian and Slovenian border guard officials in Spring 2006.

<sup>123</sup> EDPS (2008), p. 2

<sup>124</sup> see also Hobbing (2008), pp. 52f

- Lack of a coherent basic concept. In view of the many mandatory or optional exemptions the EU law foresees from the normal entry/exit formalities (e.g. local border traffic), it is difficult to see how a “watertight” recording system may be implemented (Peers, 2008: 3ff).

This situation should be reason enough to closely look into the matter before any decisions are taken. Probably postponement of the legislative procedure until the entry into force of Lisbon would be desirable to ensure that all aspects are being duly considered, especially under the angle of data protection.

### **(3) Electronic System of Travel Authorisation (ESTA)**

Since the Communication spends just one single paragraph on the issue of ESTA, while referring to a study to be undertaken by the Commission and available by 2009, we are currently lacking sufficient elements for giving a reasoned opinion.

However, from the details available, there might be concerns about the compatibility of the travel authorisation requirement with the international asylum system: pre-border mechanisms like ESTA make it harder for victims of persecution to reach safe havens.<sup>125</sup>

#### *3.1.2.2 “Future development of FRONTEX” (EU Commission 2008a)*

The proposed development of FRONTEX continues to follow the moderate step-by-step strategy employed during the first years of its existence. Nevertheless progress is visible and the orientation pursued seems well chosen to consolidate the management of the external border in view of more coherence.

Based on the conclusions drawn from the 2005-2007 period, the communication contains some punctual proposals designed to fill specific loopholes such as the following:

- mandate for FRONTEX to acquire its own equipment for maritime operations including RABITs, given that Member States did not fully comply with their commitments under the CRATE/RABITs mechanisms
- establishment of specialised branches of FRONTEX to be located in particular in the Mediterranean region closer to the operational area
- cooperation regarding joint risk analysis with Europol, international organisations, third countries

Long-term visions would include “horizontal integration” in the sense of closer cooperation with customs and other border-related agencies (an aspect which had been persistently neglected at EU level), as well as the permanent assignment of border guards and equipment (rather than a temporary deployment as operated until now).

These changes confirm the impression that FRONTEX is well on its way to provide the external border with a more “federal image” and gradually straighten out inconsistencies between diverse national management and operational approaches. Besides expert advice and budgetary support, FRONTEX’s growing influence is also based on an instrument of pressure, i.e. the explicit hint that in case of unsatisfactory progress in integration efforts (such as RABITs), the Commission would intend to “return to the question of a fully fledged European Border Guard” (EU Commission 2008a: 10). This strategy is also supported by the European Parliament (EP 2008e) which encourages the Commission to strengthen its [FRONTEX’s] role and make it more effective following the objective of a “truly EU integrated border management”.

At the same time, additional efforts need to be made to “meet international human rights standards and a duty towards asylum seekers in rescue operations at high sea (ibid<sup>126</sup>), in particular in view of FRONTEX’s role as a fully-fledged Community body.

<sup>125</sup> see EUobserver of 13.2.2008 <http://euobserver.com/9/25650>

### 3.1.2.3 “European Border Surveillance System EUROSUR” (EU Commission 2008b)

Again in the perspective of a truly EU integrated border management, the EUROSUR communication proposes 3 implementation phases for in the period before 2013. While the future system in the end should cover the surveillance of land and sea borders (i.e. the “green” and “blue” border stretches outside official crossing points), its current focus is primarily on the southern maritime borders.

Although each of the 3 phases targets different levels of achievement, they all undertake to strengthen not only the surveillance apparatus at the border but incidentally also the role and competences of FRONTEX. While Phase 1 intends to interlink existing national surveillance systems. Phases 2 and 3 both imply the “development and implementation of common tools at EU level”, whereby Phase 3 adds an important feature, a “common monitoring and information sharing environment for the EU maritime domain”.

From a feasibility point of view; Phase/option 1 appears problematic in view of the doubtful interlinking capacity of national systems, which have been developed separately and are often not even linked at the national level.<sup>127</sup> It would therefore appear more likely that the attention be immediately drawn to the last two options, probably even Phase 3 which would give FRONTEX a direct operational input (hub for sharing of information and intelligence gathered by border surveillance).

The implementation of information/intelligence hub with operational involvement of FRONTEX would require two important changes in FRONTEX’s legal bases, ie the amendment of Regulation (EC) 2007/2004 to cover the new operational remit and foresee appropriate safeguards for the correct processing of data, to be identified with the due involvement of data protection authorities.

As an overall impression, EUROSUR just as the other projects proposed under the border package contributes to the design of a future European border scenario with a strong input from the central EU level and thus more comparable to the structures existing in the US.

### 3.1.2.4 European PNR System on the use of air passenger data (PNR) for law enforcement purposes (EU Commission 2007)

When comparing the current/planned EU-border devices with those of other partners around the world, the only major item definitely missing is that of a European PNR system. Although the EU already serves the systems of countries such as USA, Canada and Australia on the basis of bilateral agreements, the corresponding EU proposal for such mechanism is pending since November 2007. And according to the latest developments, things seem to go backwards rather than advance.

In July 2008, the Council decided to abandon the original Commission proposal and follow specific concerns expressed by Member States: what is currently in sight corresponds to a patchwork solution rather than a coherent EU system.

To suit divergent opinions/needs, the new instrument would each time cover the various options<sup>128</sup>:

- in principle, collection of passenger data from all air travel between the EU and third countries; however, with the option that Member States extend the system to other modes of transport (sea, land) and to internal EU flights
- in principle, collection of data for the purpose of counter-terrorism and fighting serious crime, but also covering “other offences brought to light during controls”

---

<sup>126</sup> see also Jeandesboz (2008: 16)

<sup>127</sup> also Jeandesboz (2008: 15)

<sup>128</sup> EU Council (2008)

- decentralised management of the system by national Passenger Information Units (PIUs)
- checking of data not only against international and European but also against highly divergent national watchlists.

This unfortunate project suffers also from yet other inconsistencies which further reduce the added-value to be expected from its adoption. Privacy authorities as well as the European Parliament object to highly imprecise purpose descriptions diverging from international standards insofar as they include not just actors but also “associates” of the crimes in question. It is based on 3<sup>rd</sup> Pillar legal bases which exclude EP and privacy authorities from involvement in the decision-making process.

It would therefore appear unlikely that the proposed instrument will contribute to an adequate protection of the external border. It rather appears as a regression into old particularistic patterns, just as if all New England states would apply different criteria when checking passengers from abroad.

### **Intermediary conclusions for Part 3.1**

Did the EU after all succeed in closing or at least narrowing the gap? The answer is yes and no. No insofar as European border structures have not come anywhere close to US to the extent of US border security system development, nor are they likely to achieve this aim within the next few years. Too different were the starting points, an established monolithic state structure there and an emerging union here with a yet unfinished internal organisation and undetermined external confines.

Nevertheless the past few years have brought about an important shift in tendency comparable to the transposition manoeuvre of a big ocean liner: while in the past border security (together with police and criminal justice matters) was largely out of reach for systematic EU intervention, the EU legislator to directly focus its action on the border, i.e. to protect the AFSJ against any negative impacts from the outside. This influence materialises not only in form of legislation regulating the conditions under which the external border may be crossed (Schengen Border Code and related instruments), but also by the large scale IT-systems which increasingly tend to go beyond their initial Schengen purpose aiming for coherent safeguards and ultimately a US-style entry-exit system. Above all, with creation of the FRONTEX agency, the EU also managed to make its entry into operational border security as the former stronghold of national Member States influence.

While for a final evaluation of the new EU approach the latest US developments have to be taken into account, it is interesting to note already at this point to what extent the reforms envisaged by the Future Group as well as the Commission Border Package mirror existing US (and partially Australian) models. The proposed entry-exit system has been inspired by US-VISIT, the Electronic Travel Authorisation scheme ESTA find its counterpart in an US system bearing exactly the same name and many technology features suggested by EUROSUR may be traced to the corresponding US surveillance programme SBInet, notably as regards the concept of a “virtual fence”.

## **3.2 US strategies to counter remaining weaknesses/loopholes**

### **3.2.1. Western Hemisphere Travel Initiative (WHTI)**

The 9/11 Commission recommended ending the so-called “Western Hemisphere exemption” that allows U.S., Canadian and Mexican citizens to cross U.S. land borders without passports in order to eliminate the security loophole whereby individuals entered the US without having travel documents such as passports inspected. Families of the 9/11 victims pressured Congress to enact these recommendations and the resulting Intelligence Reform and Terrorism Prevention Act of 2004 requires that everyone, including U.S. citizens, be required to have a valid passport or other designated documentary proof of citizenship in order to enter the U.S. beginning January 1, 2008. Members of Congress, particularly from border states, began to argue against the passport requirement, contending

that it would impose too great a burden on Americans who have been able to travel to Canada and Mexico without the costs of getting a passport; that the 74% of Americans who do not have a passport would choose not to travel to Canada and Mexico and millions of dollars of cross-border economic activity would be threatened. Senators Patrick Leahy and Ted Stevens added an amendment to the Department of Homeland Security appropriations bill that succeeded in delaying the deadline for implementation of this requirement until June 1, 2009. Nevertheless, in January 2008, the DHS did end the practice of allowing US citizens to enter on the basis of an oral declaration at land borders and requires proof of identity in the form of a government issued identification document (e.g. drivers license) and proof of citizenship (birth certificate). The DHS implemented the WHTI requirement for a passport or other WHTI compliant travel document for arrival by air and sea and plans on implementing the requirement for entry at land border crossing points by June 2009.

Given the WHTI requirement that U.S. citizens present a passport or other proof of citizenship, the State Department and DHS developed the People Access Security Service (PASS) card, an alternative, less expensive wallet-sized biometric passport card for use by U.S. citizens to cross the U.S. land borders with Canada and Mexico. The new PASS cards are to have Radio Frequency Identification (RFID) chips that can be read 30 feet away and will transmit a unique number. This number will trigger retrieval of the individual's passport data, enable automated watch list screening and this information could be pulled up on the inspector's computer screen as the vehicle arrives at the inspection booth (DOS 2006).

Inspection of an RF-enabled PASS card would clearly be faster than inspecting existing passports of all U.S. citizens, however, travelers would still have to stop at the border and inspectors would have to visually verify that the person in front of them matches the passport photo.

### 3.2.2. Building border crossing infrastructure

As Geronimo Gutierrez, the undersecretary for North America at the Mexican Secretariat of External Relations, put it, "We have pre-NAFTA infrastructure at our borders."<sup>129</sup> With new data collection requirements in addition to increasing trade and travel flows, it may become impossible to process visitors and shipments without backing up traffic unless larger secure areas at border crossings are cleared for inspection lanes and booths and more bridges and tunnels are built, especially between the Canada and the United States. Even without the new requirements of US-VISIT, many land ports of entry do not have sufficient space for current operations. Indeed, sixty-four ports of entry have less than 25 percent of the space they require.<sup>130</sup>

The challenge of implementing the entry process of US-VISIT at land borders is evident at the country's busiest border crossing, where there would be a significant impact if the percentage of entries requiring US-VISIT were significantly increased beyond single digits. According to a DHS official, on an average day at the San Ysidro, California, port of entry, 53,000 vehicles with drivers and 80,000 passengers enter through twenty-four inbound lanes, together with 20,000 to 30,000 pedestrians, for a total of about 150,000 entries. This official flatly stated that if enrollment in US-VISIT took place in primary inspection and added only ten seconds to each individual crossing, it would "kill operations" and lead to unsustainable backups. Similarly, a stakeholder from the Detroit-Windsor area said that the addition of ten to fifteen seconds to the processing of every driver and passenger entering the United States over the Ambassador Bridge would "shut down the bridge." There were no shutdowns when US-VISIT was deployed at San Ysidro and the Ambassador Bridge at the end of 2004 because enrollment of US-VISIT was accomplished in secondary inspection and

---

<sup>129</sup> Geronimo Gutierrez, "Remarks by Germonimo Gutierrez, Mexican Secretariat of External Relations," *North American Integration: Migration, Trade, and Security* Institute for Research on Public Policy, Ottawa, April 1-2, 2004.

<sup>130</sup> "Data Management Improvement Act (DMIA) Task Force Second Annual Report to Congress," Department of Homeland Security, 2003.

required of only a very small percentage of those who entered, and most of these people were already going to secondary for I-94 form processing.

At most land border crossings there are currently no facilities for outbound inspections. The existing exit data collection at land borders involves those traveling on visas and under the Visa Waiver Program depositing their I-94 forms in drop boxes when they leave, usually at CBP secondary inspection locations on inbound lanes. At San Ysidro, the Detroit-Windsor Tunnel, and the Ambassador Bridge there was no clear signage on outbound lanes instructing an exiting foreigner who wanted to submit his or her I-94 form where to go to deposit the form. At those border crossings in urban areas, the outbound lanes often have very little, if any, room to pull over and park. A persistent, regulation-obeying individual would have to locate and interrupt a CBP officer to find out what to do with the form, and the most visible officers are those working the inbound lanes. At some crossings into Canada—at the Ambassador Bridge, for example—Canadian inspectors will take I-94 forms given to them and send the forms back across the border to be added to the drop box collection. Contactors then enter the information written on the forms into a database, which can be compared to entry records in the Arrival Departure Information System (ADIS), a legacy system component of US-VISIT.

Although there are currently no exit controls at most U.S. land borders, one could envision exit controls at land borders that would mirror entry controls with the construction of additional lanes and booths, the installation of biometric readers and workstations, and the hiring of inspectors to process departing foreigners and record exit data for US-VISIT. The DHS estimated that the cost of infrastructure improvements necessary for the final increment of US-VISIT would be approximately \$2.9 billion. This figure, however, assumes that no additional lanes would be required for entry and that exit lane requirements would be the same as those for entry (Hite 2004). Given the prospects for increased average crossing times and declining throughput at entry discussed above, this is a rather heroic assumption.

At some border crossings such as the Detroit-Windsor Tunnel, there is little room for secondary inspection of outbound traffic and for additional exit lanes that accommodated primary inspection booths for collection of exit data. Even if only a few vehicles were to be stopped at exit stations, especially at peak traffic times, rows of departing vehicles would quickly back up into the main streets of downtown Detroit. In order to implement a secure exit process, it would be necessary to expand the number of lanes and to build exit booths. The economic stimulus package passed by the US House of Representatives on January 29, 2009 includes “Border Ports of Entry: \$1.15 billion to construct GSA and Customs and Border Protection land ports of entry to improve border security, make trade and travel easier and reduce wait times, and to procure non-intrusive inspection technology at sea ports of entry, which is used to scan cargo containers to reduce the risk that containers can be used to smuggle weapons of mass destruction.”<sup>131</sup> However, there are limitations on expanding the physical infrastructure of approaches to bridges and tunnels within the time frame envisioned for the implementation of US-VISIT. If similar legislation is passed by the Senate and signed by President Obama, it may ease the congestion at land border crossings resulting from increased security requirements, nevertheless, given that GAO estimates for necessary border infrastructure improvements to fully implement US-VISIT are almost three times this amount, this appropriation can only serve as a stop gap measure.

### 3.2.3. Radio Frequency Identification (RFID)

The DHS had great hopes for using RF technology to expedite travelers through border controls at land border crossings and avoid building extensive exit control infrastructure as well as adding staff. RF-enabled exit controls at land borders that did not include a primary inspection by a DHS officer might save billions of dollars but if US-VISIT were to depend upon RF-enabled exit controls, it may be next to impossible for US-VISIT to achieve its objectives of determining whether someone has

---

<sup>131</sup> *American Recovery and Reinvestment Act of 2009*, HR 1.

overstayed or should be apprehended when leaving because there are limits as to what processes can be securely automated in the collection of exit data. An RF-based exit system may record the exit of an RF-enabled travel document, but one can only be certain that the person exiting with the document is the same person who entered with that document if that person is physically checked against the picture on the document and the biometric on the chip.

According to the US-VISIT Request for Proposals (RFP), “As foreign national travelers leave the United States, their exit will be recorded and, if warranted based on watch list screening results, immediate detention action will be taken. Entry and exit records will be matched and visa compliance will be determined and maintained along with travel history (DHS 2003, p. 9).” The RFP further states, “The Government intends to deploy RF capability at vehicle lanes and use this technology to record biographic entry and exit data for RF-enabled vehicles/passengers (p. 118).” It also states, “The Contractor’s exit solution cannot assume that vehicles can be stopped in traffic lanes (p. 121).”

The DHS piloted an RFID system at five land ports of entry (Nogales East and Nogales West in Arizona; Alexandria Bay in New York; Pacific Highway and Peace Arch in Washington) in 2005. The pilot projects used automatic identifiers (a-IDs) to register exits and the process tested went as follows: When a foreign national enters at one of the pilot land ports of entry, he or she goes to secondary inspection to submit biographical and biometric data for I-94 processing and is issued an a-ID. The a-ID has a number that is linked to a database with the traveler’s biographical and biometric data. No biographical or biometric data are stored on the a-ID itself. The system then registers entries and exits of the traveler with the a-ID when crossing in a vehicle. Pedestrian entry also includes real-time biographic watch list checks. In a second phase of system deployment, a-ID crossings were to pull up biographic and biometric data for vehicle primary inspection (DHS 2005b, p. 3). In order for such a system to operate, CBP would need to install RF readers over all exit lanes. The RF readers appear to be similar to those used for EZ-Pass and other automated toll systems, some of which now read RFID tags on cars passing by at fifty-five miles per hour. The GAO reported that the US-VISIT pilot system’s ability to read the a-ID in the I-94 form of those exiting, whether by car or on foot, did not reach target ranges, often by very large margins (GAO 2006, Appendix VII, Table 5, p. 85). If drivers and passengers placed their I-94 forms against side windows of vehicles, read rates did improve. Shortly after the GAO issued its report the pilot projects were terminated.

It is hard to envision how an RF system could automatically “check out” holders of automatic identifier cards and RF-enabled biometric passports as they drive through exit lanes and be able to determine whether the person leaving is the same person who arrived. For example, a criminal or terrorist could overstay his visa but be registered as having “checked out” by paying a Canadian national to take his RF-enabled a-ID and exit the United States as a passenger of a car driven through the exit lane into Canada.

To deal with this problem, DHS officials have suggested that a wireless biometric card could be used. As individuals are enrolled in US-VISIT upon entry they would be given an RF-enabled entry-exit card with a wireless fingerprint reader that could transmit a live read of the individual’s fingerprint as the person exited so as to verify that the person did indeed leave with the entry-exit card (Jacksta 2004). As drivers and passengers subject to US-VISIT exit requirements cross the land border out of the United States, they would put their finger on the finger scan section of the card as they pass under the RF readers. The reader would collect the data transmitted from the card and the digitized finger scan biometric. The biographical data would be used to register an exit to correspond to the individual’s entry and the finger scan biometric would be matched to the finger scan collected upon enrollment to verify the identity of the individual exiting.

Even if such an RF-enabled exit process can be developed, there is major problem with its practical application. Acquiring a readable fingerprint scan often involves careful placement of the finger on the reader and takes several tries. If the fingerprint is not properly read and transmitted and the exit is not recorded, the departing visitor risks being denied entry to the United States in the future. Unless

there is some way of transmitting a signal that the finger scan has been read and the data received, people may think that their exits were registered when they in fact were not.

The proposed RF-enabled exit process would also be very susceptible to deception by those who wish to register an exit but then overstay their visas. A finger scan reader on a wireless entry-exit card is much more susceptible to “spoofing” than enrollment in US-VISIT at ports of entry. There have been several experiments showing that finger scan readers can be spoofed with fake fingers made of gelatin and other materials (Van der Putte and Keuning 2002). Someone could make a fake finger (following instructions readily available in articles on the Internet) and have someone drive it over the border while pressed on the finger scan reader of the wireless entry-exit card. Antispoofing techniques include supervised enrollment, enrolling several biometric samples, e.g., two or more fingers instead of one, and multimodal biometrics, e.g., facial and fingerprint (Schuckers 2002). Enrollment in US-VISIT at ports of entry employs all three anti-spoofing techniques while the proposed wireless biometric reader solution utilizes none.

Even if a criminal or terrorism suspect attempted to exit without pressing his finger to the finger scan reader or if the RF system registered a “hit,” what could U.S. authorities do if the suspect had already crossed the border into Canada or Mexico, especially if the individual in question holds a Canadian or Mexican passport? Are the enforcement measures in this situation as good as what could be attained with an exit inspection process that was similar to the entry process (i.e., presentation of travel documents to an inspector, identity check based on facial recognition and fingerprint scan, watch list check, and optional secondary inspection)?

It is unlikely that a land border exit process in which the automobile does not stop is viable. At best, an automated, self-service exit station could be envisioned. Individuals could drive up to the exit station; drivers and passengers could use their wireless entry-exit cards to transmit their finger scans to the RF reader. When the exit is recorded, the station would print out paper receipts, and the barrier would lift to allow the car to pass. If the exit generated a lookout hit, the barrier would not raise and CBP officers could pull the vehicle over for secondary inspection. This solution would still be susceptible to deception with fake fingers. The only secure solution would be to require inspector supervised collection of scans of at least two, if not ten, fingers and a digital photo.

### 3.2.4 Requiring airlines to collect biometric exit data.

VWP reform legislation requires “an exit system that records the departure on a flight leaving the United States of every alien participating in the visa waiver program” and that the system shall “match biometric information of the alien against relevant watch lists and immigration information; and compare such biometric information against manifest information collected by air carriers on passengers departing the United States to confirm such individuals have departed the United States.”<sup>132</sup> DHS considered three options for collecting biometrics upon exit from an airport in the US: at the airline check in counter; at the Transportation Security Administration (TSA) security checkpoint or at the gate. Each option has its advantages and disadvantages as well as its proponents and opponents in the private sector. US airports are not physically designed for exit controls at gates and modifications could be costly and result in a loss of airport space. Collection of biometrics at TSA checkpoints would make increase the time passengers spend at what have become chokepoints in the movement of passengers through airport to their planes. Since airlines have been automating the check-in process and would like to eliminate the need for a person-to-person interaction altogether, they argue that collecting biometrics should be not become the responsibility of their employees but rather the work of government officials. In May 2007, DHS indicated that it planned to work with the airlines to collect biometrics at the check-in counter. Despite loud protests of the airlines, DHS issued a proposed rule in April 2008 that would require that airlines collect travelers biometric data. The new exit process has yet to move forward, however, in January 2009, US-VISIT Program Director Robert Mocny indicated that tests of biometric collection by airlines will commence in the near future.

---

<sup>132</sup> *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law 109-367



Interestingly, however, he indicated that tests of biometric collection by TSA officers at security checkpoints and at the gates will take place as well (Aviation News 2009).

If DHS cannot certify that a biometric air exit system is in place by June 30, 2009, the DHS Secretary loses waiver authority to allow states with visa rejection rates of 3-10% into the VWP. Given that tests of this system have not yet begun, it appears unlikely that a biometric air exit capability will be in place by the end of June. If that happens it is unlikely that additional “road map” countries such as Poland will be admitted into the VWP program, however, it is not clear if those who have already been admitted would (or could) be removed.

### **Intermediary conclusions on Part 3.**

Our deliberations have shown some astonishing tendencies of convergence, partially in a double and even contradictory sense. On the one side, we have seen the EU orient its reform initiative clearly towards US models – which may be a less surprising statement. On the other side, also the US in parallel to its still not accomplished quest for a completely watertight entry-exit system has turned to alternative solutions outside the traditional border-related tool-set. E-Verify as a means to support the internal enforcement of immigration laws via the labour market bears striking similarities to certain European approaches which identify illegal immigrants by controls at the work place.

Another important US move onto unfamiliar territory was the abolition of the so-called “Western Hemisphere exemption” by requiring passport or other documentary proof of citizenship for all Mexican, Canadian and even US travellers crossing US borders, including land borders. This must all the more be seen as a landmark decision as it occurred against the fierce opposition of the local border communities with all economic weight.

A third observation concerns the relatively static focus of the remaining measures as they are all targeted at the closing of gaps within the existing entry-exit system. Although they address the loopholes with great inventiveness and enormous budgetary resources the concept turns out to be a bottomless pit; whether it is a state-of-the-art “virtual fence” intended under SBInet or advanced RFID devices to record movements across land borders, we have each time been able to identify ways to fool or circumvent these mechanisms. At least for those travellers, with a terrorist background or not, who are decided to enter the US by all means, there will be no major obstacle in crossing the border. This finding should be taken to heart by the EU side, before engaging in ventures of a similar dimension such as EU entry-exit and EUROSUR.

## **4. CONCLUSIONS/OUTLOOK**

As we have come full circle with our study there is at least one lesson to be retained: Even if problems such as terrorism, organised crime or migratory pressure may be global but solutions are not necessarily the same. Too different are the starting conditions under the aspects of state/governmental structures, constitutional values, geographic neighbourhood etc to conceive a magic one size fit all-solution. The direct transfer of foreign models should therefore be considered with great care.

The EU-US relationship represents such a case of doubtful compatibility; although border security is a common concern for them, solutions will not necessarily fit both sides to the same degree.

In terms of differences, there is first of all the unilateral **EU-problem of a yet emerging union** with incomplete structures which the EU has to resolve for itself. Although acceptance is increasingly widespread that well-functioning external borders are essential not only from an economic/tax revenue point of view but also to safeguard common security interests, the practical implementation of this insight still encounters multiple obstacles. It is thereby not enough just to make progress in view of harmonising border security, but also indispensable that this process takes place under the auspices of democratic legitimacy and accountability, Only parliamentary and judicial control combined with the

expertise of data protection authorities are capable to sufficiently protect the individuals against excessive intrusion into their rights, in particular privacy. Such protection can best be ensured by the prior entry into force of the Lisbon Treaty which should thus be seen as a prerequisite of any progress in EU border security.

There is furthermore the question to what extent the **US concept** mainly marked by its seamless entry-exit system really qualifies as model for EU development as defined by Future Group and Commission. Doubts towards its direct implementation in Europe arise under various aspects, notably to what extent it is compatible with **European values**. Recent debates in the framework of the transatlantic PNR agreements and the High Level Group on Information Sharing have shown how difficult it is to accomplish a comprehensive transatlantic understanding this field.

The second dividing line concerns **geography**: endless land borders and short-distance maritime waters combined with strong migratory pressure represent a major challenge to any border - even where equipped with hi-tech surveillance devices. This lesson taught to the US themselves by the repeated failure to shut off the Mexican border should be seriously taken to heart by the Europeans. Their border lines being longer, at least currently less well equipped while exposed to greater pressure, the EU should think twice before enacting huge investments in technology. Characteristically enough, the US with its huge advance in border organisation and technology still spent considerable resources on closing the last gaps (see Part 3.2 above), but with a yet uncertain outcome. Spoofing of scan readers or RFID devices is technically possible and therefore as likely to be used for circumventing border controls as long stretches of rarely controlled green or blue borders. In the light of the considerable problems, even the US continue to encounter with the complete roll-out of US-VISIT at land borders, one should possibly reconsider the value/suitability of entry-exit systems for anything else but complete island territories such as Australia.

Rather than globally importing foreign approaches, the EU should also remember its traditional, specifically **European techniques of migration control** which rely on second-line checks of ID-cards and work permits inside the territory. Interestingly enough also the US starts to develop an interest in internal control strategies as shown by the labour-market-oriented pilot project e-Verify.

At the current state of affairs, the EU would do well to closely examine US developments since 1996 when the development of an entry-exit system was first mandated by Congress. Although all essential features were in place by 2003 the **struggle for completion** of the system continues until today. In view of conditions much less favourable in Europe, would it really be a responsible decision to launch such complex and expensive projects as EU Entry-Exit and EUROSUR – with a yet unknown perspective of success?

If convergence of systems is a reasonable transatlantic objective the **point of convergence** should not be determined by a unilateral acceptance of American standards. In view of recent US strategy changes, it would appear likely that the most rewarding encounter would take place somewhere in the middle in combining EU and US standards.

## 5. RECOMMENDATIONS TO THE EUROPEAN PARLIAMENT

In the light of this study, the following recommendations can be made:

- Current reform ideas in border security as presented by the Commission border package as well as the Future Group report do contain interesting but at the same risky features. In view of their direct impact on individual rights and freedoms it is not acceptable that such decisions be taken within the law enforcement-driven environment of the Third Pillar.
- To ensure the due respect of individual rights and freedoms the European Parliament should insist that the decision-making process is subject to legislative and judicial control as well as advice by the data protection authorities. The entry into force of the Lisbon Treaty should be a prerequisite for any legislative progress to be made in border security matters.

- A successful reform of EU border security, even in the operational field, cannot solely be based on intergovernmental models but also needs strong communitarian elements. Besides greater efficiency, this is indispensable for ensuring due respect of human rights in any action led or coordinated by FRONTEX.
- In view of US standards suggested as model for the current reform, legislators should be aware that these mechanisms are strongly shaped by local factors such as legal/ organisational traditions and geography(!), and are therefore not fit for a direct transfer to other parts of the world. The EU should also pay attention to (a) the continuing implementation difficulties encountered in the US and (b) the generally limited role technology can play for resolving border problems.
- Inspiration should also be taken from established European techniques of internal ID controls (ID cards, work permits) which relieve some of the pressure weighing on exclusively borders-based systems. Since also the US seems willing to consider such alternative models (e-Verify), there may be hope of finding transatlantic convergence in border security somewhere in the middle between both systems

**ANNEX**  
**EU/US systems of border security:**  
**Table of correspondence\***

	<b>EU</b>	<b>Legal basis/reference</b>	<b>US</b>	<b>Legal basis/reference</b>
<b>General border management</b>	<b>EU-IBM concept</b>	Schengen border code; IBM Handbook		
<b>Lead authority</b>	<b>FRONTEX</b> - independent European Community agency; <b>DG JLS</b> - European Commission	Regulation (EC) 2007/2004	<b>Customs and Border Security (CBS)</b> - under Department of Homeland Security (DHS)	Homeland Security Act of 2002
<b>Database systems - visa-related</b>	<b>Visa Information System (VIS)</b>	Regulation (EC) 767/2008	Functions spread over various databases such as <b>IBIS/IDENT, CDD, CLASS,</b>	Enhanced Border Security and Visa Entry Reform Act of 2002
<b>- security-related</b>	<b>Schengen information system (SIS II)</b>	Regulation (EC) 1987/2006; Decision 2007/533/JHA	Various systems (watch lists etc) linked to US VISIT	Enhanced Border Security and Visa Entry Reform Act of 2002
<b>Entry-exit system</b>	<i>EU entry/exit system</i> (considered)	COM (2008) 69	<b>US VISIT</b>	Data Management Improvement Act of 2000; Enhanced Border Security and Visa Entry Reform Act of 2002
<b>Trusted traveller concept</b>	<i>Bona fide traveller-concept</i> (considered): Planned for 3rd country nationals and EU citizens	COM (2008) 69	<b>NEXUS, CANPASS, Global Entry:</b> Available for US/Canadian citizens only	
<b>Electronic travel authorisation (ETA)</b>	<i>Electronic system of travel authorisation (ESTA)</i> (considered)	COM (2008) 69	<b>Electronic system of travel authorization (ESTA)</b>	The Intelligence Reform and Terrorism Prevention Act of 2004
<b>Surveillance of green/blue border</b>	<b>EUROSUR</b> (considered)	COM (2008) 68	<b>SBI/SBIInet</b>	Secure Fence Act of 2006

\* Please note that the correspondences indicated in this table are of an approximate nature. In most cases the systems/concepts in question have been structured differently in the EU and the US. The table should therefore not be understood in the sense of exact equations, but as a guide to facilitate the general understanding of the situation in border security matters.

## Bibliography

- Aguilar, David (2005), Statement before the United States Senate Committee on the Judiciary, April 28, 2005.
- AP (2007), "Migrants Become Pawns of Mexico Druglords," Associated Press, April 30, 2007.
- Aviation News (2009), "DHS To Pilot US-VISIT Exit Processes" *Aviation News*, Jan. 5, 2009.
- Barth, Richard (2007), Testimony of Richard Barth, Assistant Secretary for Policy Development and Robert Moczyn, Acting Director, US-VISIT Program, Department of Homeland Security, before the Senate Committee of the Judiciary, "US-VISIT: Challenges and Strategies for Securing the U.S. Border, January 31, 2007.
- Bromwich (1999), Statement of Michael R. Bromwich before the House Judiciary Committee, Subcommittee on Immigration and Claims, March 18, 1999.
- Bunyan, T. (2008), *The Shape of Things to Come – The EU Future Group*. Statewatch analysis. August 2008. Retrieved from <http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf>
- Carrera, S. (2007), *The EU Border Management Strategy. FRONTEX and the Challenges of Irregular Immigration in the Canary Islands*. Working document No. 261. CEPS, Brussels, March. Retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1482](http://shop.ceps.eu/BookDetail.php?item_id=1482)
- Carrera, S. and E. Guild (2008), *The French Presidency's European Pact on Immigration and Asylum: Intergovernmentalism vs. Europeanisation? Security vs. Rights?*. Policy brief No 170, June. Retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1706](http://shop.ceps.eu/BookDetail.php?item_id=1706)
- CBP (2006), "What SBInet Means to CBP Officers and Agents," CBP Fact Sheet, October 2006.
- CESS (2007), STARLINK: Security, Transparency, Accountability and Reform: Linking the Security Sectors of Georgia, Moldova and Ukraine to the European Mainstream. Retrieved from <http://www.cess.org/programmes/past/view/?id=5>
- Chertoff, Michael (2008), "Remarks by Homeland Security Secretary Michael Chertoff at the U.S. Department of Homeland Security Fifth Year Anniversary," Constitution Hall, Washington, DC, March 6, 2008
- Chin, Ko-lin (2001), "The Social Organization of Chinese Human Smuggling," and Peter Kwong, "Impact of Chinese Human Smuggling on the American Labor Market," In David Kyle and Rey Koslowski, eds., *Global Human Smuggling: Comparative Perspectives* (Baltimore, MD: Johns Hopkins University Press, 2001).
- Cohn, Theodore H. (1999), "Cross-Border Travel in North America: The Challenge of U.S. Section 110 Legislation," *Canadian American Public Policy*, (Occasional Paper Series of the Canadian-American Center, University of Maine at Orono), no. 40 (October 1999): 25-38.
- Daté, Shruti 2000. "Immigration Service Patrols with Sensors and Video," *Government Computing News*, Feb. 7, 2000.
- Dermota, Ken (2007), "Human smugglers launch 'coyote express' into US," Agence France Press, May 18, 2007.
- DIMA (2005), Australian Government, Department of Immigration and Multicultural Affairs, *Population Flows: Immigration Aspects, 2004-05 edition*.
- Dizard, Wilson P. III and Alice Lipowicz (2005), "DHS reshapes border technology plan," *Government Computing News*, August 1, 2005.
- DHS (2003), "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," RFP no. HSSCHQ-04-R-0096, US-VISIT Office, Department of Homeland Security, November 28, 2003.
- (2005), "DHS Completes Foundation of Biometric Entry System," Department of Homeland Security, press release, December 2005.
- (2005a), "Secure Border Initiative Fact Sheet," Department of Homeland Security, November 2, 2005.
- (2005b), *Final Environmental Assessment, US-VISIT Increment 2C Proof of Concept at Select Ports of Entry*, Department of Homeland Security, April 13, 2005.
- (2006), *FY2006 Yearbook of Immigration Statistics*, DHS Office of Immigration Statistics
- (2006a), "Border Apprehensions: 2005," Fact Sheet, DHS Office of Immigration Statistics, November 2006.

DHS-OIG (2004), "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," Department of Homeland Security, Office of Inspector General, OIG-05-07 December 2004.

DOS (2006), "Passport Card Stock and Printer Supply Procurement Request for Information," US Department of State (DOS), October 27, 2006.

EU Council (2006), Conclusions of the 2768th Council Meeting Justice and Home Affairs, Brussels, 4-5 December, Press Release, 15801/06, p. 26. Retrieved from [http://www.consilium.europa.eu/ueDocs/cms\\_Data/docs/pressData/en/jha/91997.pdf](http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/91997.pdf)

----- (2008), Presidency note "Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes". Doc. 13803/1/08 REV 1 of 9 October. Retrieved from <http://www.statewatch.org/news/2008/oct/eu-pnr-13803-rev1-08.pdf>

European Commission (2002), Communication, Towards integrated management of the external borders of the Member States of the European Union, COM(2002) 233 final, Brussels, 7.5.2002 (retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0233:FIN:EN:PDF>)

----- (2003), Communication from the Commission to the Council and the European Parliament: Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS), COM (2003) 771, 11.12.03

----- (2005), Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, Brussels, 24.11.05

----- (2006), Recommendation establishing a common "Practical Handbook for Border Guards (Schengen Handbook)" to be used by Member States' competent authorities when carrying out the border control of persons. COM (2006) 5186 final of 6 November. Retrieved from [http://ec.europa.eu/justice\\_home/doc\\_centre/freetravel/rights/doc/C\\_2006\\_5186\\_F\\_en.pdf](http://ec.europa.eu/justice_home/doc_centre/freetravel/rights/doc/C_2006_5186_F_en.pdf)

----- (2006a), Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, COM(2006) 269 final of 31.5.06, retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0269:FIN:EN:PDF>

----- (2007), Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final, European Commission, Brussels, 6 November. Retrieved from [http://ec.europa.eu/commission\\_barroso/frattini/archive/COM\(2007\)654%20EN.pdf](http://ec.europa.eu/commission_barroso/frattini/archive/COM(2007)654%20EN.pdf)

----- (2007a), Proposal for a Directive of the European Parliament and of the Council providing for sanctions against employers of illegally staying third-country nationals, COM(2007) 249 final of 16.5.2007, retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0249:FIN:EN:PDF>

----- (2008), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code. COM(2008) 101 final of 22.2.08

----- (2008a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Report on the evaluation and future development of the FRONTEX Agency. COM(2008) 67 final of 13.2.2008.

----- (2008b), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Examining the creation of a European Border Surveillance System (EUROSUR). COM(2008) 68 final of 13.2.2008

----- (2008c), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the next steps in border management in the European Union. COM(2008) 69 final of 13.2.2008

----- (2008d), Staff Working Document, accompanying document to the Communication on "Preparing the next steps in border management in the European Union". SEC(2008) 154 of 13 February. Retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008SC0153:EN:HTML>

European Data Protection Supervisor (EDPS) (2008), "Preliminary Comments of the European Data Protection Supervisor on the Commission Border Package of February 2008", 3 March. Retrieved from

<http://www.europarl.europa.eu/document/activities/cont/200806/20080611ATT31347/20080611ATT31347EN.pdf>

- European Parliament (2008), Report on the draft Council regulation on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) of 16 September, retrieved from <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0352+0+DOC+PDF+V0//EN>
- (2008a), Procedure file “External and internal borders”: Schengen Borders Code, Visa Information System VIS, COD/2008/0041/COM(2008) 101, retrieved on 12.1.2009 from <http://www.europarl.europa.eu/oeil/file.jsp?id=5602242>
- (2008b), Procedure file “External and internal borders”: Visas: collection of biometric identifiers, organisation of the reception and processing of visa applications, organisation of Member States consular offices for the implementation of the Visa Information System VIS. COD/2006/0088/COM(2006) 269; retrieved on 12.1.2009 from <http://www.europarl.europa.eu/oeil/file.jsp?id=5350262>
- (2008c), DRAFT REPORT on the next steps in border management in the European Union and similar experiences in third countries. Doc. 2008/2181(INI) of 21.11.08. Retrieved from <http://www.europarl.europa.eu/oeil/file.jsp?id=5666192>
- (2008d), Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Constitutional Affairs on Parliament's new role and responsibilities implementing the Treaty of Lisbon. Doc. 2008/2063(INI) of 30.6.08. Retrieved from <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-406.164+02+DOC+PDF+V0//EN&language=EN>
- (2008e), Procedure file “Evaluation and future development of the FRONTEX Agency and a European Border Surveillance System EUROSUR”, Resolution of 5.11./18.12. INI/2008/2157, retrieved on 12.1.2009 from <http://www.europarl.europa.eu/oeil/file.jsp?id=5651072>
- Faure Atger, A. (2008), The Abolition of Internal Border Checks in an Enlarged Schengen Area: Freedom of movement or a scattered web of security checks? Research Paper No. 8. CEPS Brussels, March. Retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1629](http://shop.ceps.eu/BookDetail.php?item_id=1629)
- Federal Register (2006), *Federal Register*, Vol. 71, No 144, July 27, 2006, pp. 42605-42611.
- Future Group (2008), Freedom, Security, Privacy – European Home Affairs in an open world. Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy („The Future Group“). June 2008. Retrieved from [http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Themen/Europa\\_Internationales/Zukunftsgruppe/European\\_home\\_Affairs\\_executive\\_summary\\_en.templateId=raw.property=publicationFile.pdf/European\\_home\\_Affairs\\_executive\\_summary\\_en.pdf](http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Themen/Europa_Internationales/Zukunftsgruppe/European_home_Affairs_executive_summary_en.templateId=raw.property=publicationFile.pdf/European_home_Affairs_executive_summary_en.pdf)
- GAO (2004), “First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed,” General Accounting Office, GAO-04-586, May 2004.
- GAO (2006), “US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry,” General Accountability Office (GAO), December 2006, GAO-07-248.
- GAO (2006a), Government Accountability Office (GAO), Report to Congressional Committees: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program, GAO-06-295, February 2006.
- GAO (2007), “Despite Progress, Weaknesses in Traveler Inspections Exist at Our Nation’s Ports of Entry,” Government Accountability Office (GAO), November 2007, GAO-08-219.
- Georgi, F. (2008), *Bordering on a Nightmare? A Commentary on the 2008 “Vision for an EU Border Management System”*, MCP Prague. Retrieved from [http://aa.ecn.cz/img\\_upload/6334c0c7298d6b396d213ccd19be5999/FGeorgi\\_CommentaryontheVisionforanEUBorderManagementSystem.pdf](http://aa.ecn.cz/img_upload/6334c0c7298d6b396d213ccd19be5999/FGeorgi_CommentaryontheVisionforanEUBorderManagementSystem.pdf)
- Guild, E., S. Carrera and F. Geyer (2008), The Commission’s New Border Package Does it take us one step closer to a ‘cyber-fortress Europe’? Policy brief No 154, March. Retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1622](http://shop.ceps.eu/BookDetail.php?item_id=1622)



- Guild, E., K. Groenendijk and S. Carrera (2008), Ten Issues and Recommendations for the European Parliament Elections on Freedom, Security and Justice. Policy brief No 173, October. Retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1721](http://shop.ceps.eu/BookDetail.php?item_id=1721)
- Hite, Randolph C. (2004), "Testimony for oversight hearing, "US VISIT—A Down Payment on Homeland Security," House Committee on the Judiciary, March 18, 2004.
- Hobbing, P. (2003), *Management of External EU Borders: Enlargement and the European Guard Issue*, DCAF Conference on "Managing International and Inter-Agency Cooperation at the Border", held in Geneva 13-15 March 2003 (retrieved from [http://www.dcaf.ch/news/Border%20Mgt\\_031303/Hobbing.pdf](http://www.dcaf.ch/news/Border%20Mgt_031303/Hobbing.pdf)).
- (2005), *Integrated Border Management at the EU Level*, CEPS, Brussels 2005 (retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1254](http://shop.ceps.eu/BookDetail.php?item_id=1254))
- (2006), "An assessment of the proposals of regulation and decision which define the purpose, functionality and responsibilities of the future SIS II", Briefing Paper for the European Parliament, 15 February (retrieved from <http://www.libertysecurity.org/article1179.html>)
- (2006a), "An Analysis of the Commission Communication (COM (2005) 597 Final of 24.11.2005) on Improved Effectiveness, Enhanced Interoperability and Synergies among European Databases in the Area of Justice And Home Affairs ", Briefing Paper for the European Parliament, 31 January (retrieved from <http://www.libertysecurity.org/article1182.html>)
- (2007), "A comparison of the now agreed VIS package and the US-VISIT system", Briefing Paper for the European Parliament, 4 July (retrieved from <http://www.europarl.europa.eu/activities/committees/studies/download.do?file=17239>).
- (2008), *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*. CEPS Special Report/September 2008. Retrieved from [http://shop.ceps.eu/BookDetail.php?item\\_id=1704](http://shop.ceps.eu/BookDetail.php?item_id=1704)
- (2008a), "Uniforms without Uniformity: A Critical Look at European Standards in Policing", in: E. Guild and F. Geyer (eds), *Security versus Justice. Police and Judicial Cooperation in the European Union*. Aldershot: Ashgate., pp. 243 - 263
- INTERPOL (2006), INTERPOL Presentation, Border Security 2006, Warsaw Poland, May 9-10, 2006
- IOM (2008), About Migration: Facts and Figures. Retrieved from <http://www.iom.int/jahia/Jahia/lang/en/pid/241>
- Jacksta, Robert (2004), "Smart Borders: The Implementation of US-VISIT and other Biometric Control Systems," Alexandria, VA, October 26-27, 2004.
- Jacobs, Janice (2003), "Post 9/11 Visa Reforms and New Technology: Achieving the Necessary Improvements in a Global Environment," testimony of Janice L. Jacobs,
- Jeandesboz, J. (2008), *Reinforcing the Surveillance of EU Borders: The Future Development of FRONTEX and EUROSUR*, CHALLENGE Research Paper, No. 11, CEPS, Brussels, August.
- King, Steve (2006), "Statement of Representative Steve King before the U.S. Congress, Illegal Immigration, July 11, 2006, Congressional Record-House p. H5027.
- Laitinen, I. (2007), News release of 11.6.2007 "Frontex - facts and myths", retrieved from [http://www.frontex.europa.eu/newsroom/news\\_releases/art26.html](http://www.frontex.europa.eu/newsroom/news_releases/art26.html)
- Lee, Jennifer (2006), "Human Smuggling, for a Hefty Fee," *New York Times*, May 28, 2006.
- Loy, James (2005), "Statement of Deputy Secretary Admiral James Loy on the World Wide Threat," U.S. Senate Select Committee on Intelligence, February 16, 2005.
- Meyers, D., R. Koslowski and S. Ginsburg (2007), Room for progress. Reinventing Euro-atlantic Borders for a New Strategic Environment. MPI October 2007. Retrieved from <http://www.migrationpolicy.org/pubs/EuroAtlanticBorders103107.pdf>
- NATO (2003), Common Platform of the Ohrid Regional Conference on Border Security and Management. Retrieved from [http://www.nato.int/docu/conf/2003/030522\\_ohrid/c030522a.htm](http://www.nato.int/docu/conf/2003/030522_ohrid/c030522a.htm)
- Paul, F. (2007), "Europäische IT-Großsysteme: SISII und VIS", 10. Europäischer Polizeikongress, 13-14 February. Retrieved from [http://www.euro-police.com/pdf/paul\\_2007.pdf](http://www.euro-police.com/pdf/paul_2007.pdf)
- (2008), "Biometrics for European Borders: perspectives of European border control and immigration", European Biometrics Forum, 31. October, retrieved from <http://eubiometricsforum.com/dmdocuments2/4thRSFrankPaul.pdf>



- Pew (2006), "Modes of Entry for the Unauthorized Migrant Population," Pew Hispanic Center, Fact Sheet, May 22, 2006.
- Schuckers, S.A.C. (2002), "Spoofing and Anti-spoofing Measures," *Information Security Technical Report 7*, no. 4 (2002), 56-62.
- Senate (1998), Senate Judiciary Committee Report, submitted with *The Border Improvement and Immigration Act of 1998*, Senate Report 105-197.
- Sieber, U. (2009), Die Zukunft des Europäischen Strafrechts. Ein neuer Ansatz zu den Zielen und Modellen des europäischen Strafrechtssystems. To be published at ZStW 121 (2009), pp. 1 - 63. English translation under title "The Future of European Criminal Law. A New Approach to the Aims and Models of the European Criminal Law System" planned in Grasso, G. and R. Sicurella (eds), *Per un rilancia del progetto europeo: esigenze di tutela degli interessi comunitari e strategie di integrazione penale*, Catania (2009), pp. 685-757.
- Stana, Richard (2008), "Secure Border Initiative: Observations on the Importance of Applying Lessons Learned to Future Project," Testimony of Richard M. Stana, Director of Homeland Security and Justice Issues, Government Accountability Office (GAO) before the Subcommittees on Management, investigations, and Oversight, and Border, Maritime and Global Counterterrorism, Committee on Homeland Security, House of Representatives, February 27, 2008, GAO-08-508T.
- Statewatch News Online (2008), "EU-PNR scheme being re-written by the Council", October 2008, retrieved from <http://www.statewatch.org/news/2008/oct/04eu-pnr-rewrite.htm>
- UK Parliament, House of Lords (2007), *Schengen Information System II (SIS II)*, European Union - Ninth Report, European Union Committee, London, 20 February, retrieved from <http://www.publications.parliament.uk/pa/ld200607/ldselect/lducom/49/4902.htm>
- UK Parliament, House of Lords (2008), *FRONTEX: the EU external borders agency* European Union - Ninth Report, European Union Committee, London, 26 February, retrieved from <http://www.publications.parliament.uk/pa/ld200708/ldselect/lducom/60/6002.htm>
- Van der Putte T. and J. Keuning (2002), "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned," *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications* (Kluwer Academic Publishers: 2000); T. Matsumoto, et. al. "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," *Proceedings of SPIE 4677* (January 2002).
- White House (2005), "Fact Sheet: Border Security," The White House, January 25, 2002, <http://www.whitehouse.gov/news/releases/2002/01/20020125.html> (accessed January 27, 2005).

## Legislation

- Decision 2004/512/EC of the Council of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213 of 15.06.04, p. 5
- Decision 2007/533/JHA of the Council of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205 of 7.8.07, p. 63
- Decision 2008/633/JHA of the Council of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences
- Regulation (EC) No 2725/2000 of the Council of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. OJ L 316 of 15.12.00, p. 1
- Regulation (EC) No 539/2001 of the Council of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, L 81 of 21.3.01, p. 1
- Regulation (EC) No 343/2003 of the Council of 18 February 2003 establishing criteria and mechanism for determining the Member State responsible for examining an asylum application lodged in one of the Member States of the European Union, OJ L 50 of 25.2.03, p. 1
- Regulation (EC) No 2007/2004 of the Council of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349 of 25.11.04, p. 1.
- Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code, OJ L 105 of 13.4.2006, p. 1
- Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, OJ L 381 of 28.12.06, p. 1
- 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 of 28.12.06, p. 4.
- Regulation (EC) No 863/2007 of the European Parliament and of the Council of 11 July 2007 establishing a mechanism for the creation of Rapid Border Intervention Teams and amending Council Regulation (EC) No 2007/2004 as regards that mechanism and regulating the tasks and powers of guest officers, OJ L 199 of 31.7.07, p. 30
- 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 L 218 of 13.8.08, p. 60

## Abbreviations

CESS	Centre for European Security Studies, Groningen, Netherlands
CRATE	Central Register of Available Technical Equipment (FRONTEX)
CSI	Container Security Initiative
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EP	European Parliament
FG	Future Group (Informal High Level Advisory Group on the Future of European Home Affairs Policy, created in January 2007)
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States
Future Group	Informal High Level Advisory Group on the Future of European Home Affairs Policy, created in January 2007
HLCG	EU-US High Level Contact Group on information sharing and privacy and data protection
PCCC	Police and Customs Cooperation Centre
PNR	Passenger Name Record
RABITs	Rapid Border Intervention Teams (FRONTEX)
SAR	Search and rescue operations
VWP	Visa Waiver Program