International Terrorism and Migration

IOM International Organization for Migration

The opinions expressed in the report are those of the authors and do not necessarily reflect the views of the International Organization for Migration (IOM). The designations employed and the presentation of material throughout the report do not imply the expression of any opinion whatsoever on the part of IOM concerning the legal status of any country, territory, city or area, or of its authorities, or concerning its frontiers or boundaries.

IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM acts with its partners in the international community to: assist in meeting the operational challenges of migration; advance understanding of migration issues; encourage social and economic development through migration; and uphold the human dignity and well-being of migrants.

Publisher: International Organization for Migration
17 route des Morillons
1211 Geneva 19
Switzerland
Tel: +41.22.717 91 11
Fax: +41.22.798 61 50
E-mail: hq@iom.int
Internet: http://www.iom.int

38_10

International Terrorism and Migration

JUNE 2010

IOM International Organization for Migration

Table of Contents

INTRODUCTION

In 2003, IOM produced the report International Terrorism and Migration, discussing the relationship between the two phenomena and noting some of the more prominent initiatives and measures in areas where interlinkages exist between the two fields. Since then, national governments and international coalitions of organizations and states working at the regional and global level have made important progress in a number of key areas. The strategies developed in relation to border control, carrier sanctions, extradition procedures, etc. have been applied and developed further in relation to the fight against terrorism. This up-dated report aims to provide an overview of some of the most significant developments in recent years.

Chapter 1 discusses the relationship between migration and terrorism. While warning against linking migration too closely to security issues, it points to a number of areas where migration measures intersect with security issues. It is crucial that such distinctions are clearly drawn at the outset, since this initial discussion informs subsequent chapters.

Chapter 2 is devoted to border and entry controls. Increasing globalization and substantial international flows of goods and people constitute powerful drivers of development in this area. The chapter describes efforts by governments to enhance border management. Such measures have been implemented with the twin aim of facilitation and control in mind, and there has been a significant trend towards pre-inspection measures.

Chapter 3 outlines developments in identification systems, focusing on the use of biometrics. Just as with border and entry measures, initiatives in this area have reflected a more sophisticated approach, facilitating cross-border travel as an integral part of efforts to enhance security. This has involved improvements in travel document standards and, increasingly, automation of border controls. A number of examples are provided to illustrate such developments. Although these examples do not provide an exhaustive list of recent measures, they should give some indication of trends in identification systems.

Information exchange and cross-border cooperation form the subject of Chapter 4, which aims to provide an overview of some of the most active international and regional institutions established for the purpose of cooperation in attempting to make the world safer from terrorism. The chapter examines trends towards increased information-sharing in migration-related areas, law enforcement, the sharing of watch lists[1] and the establishment of regional and global databases for these purposes.

Chapter 5 turns to the domestic scene and discusses integration policies implemented by governments and how these can contribute to more stable and cohesive societies, considering that terrorism can grow out of failed and inexistent integration policies. The chapter proceeds to review recent legislation and policies formulated by states for national security purposes, including identification and tracking measures. Such policies can be of particular significance to migrants who are often in a vulnerable situation in host countries. In many countries, for example,

[1] Watch lists are a commonly used instrument to control access to a country's territory by those who are wanted for, or suspected of, crimes.

anti-terrorism legislation has included controversial provisions for detention and deportation.

Finally, the concluding discussion draws together the main themes of the report and summarizes key points for governments and other relevant stakeholders to consider. With likely increased levels of migration over the coming decades, it calls for increased international cooperation and enhancement of global efforts to close the door to terrorists and others who wish to exploit migration channels, while facilitating the positive aspirations of legitimate migrants and their many contributions to society and development. IOM is committed to working with governments toward managing migration flows in an orderly and humane manner.

LIST OF ABBREVIATIONS

ABC	Automated Border Control
ALO	Airline Liaison Officer
APEC	Asia-Pacific Economic Cooperation
API	Advance Passenger Information
APIS	Advance Passenger Information System
APP	Advance Passenger Processing
ATU	[OSCE] Action against Terrorism Unit
AU	African Union
BMG	[APEC] Business Mobility Group
CAI	[EU] Common Agenda for Integration
CBP	[US] Customs and Border Protection
CICTE	[OAS] Inter-American Committee against Terrorism
CTC	[UN] Counter-Terrorism Committee
CTED	[UN] Counter-Terrorism Committee Executive Directorate
DHS	[US] Department of Homeland Security
e-MRTD	Electronic Machine-Readable Travel Document
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ETA	Electronic Travel Authority
IATA	International Air Transport Association
ICAO	International Civil Aviation Association
ICPAT	IGAD Capacity Building Program against Terrorism
IGAD	Intergovernmental Authority on Development in Eastern Africa
ILO	Immigration Liaison Officer
IMF	International Monetary Fund
IOM	International Organization for Migration
MRTD	Machine-Readable Travel Document
MRZ	Machine-Readable Zone
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
PAXIS	[Canadian] Passenger Information System
PKD	Public Key Directory
PNR	Passenger Name Record
RFID	Radio-Frequency Identification
RMAL	Regional Movement Alert List
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
SPP	Security and Prosperity Partnership of North America
UNHCR	United Nations High Commissioner for Refugees
US-VISIT	United States Visitor and Immigrant Status Indicator Technology program
VIS	Visa Information System
WCO	World Customs Organization

CHAPTER 1
THE RELATIONSHIP BETWEEN INTERNATIONAL TERRORISM AND MIGRATION

The terrorist attacks in New York on 11 September 2001 (henceforth, 9/11) have undeniably had a lasting effect in many areas. One significant consequence was that migration became more strongly linked to national security issues. In the wake of the 9/11 attacks, measures aimed at preventing terrorism were often explicitly linked to immigration policies. The following years have seen many laws, regulations and international conventions on terrorism. Not just in the US, but all over the world, states have worked to strengthen border and immigration controls and tighten security. While this latest impulse derives from 9/11, governments were working to address many of the reforms mentioned in this report long before security became a major issue. Nevertheless, a number of incidents have demonstrated the continuing threat of international terrorism. Since 9/11, high profile attacks against commercial and civilian targets in countries such as the UK, Jordan, Indonesia, the Philippines, the Russian Federation, Saudi Arabia, Spain and Turkey have resulted in substantial loss of life and injury, and in significant emotional and economic costs. These events initiated new policies. Western European countries, the US and Canada introduced a non-arrival or non-entry policy in order to create barriers to the new influx of asylum seekers and economic migrants. While policies in the late 1980s were developed with a multifaceted approach (visa requirements combined with carrier sanctions; creation of international zones in airports; isolation of applicants and processing of applications for asylum at military bases abroad), the next step, following the terrorist attacks, was the posting of immigration officers or airline liaison officers in countries of origin or important transit countries such as Pakistan and Turkey.

Although European countries already had to face the reality of an external threat, the link between migration and international terrorism seems to have re-emerged as a result of those attacks, and follows from a lesson learned by states: that terrorism is no longer limited to nations or regions. Just as goods, capital and services are moving quickly and with fewer restrictions around the world in complex globalized networks, so are terrorists, and their activities display a supranational dynamic beyond the reach of many national law enforcement agencies. In other words, there has been a realization that the very processes which facilitate travel and economic and cultural exchange can also be exploited by terrorists. While this connection between migration and international terrorism is the outcome of relatively recent developments, it is important to recognize that migration is not a new phenomenon and that it has often formed a vital part of the economic and social development of destination/host countries, while providing migrants with new opportunities and relieving some of the pressures of unemployment and underemployment in their countries of origin. Migration has traditionally, and correctly, been seen primarily as an economic and social issue, rather than a security issue.

How migration relates to security issues is a multi-dimensional subject. International terrorism could, because of its cross-border dimensions, also be considered a migration issue. It touches on a range of matters directly affecting migration policy, including: border integrity (entry and/or residence with illicit intent), national security, integration, ethnic/ multicultural affairs and citizenship. International terrorism is a test, *in extremis*, of the degree to which national immigration policies continue to be relevant in an increasingly borderless world. However, migration policy, particularly with regard to managing who comes in and out of a country and resides there, is just one area where national and international law enforcement can act against terrorism.

More importantly, the securitization of migration is unwarranted and unhelpful in some respects. Specifically, when migration and terrorism are linked too closely, or in a simplistic causal manner, there is a risk that policy prescriptions will be misguided or could even backfire by increasing community tensions and compromising social cohesion. The argument that there exists a link between migrants and terrorism needs to be challenged.

One of the difficulties associated with measures to combat terrorism on a global scale is the formulation of an appropriate universally accepted definition of “terrorism”. Terrorism is defined by UN Security Council Resolution 1566 as:

> Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act.

It is a complex and extreme political act that grows out of a combination of cultural, economic, political and psychological forces. By closely linking migrants to terrorism, states may antagonize immigrant communities, inadvertently breeding hostile sentiments towards the state. They may also risk an increase in xenophobia and the resulting inter-societal violence. Finally, entry for potential migrants might be hindered or deterred, thus depriving countries of the economic benefits of migration while simultaneously reducing legitimate avenues for persons seeking international protection, by making it more difficult for asylum seekers to cross an international border to a safe haven as highlighted by the issue of mixed flows.

Finding the appropriate balance between facilitation, protection of human rights and control is a key challenge for all countries in attempting to make international borders more secure. It is understandable that national governments are concerned about the risks posed by terrorism and the capacity of terrorist groups to exploit weaknesses in immigration management and border controls. Where such weaknesses exist, there is certainly a need for improved security. However, security measures undertaken must always be justified by, and be proportionate to, the level of threat faced by states, particularly if increased security means increased obstructions and potential intrusions into privacy and civil rights. Furthermore, any proposal for such measures should recognize that migration management is not the primary tool in the fight against terrorism.

Having said that, it is important to recognize that there are areas where the issue of migration intersects with the issue of international terrorism, because of its cross-border dimensions. These include, among others, border systems, travel documents, information exchange, training and intergovernmental dialogue and cooperation. Broader migration policy can also help address aspects of social stability in diverse societies to reduce the potential for ethnic or other conflicts. Improvements in these areas can contribute to enhanced security as well as better functioning migration regimes, facilitating the movement of people across borders. Some of the measures implemented for this purpose may be technologically complex and highly innovative, but often it will be a matter of enhancing traditional areas of migration management capacity.

IOM believes that, while immigration policy is not central to combating terrorism, it can contribute towards addressing it, particularly to ensure better application of law enforcement and intelligence measures.[2] Immigration authorities can also contribute to national/international intelligence through direct encounters with migrants, irrespective of their immigration status, and through partner networks with other law enforcement and immigration agencies.

[2] Fighting against irregular migration, transnational criminal network and against trafficking/ smuggling; and facilitating movements for regular migrants and travellers

CHAPTER 2

BORDER AND ENTRY CONTROLS

In a matter of weeks after the attacks of 9/11, the UN Security Council unanimously adopted Resolution 1373. Calling for greater cooperation and information-sharing among states, it also called on states to:

> Prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents.[3]

Prior to 9/11, many states were already struggling with irregular migration flows and cross-border criminal activity such as smuggling and human trafficking. Since 2001, the mobility of international terrorists has been one of the main concerns of the international community and has driven many of the developments in border and entry controls in recent years, with a particular focus on border security as well as complementary initiatives, ranging from improvements in travel documents to increased collection of information on travellers.

While the specific border measures implemented by any particular country will depend on a number of factors – such as the nature of the borders (land/sea/air), the volume of crossing, the situation in neighbouring countries, and the number of personnel and resources available – there appears to be a trend towards layered controls, with an increasing number of countries implementing pre-inspection measures to collect information and screen passengers prior to their arrival at a national border. This type of strategy has the potential to enhance security by providing border officials with more time and information needed to make appropriate decisions. At the same time, it promises facilitated travel for the majority of low-risk passengers.

However, the financial and political costs of too strict an immigration control regime can be high, and there is a danger that too heavy an emphasis on entry control can jeopardize the maintenance of a balanced migration policy. The stricter the regime and the more difficult it is to secure visas, the greater the potential for deterring business travellers and other bona fide visitors. This can impact both on a nation's wealth, by impeding trade, and its reputation for welcoming foreigners. It may in turn lead to retaliation from other countries facing harsher entry conditions for their nationals with the potential of increased isolationism. Such an immigration control regime risks affecting particularly refugees fleeing persecution or conflict. At a time when the threat of terrorism is a reality and border security measures appear to be increasing, it is vital that states find ways to identify and admit vulnerable individuals in need of asylum, in accordance with their international obligations under the 1951 Refugee Convention.[4] What is important to emphasize is the need for a reasonable balance between addressing legitimate security concerns and protecting individual human rights and freedoms.

[3] UNSC Res. 1373, UNSC, 56th Sess., 4385th Mtg at 2, UN Doc. S/RES/1373 (28 Sept. 2001); the full text of the resolution is available at: http://www.un.org/News/Press/docs/2001/sc7158.doc.htm

[4] A. Schoenholtz (2007) "Anti-Terrorism Laws and the Legal Framework for International Migration" in R. Cholewinski et al. (eds.), *International Migration Law*, T.M.C. Asser Press, The Hague, p. 16

i) PASSENGER PRE-INSPECTION

The large numbers of travellers crossing international borders each day, coupled with the constant challenge to maintain security and border integrity, have prompted many countries to develop innovative measures in border management. Among these measures, there has been a continued trend towards the shifting of border control measures beyond a country's territorial boundaries. This has meant extending controls to points of embarkation, so as to allow for pre-inspection of passengers. Bearing in mind that the balancing of facilitation and control is the key challenge faced by states, pre-inspection measures allow for smoother processing of bona fide travellers, while at the same time enabling states to detect passengers who present security risks at an early stage. Such a targeted approach enhances security by providing for the exclusion of those who constitute a threat, or for a closer inspection upon arrival. Among the measures employed by states to inspect passengers at an earlier stage are long-standing policies such as the issuing of visas, but also include such measures as the stationing of immigration officers at airports and embassies abroad and, increasingly, sophisticated systems for electronically transmitting pre-arrival information on passengers to border and immigration authorities. The following section outlines developments in these areas.

a) Visas

An important way to manage migration before the traveller approaches the border is through systems for issuing visas prior to travel. If issued abroad, this process provides representatives of the country of destination with the opportunity to make an assessment ahead of travel, thus facilitating the travel and entry of bona fide travellers. As noted earlier, the key challenge for states is to balance facilitation and control. A targeted approach may be necessary, not only from a security perspective, but also for practical and financial reasons. This may mean visa requirements for the nationals of some countries but not others. If, on the other hand, a country opts for a universal visa regime, as in Australia's case, it may be necessary to find other ways of minimizing costs and ensuring that the process runs smoothly, with as few obstacles for passengers as possible. With its **Electronic Travel Authority (ETA)**, Australia allows citizens from a number of countries to obtain an electronic visa as part of the existing travel/airline reservations system. The ETA is electronically stored and accessible to airlines and travel agents and Australian officials, but no document is issued.

Another approach has been taken by the United States since the 9/11 attacks. Rather than opt for universal visa requirements, the US has long had a visa waiver programme targeting a number of countries, mainly in Europe. As part of efforts to increase security, the US has instituted requirements for all passengers from countries eligible for the visa waiver programme to present machine-readable passports. In addition, and to remain in the visa waiver programme, these countries must ensure that any passports issued after 2006 are e-passports storing biometric information.[5] Thus, security is improved without burdening individual passengers with further visa requirements.[6] Indeed, the visa waiver programme continues to expand. Furthermore, in 2009, the US launched an ETA scheme (called ESTA: Electronic System for Travel Authorization),[7] modelled on the one in Australia. According to this system, travellers eligible for Visa Waiver Programme (VWP) required to apply and

[5] http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/epssprt_vwp.xml

[6] Such measures, however, have a cost that can be a burden for countries with limited resources.

[7] See US Customs and Border Protection, Electronic System for Travel Authorization (ESTA), http://www.cbp.gov/xp/cgov/travel/id_visa/esta/.

be authorized for travel before departure via the ESTA website. In the Schengen area,[8] states have also discussed implementing a European ETA scheme.[9]

b) Liaison Officers Stationed Abroad

Many countries now deploy immigration officials to work with foreign governments and airline personnel to identify persons travelling with fraudulent documents and to combat smuggling of migrants and trafficking in persons. Under arrangements established through bilateral agreements, immigration inspection officers who carry out full clearance for entry to the country of destination are stationed abroad at airports, inspecting passengers departing for the officers' country, and at times for other collaborating countries. The officers are also working with, training, and advising airline staff on the prevention of travel of persons with fraudulent documents or other fraudulent identification. Canada and the United States were the first countries to place immigration and airline liaison officers at international airports overseas; this model was later adopted by Australia and other countries. Although the various schemes developed by countries differ slightly in terms of structure as well as the job titles and responsibilities of officers stationed abroad, the main idea is the same: to screen passengers as early as possible, and to facilitate the travel of bona fide passengers, while preventing the movement of those who pose a threat to national security. Different liaison officers (immigration liaison officers and airline liaison officers) cooperate and joint initiatives have been launched, e.g. by the EU.

Immigration Liaison Officers (ILOs) are liaison officers posted close to the centres of criminal activity, or in source countries of irregular migrants, to work with local law enforcement agencies and international agencies such as EUROPOL[10] to prevent irregular migration and help close down related illegal and criminal operations. In 2004, the EU established an Immigration Liaison Officers Network in order to coordinate the activities of ILOs posted by Member States.[11] Under this structure, ILOs posted to the same country form a local network for the purposes of information-sharing and coordination of activities, policies and training courses. In addition, by further agreement, an ILO from one Member State may be designated to attend to the interest of other Member States.

Airline Liaison Officers (ALOs) are immigration inspection officers posted abroad to work with and train airline staff to prevent the travel of persons with fraudulent documents or IDs. Although they have no legal powers to prevent passengers from

[8] See p. 18 for further information on Schengen agreement.

[9] Communication from the Commission to the European Parliament and to the Council on an entry/exit system at the external borders of the European Union, facilitation of border crossings for *bona fide* travellers, and an electronic travel authorization system, COM(2008).
Discussions have taken place on whether the EU should create an electronic travel authorization (ETA) system. It could be applicable to third-country nationals not subject to the visa obligation, and as a consequence have an influence on the countries to be subject to that obligation in the future. As part of the further development of the integrated management of the EU external borders, the setting up of an ETA system should be analysed to assess its potential added value compared to existing and planned initiatives. Technical, financial and practical implications in the light of current provisions on Advance Passenger Information (API) and future provisions on a European passenger name record (PNR) system should be examined.

[10] Europol has a team of counter-terrorist specialists. These are "liaison officers" from police, internal security and intelligence agencies specializing in terrorism, in charge of collecting and analysing information and intelligence and providing operational and strategic analysis; and drafting a threat assessment document including targets, damage, potential modi operandi, consequences for security and preventive measures.

[11] Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network, OJ 2004 L 64/1

embarking, their authority is implied since, in essence, the ALO lets the carrier know that the individual would not be admitted at a destination port of entry.[12]

ALOs often work in tandem with ALOs and ILOs from other countries. It clearly becomes untenable for the host country if each country of destination seeks to post its own ALO at the same airport. Therefore local networks have been set up in many locations. For example, the EU has brokered such cooperative arrangements and some joint ALO initiatives have been launched.

The International Civil Aviation Organization (ICAO) has designated the posting of ALOs as a recommended practice,[13] and the number of ALOs posted worldwide has steadily increased. For example, the UK has progressively expanded its network of ALOs to 34 airline liaison officers, five ALO floaters and 12 deputy airline liaison officers (DALOs). UK ALOs are based overseas at source and transit locations which have been identified as significant points of embarkation for inadequately documented arrivals (IDAs) in the UK. Working according to the International Air Transport Association (IATA) code of conduct for immigration liaison officers,[14] they maintain a presence in 32 locations overseas. However, by giving some ALOs responsibility for a number of other countries in their region, more than 120 countries are covered by the UK ALOs.[15] According to the UK Home Office, over 30,000 passengers were prevented from embarking on flights in 2004, based on the advice of UK ALOs worldwide.[16] Other countries which have extensive ALO networks include Australia, Canada and the Netherlands. Building on previous steps in this direction, the US established its Immigration Advisory Program (IAP) in 2004. In 2008, IAP maintained liaison officers at seven overseas locations. While adding a layer of security, IAP is also estimated to have ensured cost savings of approximately USD 1.6 million in its first two years, as a result of excluding passengers who would have been detained and returned after being refused admission to the US.[17]

c) Advance Passenger Information

While liaison officers are tasked primarily with preventing the travel of undesirable passengers, the main purpose of Advance Passenger Information (API) is to facilitate travel for bona fide passengers by allowing for early registration and processing of travellers, thus reducing delays at the border. API involves agreement between countries, and between airlines and governments, permitting passenger manifests to be electronically sent by the airlines ahead of flights to the immigration authorities of the country of destination for pre-checking before arrival. API is limited to a relatively small number of core data elements. For example, Canada's API programme[18] involves the transfer of the following information:

- full name
- date of birth
- gender
- citizenship or nationality

[12] See part on "Carrier sanctions".

[13] See http://www.caa.govt.nz/rules/ICAO_diff.htm.

[14] See http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp040_en.pdf.

[15] http://www.ukba.homeoffice.gov.uk/aboutus/workingwithus/transportindustry/rlon/howrloncanhelp/

[16] "UK Borders Further Strengthened with Expansion of Airline Liaison Officer Network", Home Office Press Release, 22 February 2005, http://press.homeoffice.gov.uk/press-releases/Uk_Borders_Further_Strengthened_?version=1

[17] "Fact Sheet: Select Homeland Security Accomplishments For 2006", US Department for Homeland Security, 29 December 2006, http://www.dhs.gov/xnews/releases/pr_1167404984182.shtm

[18] http://www.aircanada.com/en/travelinfo/APIS/apis.html

- type of travel document, the country of issue and the number
- reservation record locator (if any)
- flight manifest data.

This information is contained in the machine-readable zone (MRZ) of passports, and can therefore be collected by airlines at airport check-in. In some cases, the airline will have to ask passengers to provide additional information. For example, the US API programme requires the destination address for foreign nationals, as well as their country of residence. Once the API has been collected, it is transmitted to the country of destination, where it is analysed and checked against databases and alert lists. The information then becomes available to immigration and customs officials at the airport of arrival. Ultimately, this leads to enhanced security, since officials have more time to identify those travellers who may pose a threat and can consequently focus their attention on these passengers upon arrival. This also means faster processing of the majority of passengers who do not need to be singled out for closer inspection and whose data has already been captured through the API system. Upon arrival, it may suffice for them to just verify their identity.

In most cases, API is transmitted only after the flight has taken off. This means that while immigration officials have time to prepare for the arrival of persons who have been identified as security threats, they cannot stop them from embarking on the flight. However, if API is transmitted before the flight takes off, the API system can be designed to verify all passenger information and inform airlines prior to departure as to an individual's likely immigration status upon arrival. The airline can then be requested to prevent the passenger from boarding the flight. Such an interactive system is sometimes called Advance Passenger Processing (APP) or Authority to Carry. By verifying immigration status prior to departure, this system reduces the likelihood that individuals will have to be returned home immediately after being turned away by officials at their destination. As well as increasing security further, this also reduces airline and border control costs as well as unnecessary trouble of travelling for the person in question.

As API schemes were originally seen first and foremost as facilitation measures, they were not mandatory. For example, the US Advance Passenger Information System (APIS) began in 1989 as a voluntary programme developed on behalf of the US Customs Service, the US Immigration and Naturalization Service, and the airline industry. The system was designed to allow air and sea vessels en route to the US to convey the biographical data of passengers to authorities ahead of arrival. As a part of the push for tightened border security after 9/11, the voluntary nature of the APIS was ended under the conditions set out in the US Aviation and Transportation Security Act of 2001 (ATSA) and the Enhanced Border Security and Visa Reform Act of 2002 (EBSA). This legislation made it mandatory to collect certain information in advance on all persons arriving in, departing from, or transiting through the US via commercial carriers.

In recent years, a number of other countries, such as Australia, Canada, China and the UK have also instituted requirements that airlines provide API data.

For example, in the UK, the Immigration (Passenger Information) Order 2000 extended immigration officers' powers to require carriers to provide data on passengers arriving in and departing from the UK. The Immigration, Asylum and Nationality Act 2006 further strengthened the legal basis underpinning the UK's API system, which forms part of **e-Borders** – a broader vision of a modernized border management system. As part of e-Borders, all cross-border transports, whether by air, sea or via the Channel tunnel rail link, will be required to submit API. However, the UK is implementing the system gradually while also applying technological improvements in border control, primarily in biometrics, which form the other major component of e-Borders. By 2014, the e-Borders programme is expected to be fully operational, covering entry as well as exit of all passengers.[19]

Canada introduced its **Passenger Information System (PAXIS)** on October 7, 2002, making it mandatory for airlines to submit API. Since not all carriers have the ability to submit API via electronic data interchange, Canada has developed alternative solutions using the Internet in order to make it possible for airlines to comply with the requirements.[20]

Australia's **Advanced Passenger Processing (APP)** was made mandatory in 2003. Since it is an interactive system, it enables airlines to pre-clear passengers at check-in. The API is electronically sent to Australia, matched against ETA visa information and checked against a Movement Alert List. Should there be a problem with the visa, or should the passenger be of concern to Australian authorities for security-related reasons, the carrier already will receive advice at check-in not to board the passenger.

Countries implementing API programmes aim to make these comply with developing international standards. Of note in this area are the joint **World Customs Organization (WCO) /International Air Transport Association (IATA)/ International Civil Aviation Organization (ICAO) Guidelines on Advance Passenger Information**[21] (due to be updated), which emphasize the expected benefits of API, both in terms of increased security and faster flight clearance time, thus facilitating travel. They also recommend that information transmitted should be limited as far as possible to the data included in machine-readable travel documents (MRTDs) in order to ensure interoperability. This becomes especially important as the number of states that have either implemented API or are in the process of doing so keeps increasing. By 2008, their number stood at over 40.[22]

In the European Union (EU), it is the Council Directive on Passenger Information[23] which governs the transfer of API, requiring airlines of all Member States to submit such data upon request.

d) Passenger Name Records

In the US, the same legislation which mandated authorities to require API also made it mandatory for carriers to provide Passenger Name Records (PNR) on US-bound passengers. A PNR is created when a travel booking is made for a passenger and is held in the travel agent's or airline's reservation system. Along with the names and ticket details of the passenger, PNR typically includes information on the date and method of ticket payment, contact details such as address, telephone number or e-

[19] For the e-Borders implementation timetable, see the UK Border Agency website at http://www.ukba.homeoffice.gov.uk/managingborders/technology/eborders/timetable/.

[20] See "The Canadian Advance Passenger Information Program", ICAO, Facilitation (FAL) Division, 12th Session, Cairo, 22 March-2 April 2004, Doc. FAL/12-WP/38 (http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp038_en.pdf).

[21]http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Procedures%20and%20Facilitation/APIGuidelines_ENG.pdf

[22] "Harmonisation of Advance Passenger Information (API) Regimes", ICAO Working Paper, Facilitation Panel, 5th Meeting, Montréal, 31 March-4 April 2008, Doc. FALP/5-WP/24, http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp24_en.pdf

[23] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 2004 L 261/24

mail, seating information and other special requirements. However, the exact number of details held on passengers in the PNR varies between carriers.

After 9/11, the US determined that PNR could make a valuable contribution towards efforts aimed at preventing terrorism. Consequently, requirements were instituted that all inbound airlines provide the US authorities with these records. PNR data is sent ahead of flight departure and is analysed and checked against the relevant US watch lists.

In addition to the US, a number of countries have introduced – or are planning to introduce – requirements for PNR. Australia, Canada and New Zealand are among the countries which also require airlines to submit PNR data. Canada began collecting PNR data in 2003 as an extension of its API programme, and Australia passed legislation in 2002 providing for the collection of PNR.

It is the relatively extensive information on passengers contained in the PNR which makes it attractive to authorities responsible for security. However, it is also this that has given rise to concerns about privacy and data protection.[24] This raises the important question of proportionality. Any limitations on rights (infringements of rights) in terms of loss of privacy must be justified by the increase in security. Some NGOs have voiced doubts about the effectiveness of a PNR system in increasing security, particularly in light of already existing provisions for API.[25] API, on the other hand, has encountered fewer objections as the data transmitted is essentially limited to that contained in the machine-readable zone of passports, information which would be available to border and customs authorities at border control posts. PNR, however, involves additional and more personal information and is consequently more intrusive in terms of privacy. Questions often raised include the number of data elements to be submitted, as well as the amount of time the information may be retained by authorities.

The sensitivity of PNR is clearly illustrated by the difficulties of achieving an agreement between the US and the EU. When the US first started requiring airlines to provide PNR data, several European airlines objected, saying that doing so would violate EU data protection rules. The 1995 EU Directive on Data Protection[26] states that such information may only be transferred to a third country with an adequate level of privacy protection. Eventually, an agreement on the transfer of PNR was reached between the European Commission and the US Customs and Border Protection (CBP) in 2004, allowing for the transfer of PNR by US-bound airlines. However, the European Parliament was critical of the deal and worked to have it overturned. It achieved this in May 2006, when the European Court of Justice invalidated the agreement. Nonetheless, US requirements for PNR remained and it was clear that a new agreement of some sort was needed. Temporary arrangements were quickly made until a new deal could be struck. Eventually, a new US-EU PNR agreement was reached in July 2007. The new agreement stated that "DHS [Department of Homeland Security] is deemed to ensure an adequate level of

[24] See European Parliament Resolution of 12 July 2007 on the PNR agreement with the United States of America, Doc. P6_TA-PROV(2007)0347, available at http://www.statewatch.org/news/2007/jul/ep-pnr-resolution-jul-07.pdf.

[25] "EU: European Commission to propose EU PNR travel surveillance system", *Statewatch News Online* (updated 15 July 2007), http://www.statewatch.org/news/2007/jul/03eu-pnr.htm

[26] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/341, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

protection for PNR data transferred from the European Union".[27] However, some observers still do not believe that is the case. They have focused their criticism on the lack of clear designations of authorities which may access the data as well as with whom it may be shared. Other areas of concern include the length of retention of the data in US databases (15 years under the new agreement, compared to 3.5 years under previous agreements) and the number of data fields requested.[28]

The number of data fields requested has varied depending on the requesting country. For example, the PNR agreement between the EU and Canada in October 2005 specifies 25 data fields, while the July 2008 agreement with Australia involves only 19 data elements. In the 2007 US-EU PNR agreement, the number of data fields was reduced to 19 from the previous 34. However, critics have argued that this reduction is largely cosmetic, achieved by combining what were previously separate fields.[29]

Another difference may be the manner in which the data is transferred. The 2004 US-EU PNR agreement provided for a "pull" system, whereby US authorities were entitled to access PNR data directly through airline reservation systems. The agreement with Canada, on the other hand, was designed for a "push" system, whereby airlines themselves transfer the information to the requesting authorities. The latter system has been deemed less intrusive[30] and the 2007 EU-US agreement states that the parties should switch to a "push" system for all airlines with the technical capacity to transfer the data as required.[31]

As of 2008, the EU had separate PNR agreements only with Australia, Canada and the US. Although the Republic of Korea also requested PNR data, the EU has so far determined that data protection is not adequate in that country.[32] Currently, there is no EU requirement for the transfer of PNR from third countries. However, discussions have been held for some time on this matter, a proposal for an EU directive on PNR has been drafted,[33] and some EU Member States have enacted legislation providing for the collection of PNR data. Under its e-Borders strategy, the UK has already run a pilot programme collecting PNR data from a number of airlines.

[27] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) OJ 2007 L 204/18, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0018:0025:EN:PDF, para. 6

[28] See European Parliament Resolution of 12 July 2007 on the PNR agreement with the United States of America, n. 17 above.

[29] See "EU: European Commission to propose EU PNR travel surveillance system", n. 18 above.

[30] UK House of Lords, European Union Committee, 15th Report of Session 2007-08, *The Passenger Name Record (PNR) Framework Decision*, http://europapoort.eerstekamer.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vhwed1h370px.pdf

[31] EU-US PNR Agreement, n. 20 above, para. 2

[32] ARTICLE 29 Data Protection Working Party, letter from the Chairman to Dr. Alberto Costa, Minister of Justice, Portugal, Brussels, 26 November 2007, available from the Statewatch website at http://www.statewatch.org/news/2007/nov/eu-dp-korea.pdf

[33] See "Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes", MEMO 07/4449, Brussels, 6 November 2007, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en; see also "Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes", Slovenian Presidency Paper, Informal Justice and Home Affairs Council, 25-26 January 2008, http://europapoort.eerstekamer.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vhscnw164bv0.pdf and the "Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement Purposes", OJ 2008 C 110/1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:110:0001:0015:EN:PDF

Clearly, there seems to be a trend towards the increased usage of PNR. As the various bilateral agreements between the EU and other states show, it is vital that care is taken to ensure that privacy concerns are carefully considered. Primarily, this involves a constant balancing of the security gains against privacy concerns. Data protection rules require that whenever information of this type is collected, there must be a clear justification for it. In cases where it is deemed justified, it is crucial that sensitive information is handled in a secure, agreed-upon manner and used exclusively for the stated purpose. As with API, international standards governing the transfer of PNR would be welcome. In recent years, ICAO has been leading developments in this direction and has published the ICAO Passenger Name Record Data Guidelines.[34]

ii) CARRIER SANCTIONS

National migration law in a number of states requires common carriers servicing their territories internationally to verify the travel documents of all boarding passengers. Sanctions are imposed upon carriers that fail to comply. The sanctions are an integral part of the pre-embarkation activities abroad and complement measures such as the issuance of visas, the stationing of ALOs and the transfer of API. Essentially, the idea is to provide airlines with an incentive to institute thorough identity and document checks by penalizing carriers transporting individuals who are subsequently denied entrance into the country of destination. This can lead to substantial cost savings as well as contribute to security, as those travelling on false documents who may pose a threat are prevented from embarking.

In 1985, States parties to the Schengen Convention in Europe agreed to impose sanctions on their domestic carriers on behalf of the States receiving the undocumented persons, and also in order to require their carriers to take responsibility for returning any passengers delivered to States parties without proper documentation. In 1997, the provisions of the Schengen Convention, the 1991 Schengen Implementing Agreement and accompanying measures (collectively known as the “Schengen acquis”) were incorporated by the Amsterdam Treaty into the Treaty of the European Union and the Treaty Establishing the European Community. They now apply to all EU Member States except for Ireland and the UK. A 2001 Council Directive (2001/51/EC of 28 June 2001) reinforces the Schengen requirements, adding that the required sanctions must be “dissuasive, effective and proportionate”, with a minimum fine of EUR 3,000 per inadmissible passenger.[35]

Carrier sanctions also provide ALOs with a large part of their authority. Although they have no legal power to prevent passengers from boarding a flight, this is unlikely to occur if the carrier is aware that boarding a passenger against the advice of the ALO will likely result in fines and/or responsibility for returning the passenger to the point of origin.

Furthermore, carrier sanctions are employed by countries to ensure that carriers comply with regulations governing the transfer of passenger information. A 2004 EU Directive on Carriers sets out the conditions for imposing financial sanctions on

[34] Passenger Name Record (PNR) Data Guidelines, 9 June 2005

[35] Council Directive 2001/51/EC of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985, OJ 2005 L 187/45, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:187:0045:0045:EN:PDF

carriers failing to submit API data.[36] As many countries have made the transfer of API by airlines mandatory, most have also instituted financial penalties for non-compliance. This includes countries such as Australia, Canada and the US. Carrier sanctions are likely to be most effective when combined with the stationing of ALOs and interactive API systems (also known as APP, Board/Don't Board, Red Light/Green Light, or APIS Quick Query), allowing the carrier to determine as early as check-in whether a passenger is likely to be denied entry at the point of destination.

However, in countries which have legislation in place regarding the transfer of PNR, carrier sanctions also apply to non-compliance in this area. At times, this has posed a problem. As the negotiations between the US and the EU have shown, airlines may be caught in the middle, threatened by fines whether they comply or not.[37] In the EU-US case, in the absence of an agreement between the two parties, airlines could be fined for breaking EU data protection laws if they submitted the information. On the other hand, they could face fines and potential loss of landing rights in the US if they failed to comply. This illustrates the importance of bilateral and multilateral agreements concerning information exchange, including harmonized standards regarding PNR. Meanwhile, IATA has suggested that "PNR requirements should be suspended in cases where national law in the country of departure prevents the transfer of PNR data, i.e. where airlines are caught in the middle".[38]

[36] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 2004 L 261/24, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:261:0024:0027:EN:PDF

[37] R. Koslowski (2004) "Possible steps toward an international regime for mobility and security", Global Commission on International Migration (GCIM), Global Migration Perspectives No. 8, October 2004, http://www.gcim.org/attachements/GMP%20No%208.pdf

[38] "Recommendations Relating to ICAO's Best Practices Relating to Passenger name Record (PNR)", ICAO Working Paper, Facilitation Panel, 5th Meeting, Montréal, 31 March-4 April 2009, Doc. FALP/5-WP/26, http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp26_en.pdf

CHAPTER 3
IDENTIFICATION SYSTEMS AND BIOMETRICS

Many developments and trial projects in the field of migration management involve biometrics. Biometrics is the study or use of measurable biological and physiological (sometimes also behavioural) characteristics to establish or verify the identity of an individual. Although it has applications in many areas other than border security, this is certainly one of the areas where it has significant potential to improve security. By deploying one or more biometric verification techniques, border security officials are able to improve their ability to verify that an individual's identity matches the one stated on the identity document presented. This is known as one-to-one verification. Should they need to, border officials can also perform a one-to-many search (identification), cross-matching a "live" sample of a person's biometric data, captured at the border control, against a database containing biometric templates. The security-enhancing capacity of biometrics stretches over a range of applications, from improvements in the integrity of travel documents, to more effective pre-inspection measures such as APP. In addition to improving security, biometric techniques also hold significant potential for travel facilitation by improving processing times and allowing for some degree of automation in border and customs controls. Public acceptance of such programmes historically has been strong, and support for them has measurably increased as a result of the 9/11 attacks. Unlike images and text information, biometric data are stored as secure templates that can only be "opened" by those who are specifically authorized to have access. While some critics have attempted to label biometrics as a risk to personal privacy, their inherent ability to safeguard data through the use of highly encrypted algorithms has led them to be recognized as "privacy enhancing technologies[39]" by the EU.

A number of different physiological and behavioural features have been tested as biometric identifiers, but some of the main ones are facial imaging, fingerprinting, iris scanning, hand geometry and voice recognition. More recent techniques involve the identification of characteristics such as DNA, hand veins, the ear canal, or a person's way of walking. In the end, the chosen biometric feature depends essentially on what its purpose is, since all techniques have advantages as well as disadvantages. Criteria that may influence the choice of biometric identifier include the time it takes to capture and process the data, the surrounding conditions (noise, light, etc.), the accuracy with which a person is correctly identified, the degree of public acceptance, as well as the costs of implementation and interoperability with other technologies.

i) BIOMETRICALLY ENHANCED TRAVEL DOCUMENTS

In the field of migration and border security, the most important developments in biometrics relate to the introduction of **electronic Machine-Readable Travel Documents (e-MRTDs)**. These documents include passports (national, diplomatic and refugee) and identity cards which include biometric data stored on a chip.

At the forefront of standardization and international cooperation on travel documents is the International Civil Aviation Organization (ICAO). In Document 9303, Part 1, it

[39] EC press release, "Promoting Data Protection by Privacy Enhancing Technologies (PETs)", May 2007, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/598&format=HTML&aged=0&language=EN&guiLanguage=en

sets out specifications for machine-readable travel documents.[40] The sixth edition of this document contains specifications for machine-readable passports (MRPs) in Volume 1, as well as biometrically enhanced machine-readable passports, known as electronic passports or e-passports, in Volume 2.

Starting in 1998, the New Technologies Working Group (NTWG) of the ICAO Technical Advisory Group conducted extensive studies to establish the fundamentals for a globally interoperable system of biometric identification. These studies focused on the travel facilitation and identification confirmation aspects of biometrics and took into account national privacy laws, as well as the differing degrees of public acceptance of the use of various biometric identifiers. ICAO has issued specifications for the use of face imaging as the primary biometric identifier to be used in e-passports, notably with the perspective that this supported identity confirmation and travel facilitation through verification "on the move". This involves capturing images of the face and using facial geometry to verify or establish a person's identity. ICAO further recommends the use of a contact-less integrated circuit (IC) chip to store the information. By means of Radio Frequency Identification (RFID), the information contained on the chip is transmitted by radio waves to a reader that is able to read e-MRTDs.

ICAO specifies that the IC chip should contain an image of the document-holder's face, as well as the information contained in the machine-readable zone of the passport. In addition, countries wishing to store further information or biometric identifiers in the passport, such as place of birth, fingerprints or iris images have the option of doing so. So far, at least 34 countries of the approximately 75 countries[41] which have issued e-passports have chosen to do so.

There are three main issues which can have an impact on the operational benefits of biometric technologies. These are:

1. enrolment
2. standardization
3. infrastructure at the border environment.

Enrolment. Enrolment is quick in cases where a country decides to collect biometric data from non-nationals upon entry, as the US does under its United States Visitor and Immigrant Status Indicator Technology (US-VISIT) programme.[42] Regarding passports, more then 75 countries issue e-passports at present, but it should be remembered that no country did so only a few years ago. In fact, the use of biometrics can improve the issuance process itself by helping to identify the applicant and ensuring that he or she does not already hold a passport under another name. This could act as an additional incentive for states to introduce biometric technology, which means that a key issue here is identity confirmation, followed by quality control of the enrolled biometric identifiers selected by ICAO. To ensure that interoperability is established, the stored biometric identifiers have to comply with international specifications and will need to be checked before issuing a travel document. The 2010 global deadline set by the ICAO for machine-readable passports must be seen as a first step towards the universal issuance of e-passports.[43]

[40] See ICAO, MRTD at http://www2.icao.int/en/mrtd/Pages/default.aspx

[41] "2009/2010 Annual Report on ePassports", Keesings Journal of Documents & Identity http://www.securitydocumentworld.com/index.cfm?&m1=e_0&m2=e_0&m3=e_0&m4=e_0&subItemID=1572)

[42] More information is provided on US-VISIT below in Chapter 3, section (ii) on "RECENT IDENTIFICATION SYSTEMS INITIATIVES".

[43] For more information, see http://www.hasbrouck.org/documents/ICAO9303-pt1-vol1.pdf

Standardization. As technologies evolve and the number of people with e-MRTDs increases, standards must be followed to ensure interoperability. With the ICAO specifications on e-MRTDs, much has been achieved already. As relevant technologies evolve, there should be a focus on backwards compatibility, since travel documents are valid for five or ten years in general. With the likely increase in the application of biometric technologies worldwide, however, it is important that procedures and requirements are coordinated. An example in this regard is the automation of certain controls at airports, for which the ICAO has issued the Guidelines on e-MRTDS & Passenger Facilitation.[44]

Infrastructure. The impact of biometrics will depend on the degree of infrastructure available in a border environment. This includes the deployment, at border control points, of readers able to process e-MRTDs, as well as the technology needed to process biometric verification or identification. It also includes systems able to store and transmit biometric information in a secure manner. Upgrading infrastructure is costly and, in cases involving databases and information sharing, also very sensitive. Developments in this area can thus be expected to take considerable time.

Data Protection and Privacy Concerns

While there have been rapid developments relating to biometrics in recent years, driven by the need felt by states to ensure the security and integrity of their borders, a number of criticisms have also been raised.[45] In particular, critics have focused on several areas related to the spread of biometric databases for identification purposes:

- There is a possibility of function creep, whereby biometric data collected for one purpose is used for another without the consent of the individual. In terms of migration controls, an example of this would be where data collected for basic immigration processing purposes might subsequently be used to audit welfare recipients.
- Biometric data might also be utilized to monitor individuals based on suspicions about their activities, health status or any other criteria not directly related to migration.
- Some forms of biometric measurement can inadvertently determine an individual's health status. For example, some speculate that an iris scan might provide an indication of the state of a person's health to the data collection agency.
- Recent history is replete with examples of the difficulties that confront authorities in maintaining the integrity of sensitive and classified data. The existence of large globally accessible databanks of biometric information would inevitably attract the interest of persons and organizations with illegitimate aims.

Recognizing the importance of biometrics for border security and for protecting the reliability of immigration regimes, but also cognizant of the need to protect the individual's right to privacy, a number of international organizations have developed guidelines designed to maintain the integrity of privacy protocols in the face of the growing use of biometric scanning methods in the management of migration flows. These include the United Nations (UN) Guidelines for the Regulation of

[44] "Guidelines on e-MRTDS and Passenger Facilitation", ICAO Working Paper, Technical Advisory Group on Machine-Readable Travel Documents, (TAG – MRTD), 18th Meeting, Montréal, 5-18 May 2008, Doc. TAG-MRTD/18-WP/3, http://www.icao.int/icao/en/atb/meetings/2008/TAGMRTD18/TagMrtd18_wp03.pdf

[45] IOM (2005) *Biometrics and International Migration*, International Migration Law No. 5

Computerized Personal Data Files,[46] the Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data,[47] and finally the OECD Guidelines for the Security of Information Systems and Networks.[48] Underpinning these guidelines is the right to privacy embodied in Article 17 of the International Covenant on Civil and Political Rights (1966) and also Article 14 of the UN International Convention on the Protection of the Rights of all Migrant Workers and their Families (1990), which as of May 2009 had been ratified by 41 countries.[49]

A review of the guidelines developed to regulate the collection of biometric data would highlight the following factors:[50]

- Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the subject.
- The purposes of data collection should be specified at the time of collection; data collection should be necessary for the purposes for which it is used; and data should not be used in a way incompatible with those purposes.
- Personal data should be kept accurate, complete and up to date.
- Personal data should be held for no longer than is required for the purpose for which it was collected.
- Data likely to give rise to unlawful or arbitrary discrimination should not be compiled, unless domestic law provides appropriate safeguards.
- Personal data should be adequately safeguarded against relevant human and non-human security risks.
- There should be a general policy of openness about practices and policies *vis-à-vis* the collection and use of personal data.
- An individual should have the right, without undue delay or expense, to know whether or not a body holds data relating to him/her, to be able to access the information, have information corrected if incorrect, and obtain a remedy if this is not complied with.

In addition to fears concerning the collection and sharing of biometric data by authorities, there has also been concern that biometrically enhanced passports may be vulnerable to what is known as “skimming”. This involves an unauthorized system or person accessing the data contained on the IC chip. It is the contact-less transfer feature of the biometric data through the RFID system that may lead to this vulnerability, since someone with malicious intent would only have to be in proximity in order to gain access to the information. Connected to this is the fear that data could be intercepted while it passes between the document and the reader, at border control for instance.

In order to prevent such scenarios, e-MRTDs will typically include what is known as Basic Access Control (BAC).[51] Incorporating several security features, BAC includes an access mechanism whereby the machine-readable zone (MRZ) of the travel document must first be optically read. Based on the information in the MRZ, a key is produced, which allows the electronic reader to access the information contained in

[46] http://www.worldlii.org/int/other/PrivLRes/1990/1.html

[47] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[48] http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

[49] See the website of the Office of the UN Office of the High Commissioner for Human Rights (OHCHR) at http://www2.ohchr.org/english/law/.

[50] IOM (2008) *Future Tools to Deal with Irregular Migration and Smuggling of Migrants in the European Union*

[51] See “Guidelines on e-MRTDS and Passenger Facilitation”, n. 34, above.

the chip. The security advantage of this is that the document has to actually be presented and opened to a reader in order for the biometric information to be "unlocked", making it much more difficult for third parties to access the data. In addition to this, the data stream that passes between document and reader once the information has been unlocked will normally be encrypted, making "eavesdropping" more difficult. Again, the information necessary to generate the decryption key can only be accessed optically by reading the MRZ.

Furthermore, Extended Access Control (EAC) provides stricter protection against unauthorized reading of sensitive data, like fingerprint and iris images, than Basic Access Control does for the less sensitive data (the face). Through EAC, an inspection system can only access areas on the eMRTD's chip to which it has been authorized by the eMRTD's issuer.[52]

Further security mechanisms have been developed to prevent identity fraud and the use of stolen documents. Many of these focus on ways to ensure the authenticity and integrity of e-MRTDs. For example, ICAO specifications include the mandatory use of digital signatures by authorities issuing such documents. When the ICAO public key chain is properly installed in the border control system, the inspection system can verify that the document has been issued by a legitimate authority and that it has not been fraudulently altered. This is called passive authentication. It is also possible to verify the authenticity of the chip by sending an encrypted challenge based on a public key (which is information that can be read from the chip) to the high security memory in the chip, which sends a response based on its internal, private key. By comparing the challenge to the response, the inspection system can establish whether the two keys belong together. This is called active authentication. Since it is not possible to separate the private key from the chip, this test will verify that the chip belongs with the document and thus is not a copy.

Such authentication methods could greatly contribute to enhanced security as well as privacy. However, it is clear that efficient and secure mechanisms are needed for the exchange of certificates between authorities authorized to examine e-MRTDs. As a crucial safety measure, this also includes the sharing of revocation lists, which contain information on compromised keys. For the purposes of sharing such information, the ICAO has established the Public Key Directory (PKD),[53] which has been operational since March 2007.[54] This enables legitimate authorities to electronically share and access accurate and updated certificates. It has the advantage of not requiring any personal information to be shared, thus limiting concerns about privacy and data protection. However, by May 2009, only 13 countries had signed up to the PKD and only half of them were using it.[55] In order for the system to achieve its potential for enhanced security, it is crucial that more countries adopt this procedure.

[52] See "Basic Access Control/Extended Access Control in e-Passports", ICAO Working Paper, Technical Advisory Group on Machine-Readable Travel Documents, (TAG – MRTD), 18th Meeting, Montréal, 5-18 May 2008, TAG-MRTD/18-WP/6, http://www.icao.int/icao/en/atb/meetings/2008/TagMRTD18/TagMrtd18_wp06.pdf.

[53] For more on the PKD, see http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx.

[54] See "Guidelines on e-MRTDS and Passenger Facilitation", n. 34 above.

[55] For more info, see http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD_Facts.pdf.

ii) RECENT IDENTIFICATION SYSTEMS INITIATIVES

As the number of people holding identification or travel documents containing biometric data has increased, so has the number of programmes making use of biometric technologies to provide additional security and to facilitate travel. Broadly, the kind of initiatives being implemented can be divided into two categories: those that are primarily security-enhancing and are designed to collect biometric data on passengers, and those that are intended to facilitate travel by automating border processes.

The **US-VISIT programme** belongs to the first category. Based on legislation enacted after 9/11, US-VISIT involves the capture of digital photographs as well as fingerprints of practically all non-US citizens arriving by air, land or sea. The Enhanced Border Security and Visa Entry Reform Act requires all US embassies and consulates to have the capacity to collect biometric data as part of the visa interview process. This was developed into the Biometric Visa Program. In the visa decision procedure, this information can be run against watch lists. Once the passenger arrives at the border, the biometric data can be compared to data captured from the newly arrived passenger to verify that he or she is the person to whom the visa was issued.[56] The information collected upon entry can also be cross-checked against watch lists before the passenger is admitted to the country. US-VISIT is intended as an entry-exit system, processing passengers departing the country as well as those arriving. The exit part of the programme is still being developed.

The **Visa Information System (VIS)** has been launched by participating EU Member States.[57] Forming part of the efforts to implement a common visa policy, it provides for storage and electronic sharing of information concerning visas and visa applications between EU Member States. Visa applicants have their photograph and the fingerprints of all ten fingers taken. In addition, VIS contains written information such as the name, address and occupation of the applicant, date and place of the application, and, importantly, any decision taken by the Member State responsible to issue, refuse, annul, revoke or extend the visa. This information can then be accessed by consulates and embassies issuing visas as well as border control authorities. When a live biometric sample is captured at a consulate or border, VIS allows cross-checking, using a Biometric Matching System, to verify whether the individual is already in the system. Once it is fully operational, it is estimated that the database will contain 70 million sets of fingerprints. VIS is intended to improve the management of visa-issuing procedures, as well as prevent instances of “visa shopping”, whereby individuals apply for visas in several different Member States under different identities. VIS can thus contribute to prevention of serious crime and terrorism, by making it more difficult for known criminals and terrorists to enter the Schengen states. Certain national authorities, such as the police and EUROPOL, can access the database, but only in instances when it is deemed necessary, and then only under controlled circumstances.[58] The VIS Regulation allows consulates and other competent authorities to start using the system when processing visa applications and to check visas. The VIS Decision allows police and law enforcement

[56] See Koslowski, n. 29 above.

[57] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS)

[58] For more information, see “Visa Information System (VIS): The JHA-Council reaches a political agreement on the VIS Regulation and VIS Decision”, Doc. IP/07/802, Brussels, 12 June 2007, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/802&format=HTML&aged=0&language EN&guiLanguage=en; and http://www.europarl.europa.eu/sides/getDoc.do?language=EN&type=IM-PRESS&reference=20070606IPR07543.

authorities to consult the data under certain conditions that ensure a high level of data protection.

The **EURODAC**[59] system, which has been operational since 15 January 2003, was created by the Regulation of the Council of Ministers.[60] It is an information system set up with the purpose of identifying the Member State responsible for an asylum application lodged within the European Union, in order to speed up the asylum procedure. It centres on EU Member States sharing the fingerprint records of those who have crossed an external border of the Community in an irregular manner and who have claimed the right to asylum in more than one Member State. EURODAC aims to enable EU Member States to determine much more effectively than in the past whether a foreign national (i.e. asylum seeker or apprehended irregular migrant) within the borders of one Member State has previously claimed asylum in another Member State. By allowing better control over asylum seekers' requests, this system contributes to the sustainability of the EU asylum regime while indirectly contributing to overall border control efforts. EURODAC operates through a unit within the European Commission equipped with a central database that allows for the electronic transmission of fingerprints data between Member States.

On 8 July 2008 the Commission adopted two legislative measures providing access to the EURODAC database for the police. The first measure consists of an amendment to the current EURODAC regulation, setting the fight against crime as a priority on the EURODAC operative agenda. The second measure is a Draft Decision based on Title VI TEU regulating the modalities to access to EURODAC for law enforcement purposes. In detail, the Commission measures propose to authorize the comparison of fingerprints which are contained in EURODAC with fingerprints in the possession of national law enforcement authorities or Europol for the fight against terrorist offences. The measures are also designed to regulate the procedure through which law enforcement authorities request comparisons with the EURODAC database and the conditions under which such requests can be forwarded. Furthermore, the measures provide a series of guarantees aimed at ensuring the protection of the personal data of the persons concerned and safeguarding the right to asylum.

The second category, in addition to large-scale security enhancing projects such as US-VISIT and VIS, includes a number of pilot projects as well as more permanent programmes that have been implemented at airports and border controls, usually targeting a limited number of trusted travellers and using biometric technologies to facilitate processing by automating control procedures (**Automated Border Control (ABC)**). In consideration of the growing number of people crossing international borders, such automation can be very valuable to regular passengers, but it is also beneficial from a security standpoint. By automating border processing partly or fully, personnel can focus on cases that attract attention and where a closer examination is warranted.

[59] The implementation rules for EURODAC are set out in Council Regulation (EC) No 407/2002 of 28 February 2002.

[60] Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:062:0001:0005:EN:PDF

Since 2001, frequent flyers with EU passports passing through Schiphol Airport in Amsterdam have been able to register for **PRIVIUM**.[61] The programme involves the creation of a smart card for each traveller, containing a template image of the person's iris. At border control, the passenger simply presents this card to the ABC system and looks into a camera which performs a live scan of the passenger's iris. The live sample is matched against the template on the smart card. If the data match, identity is verified and the passenger can proceed through border control. The whole process takes 10-15 seconds.

In the UK, frequent flyers have also been able to enrol in an ABC scheme known as **IRIS**. Although essentially performing the same operation as the Schiphol programme, the UK scheme stores the template data in a secure database, obviating the need for a token such as a smart card or chip. Instead, the passenger looks into a camera at the border control and the captured iris data is used in a one-to-many check against the database to establish the identity of the passenger. The UK has also performed trials with fingerprints as the favoured biometric, under its **miSense** programme.[62] Automated border controls using fingerprints as the chosen biometric have also been implemented in Hong Kong Special Administrative Region of China, Singapore and Malaysia.

In Australia, another programme has been implemented. Starting in 2007, Australian nationals with e-passports have been able to use **Smartgate**. Instead of iris recognition, the Australian system, which has been implemented at selected Australian airports, uses facial recognition to establish a match between the passenger and the travel document presented, in this case the e-passport containing the biometric template. Since its inception, the programme has been extended to include e-passport holders from New Zealand, and future developments could see the system processing a broad range of nationals holding ICAO-compliant e-passports.

In Portugal, the **RAPID** scheme implemented in a number of airports also uses e-passports and facial recognition for automated border control. The programme, which was initialized in 2007, has so far been limited to citizens from the EU and the European Economic Area (EEA), however.

The type of automated system implemented in Australia and Portugal would seem to hold the greatest potential since it does not require any form of enrolment and is compatible with the standardized e-passport, which is issued to a steadily growing number of people. In essence, the issuance of biometrically enhanced passports constitutes enrolment in this kind of ABC scheme. It is therefore a fair prediction that the future will bring the expansion of ABC programmes working with official e-MRTDs. Signs pointing in this direction include the European Commission's proposal for an EU-wide ABC system processing all EU nationals as well as "registered travellers" from third countries.[63]

[61] For guidelines and examples of automated control programs, see "Guidelines on e-MRTDS and Passenger Facilitation", n. 34, above.

[62] For more information on miSense, see the website of the British Airports Authority (BAA) at http://www.baa.com/portal/site/baa/menuitem.6a4740fe62e293a4b03f78109328c1a0/.

[63] European Commission, Communication, *Preparing the next steps in border management in the European Union*, COM (2008) 69 final, 13.2.2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:PDF

CHAPTER 4
INFORMATION EXCHANGE AND CROSS-BORDER COOPERATION

The increasingly global nature of international terrorism renders it a uniquely difficult challenge for the international community. This is particularly so when addressing international terrorism requires the kind of international cooperation which states have been historically reluctant to embrace. For example, the need to initiate deeper forms of intelligence sharing, to place greater emphasis on harmonizing immigration policies with the expectations of the wider international community, and to become more transparent in the issuing of identity documentation are requirements that can sometimes sit uncomfortably with traditional notions of national sovereignty.

Despite these obstacles, over the last several years the international community has witnessed an impressive array of multilateral and bilateral initiatives designed to strengthen cooperation against terrorism. Not all of these initiatives have related directly to the issue of migration, but it should be remembered that cooperation in outwardly peripheral areas such as intelligence sharing and capacity building in the use of electronic data collection and information management can have important downstream benefits for the maintenance of safe migration programmes.

Countries engaged in the fight against international terrorism require effective international data exchange mechanisms. Terrorists can and do use international borders to their advantage, sometimes relying on the possible inability to exchange data internationally – a weak link in the general fight against international crime. Indeed, "the Final Report of the US 9/11 Commission, published in 2004, identified a reluctance by different security authorities to share information with one another as one of the main causes of the failure to prevent the terrorist attacks".[64]

Arrangements pertaining to information exchange may involve cooperation between immigration authorities, border and customs controls, carriers, or police and law enforcement. This can take place between actors within a country as well as in the international arena. Clearly, the success of such cooperation will depend on a number of factors, such as the sensitivity of the information, the number of actors involved and the purpose for which the information is to be exchanged.

With regard to the sharing of information databases, while recognizing human rights and civil liberties concerns, more governments have taken the position that the current level of threat from international terrorism legitimately permits a proportionate response that can intrude on individual human rights, including the right to privacy. However, the impact of such possible intrusions can be lessened where governments' use of information is restricted, within a legal framework, to specific purposes, e.g. for law enforcement or immigration purposes, and the framework permits use only for such purposes. The case of VIS appears to be instructive in this regard, with access to this information carefully specified and strictly regulated.

Privacy concerns will naturally constrain information sharing, at times limiting shared resources to that of the most protective participant. In the EU context, data protection also limits the capacity of the EU and its Member States to share information with non-EU states. Although authorities in charge of security may sometimes consider

[64] House of Lords European Union Committee, 21st Report of Session 2006-07, *The EU/US Passenger Name Record (PNR) Agreement*, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf, p. 7

this as a source of obstacles and frustration, national privacy and data protection laws also act as a safeguard, ensuring that any decision to share potentially sensitive information, whether nationally or internationally, is carefully considered and deemed both necessary and proportionate.

Nonetheless, bilateral agreements that include data exchange are common and can be illustrated by the **Smart Border** project between Canada and the US. Elaborated within months of 9/11, the agreement involves increased intelligence and information sharing as well as shared lookout lists.[65] In addition, the two countries have agreed to share API as well as PNR data with each other.

As noted earlier, regarding data sharing for the purpose of pre-processing of passengers, the transfer of API data has recently become more widespread and international organizations such as the ICAO have been involved in setting standards and issuing recommendations for this practice. The transfer of PNR data, however, has been more controversial, as it has greater implications for privacy. Nonetheless, recent bilateral agreements between the EU and Australia, Canada and the US, respectively, provide some indication that progress can be made even in developing the principles that would allow more data to be transferred while ensuring that adequate privacy protection measures are put in place

Other bilateral agreements involving information exchange include: the agreement from November 2005 between Canada and EUROPOL on sharing counter-terrorism intelligence and information on criminals; the 2007 agreement between Australia and EUROPO; and agreements between Russia and other states in the Commonwealth of Independent States (CIS).

i) INTERNATIONAL, SUPRANATIONAL AND REGIONAL INSTITUTIONS FOR MULTILATERAL COOPERATION

Information exchange and international cooperation to prevent terrorism often takes place through multilateral institutions as well as by means of bilateral agreement. A number of international, supranational and regional organizations are particularly noteworthy for initiatives developed in a range of areas, from cooperation on law enforcement to counter-terrorism legislation and cooperation in border security.

The UN **Counter-Terrorism Committee (CTC)** was established by the UN Security Council Resolution 1373 (2001), which was adopted shortly after the 9/11 attacks in the US. In very broad terms, Resolution 1373 (2001) requires States to attack the funding of terrorism and to deny support to, and prevent terrorist acts. It also imposes on States the duties to deny safe haven to terrorists, to install effective border controls, to enact domestic counter-terrorism legislation, and to bring to justice those who commit terrorist acts. It further calls upon States to exchange information regarding terrorist actions, cooperate to prevent the commission of terrorist acts, and enter into the relevant international instruments relating to terrorism.

The CTC consists of all the members of the Security Council. Its primary task, constituted by delegations from the 15 Member States of the UN Security Council, is “to monitor the implementation of this resolution, with the assistance of appropriate expertise.” The Committee also calls upon all States to report to it “on the steps they have taken to implement this resolution.”

The Committee writes regular reports, where it describes the progress made by UN Member States in the main areas of counter-terrorism legislation, counter-financing

[65] Koslowski, n. 29 above

of terrorism, border control, domestic security and law enforcement, and international cooperation. In these reports, it identifies areas where efforts need to be strengthened, and issues recommendations to this end. Of special importance in this regard is the Counter-Terrorism Committee Executive Directorate (CTED), which was established in 2004. Among other things, it undertakes country visits in order to monitor progress and identify weaknesses in areas of counter-terrorism relevant to the implementation of Resolution 1373. These country assessments form the basis for the general reports issued by the CTC on global progress towards implementing the resolution.[66]

The CTC also works to coordinate the various counter-terrorism activities undertaken by states and organizations. Towards this end, it provides a list of best practices organized to correspond to the obligations in the resolution.[67] It also organizes high-level meetings, where states and international organizations discuss developments and issues related to counter-terrorism. The last "Special Meeting" (5th) was held in Nairobi, Kenya, in 2007 on the theme "Prevention of Terrorist Movement and Effective Border Security". Papers were presented in areas such as asylum and refugee protection, aviation security, and law enforcement. Participants included international organizations such as ICAO, the International Monetary Fund (IMF) and IOM, regional organizations such as the African Union and the League of Arab States, as well as UN agencies such as the United Nations High Commissioner for Refugees (UNHCR).

The CTC has played a very important role in beginning the long and critical process of building the anti-terrorism capacity of states. The most significant challenge, however, that still lies ahead of CTC in terms of performance and accomplishments is its ability to help build the capacity of states to protect and safeguard human rights while combating terrorism. Much of the CTC's future success in combating this scourge depends on its willingness to also assist in building the capacity of States to comply with their human rights obligations and the rule of law while strengthening their counter-terrorism legislation.[68]

INTERPOL works closely with states, as well as regional and international organizations. The organization has played a key role in promoting information exchange between states, with the aim of providing frontline police authorities and border officers with the information they need to identify suspected individuals. Essentially, INTERPOL aims to provide information on wanted or suspected individuals and on travel documents which have been reported stolen or lost. In order to perform these twin tasks, INTERPOL has developed the global police communications system known as **I-24/7**. This system allows for real-time queries regarding wanted individuals, and quick and secure information exchange between law enforcement authorities.

A particularly noteworthy initiative developed by INTERPOL is the global **Stolen and Lost Travel Document (SLTD)** database. This constantly growing database contains records of over 13 million travel documents from more than 120 different countries,[69] and allows police and border control officers to perform an automated scan of travel documents presented to them against the database. This initiative

[66] For the latest report, see http://www.un.org/sc/ctc/countryreports/Creports.shtml.
[67] See http://www.un.org/sc/ctc/practices.html.
[68] Refer to the section on "Terrorism and Human Rights".
[69] See the keynote speech by R.K. Noble, Secretary General, ICPO – INTERPOL, United Nations 5th Special Meeting of the Counter-Terrorism Committee with International, Regional and Sub-regional Organizations, Nairobi, 28-31 October 2007 (http://www.un.org/sc/ctc/pdf/INTERPOL_knote.pdf).

makes it more difficult for terrorists and other criminals to avoid detection and to cross international borders by using fraudulently altered travel documents, but in order for it to be truly effective in this regard, the SLTD database must be made available widely to law enforcement officers and border officers, rather than limited to central authorities. Therefore, INTERPOL has developed the **FIND/MIND** systems, which allow authorities at airports and border crossings to directly access INTERPOL's databases. Starting with Switzerland in 2005, the project has expanded and, today, a number of countries have made the SLTD database available throughout their territory.[70]

Another programme developed by INTERPOL is the **Fusion Task Force** which constitutes a global network of counter-terrorism contact officers sharing information on terrorist groups, their organizational structure, membership and financing.

The European Union is in itself perhaps one of the best examples of supranational cooperation and information exchange on the regional level. In addition to the previously discussed VIS and EURODAC, a number of other projects constitute further examples of cooperation involving measures situated at the intersection of security and migration, such as EUROPOL, SIS and the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX).

EUROPOL, established under the Maastricht Treaty of 1992, is an EU-wide law enforcement support mechanism relying on intelligence from Member States on drugs, organized crime, terrorism and human trafficking. It provides support to the Member States in the prevention, investigation and analysis of crime, and allows for appropriate threat and risk assessment. EUROPOL provides operational support with intelligence bulletins and analytical work files and supports joint investigations and operations. It also publishes annual trend reports on terrorist incidents and terrorist groupings constituting a potential threat.

In the medium term, there is an intention to give EUROPOL wider scope for supporting investigations of networks facilitating irregular immigration into Member States, including trafficking in human beings. More importantly perhaps, it is also intended to provide support for Member States and to participate in the collection and exchange of information among bodies responsible for implementing the laws which apply in such cases.

The **Schengen Information System (SIS)** was set up in response to the abolition of internal EU border controls. It allows officials from participating countries to access data on specific individuals of interest and on goods which have been lost or stolen.[71] The SIS database can be accessed by police, border police, customs officers and, to a more limited extent, by immigration officials. SIS therefore plays an important role in protecting the integrity of migration regimes within the EU. At the same time, the system is designed to protect the right of movement of lawfully resident third-country nationals in the EU.

[70] http://www.interpol.int/public/icpo/pressreleases/pr2007/pr200715.asp

[71] Although the Republic of Ireland and the UK have not lifted border controls in accordance with the Schengen Agreement, they still utilize SIS, as do three non-EU countries, Iceland, Norway and Switzerland, which are participating in application of the Schengen acquis.

The SIS includes data supplied by all EU Member States. As it relates to migration and border protection, this data is used for:

- arrest for extradition purposes;
- identification of foreign nationals for whom an alert has been issued for the purposes of refusing entry;
- persons subjected to surveillance for the purposes of prosecuting crimes or preventing threats to public security.

The capacity for SIS to foster higher levels of intra-agency information exchanges, more effective forms of border surveillance and greater use of cross-jurisdictional secondments of EU law enforcement officials implies that it continues to be a critically important element in maintaining the integrity of the EU's border control regime.

Therefore, in 2001, in response to the rapid increase in cross-border population movements within the EU and the obstacles confronting new Member States participating in the SIS, the European Commission decided to move towards the development of a second-generation Schengen Information System (SIS II). SIS II will not only increase data capacity, but will also be able to store digital images and biometric data. Its deployment date has been postponed and is currently under discussion.[72] Supplementing SIS II is an information database known as SISNET designed to facilitate the real-time sharing of certain information about persons of interest between police, customs and the judiciary of all EU Member States via satellite navigation technology (linked to the European Geostationary Navigation Overlay Service) and signal-in-space Internet technology.

FRONTEX[73] was established in 2004 with the aim to coordinate operational cooperation between EU Member States in the field of management of EU external borders. Other tasks include assisting Member States in the training of national border guards, carrying out risk analyses and following up on the development of research relevant to the control and surveillance of external borders. FRONTEX also provides Member States with technical and operational assistance in areas relating to border security. An evaluation of FRONTEX recently conducted by the European Commission has praised its work. In 2006 and 2007, FRONTEX purportedly apprehended 53,000 people or refused them entry at the border. Furthermore, the Commission praised the European Patrols Network (EPN), a network of bilateral cooperation among the EU's Mediterranean Member States. More interestingly, the review of the Central Record of Available Technical Equipment (CRATE), FRONTEX's “toolbox”, showed that at present only a few heartbeat detectors and surveillance plans have been requested. Also, the Rapid Border Intervention Teams (RABIT) have yet to be put into action. For the near future, the Commission has advanced two proposals. One proposal is the establishment of regional FRONTEX offices (specialized branches of the agency) and the other is the expansion of CRATE.[74]

[72] Council Conclusions on SIS II, February 2009, http://www.eu2009.cz/scripts/file.php?id=18357&down=yes

[73] Council Regulation No 200772004 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

[74] See “Perfection of the Border Regime”, FRONTEX's website at http://frontex.info.pl/content/perfection_border_regime.

The **Organization for Security and Co-operation in Europe** (**OSCE**) has instituted a separate instrument for the coordination and facilitation of OSCE initiatives aimed at preventing terrorism; the **Action against Terrorism Unit (ATU)**. The ATU, which was established in 2002, is tasked with supporting participating states with technical assistance in counter-terrorism projects, as well as capacity-building and training. In addition, it maintains links with external partners and acts as a counter-terrorism information source for participating states as well as other organizations.

The ATU also assists participating states in the ratification and implementation of the UN Conventions and Protocols related to terrorism, and it generally works to promote legal cooperation in criminal matters related to terrorism.

In relation to travel document security, the ATU aims to enhance border management capacity in detecting fraudulent travel documents. The ATU supports states in the implementation of ICAO standards relating to travel documents and encourages members to fully participate in INTERPOL, by speedily reporting lost or stolen documents.[75]

In the **African Union (AU)**, the foundation upon which the counter-terrorism initiatives undertaken by the 53-member Union rest is the Organization of African Unity (OAU) Convention on the Prevention and Combating of Terrorism, which was adopted in 1999 and entered into force in 2002. The corresponding Plan of Action, adopted in Algiers in 2002, calls on Member States to enhance their border control capability, including the issuance of more secure travel documents; to update and harmonize their legal systems; and to suppress the financing of terrorism.

As terrorism is often recognized as an international problem affecting states across borders, most states realize that cooperating with others, and assisting those states which have more limited means and finances available for border security and counter-terrorism measures can be mutually beneficial. Programmes which have been identified, and for which some AU Member States are receiving limited assistance, include the development of machine-readable travel documents with enhanced levels of security, the development of a “Passport Stop-list” that lists individuals whose applications for identity documentation would trigger special attention and the computerization of points of entry and exit to better monitor people flows. In 2004, the African Centre for the Study and Research on Terrorism was established in Algiers. Its function is to provide support and training to Member States in their efforts to enhance their counter-terrorism capabilities.

In June 2006, the Intergovernmental Authority on Development (IGAD) in Eastern Africa Capacity Building Program against Terrorism **(ICPAT)** was launched to implement the decision of the heads of state of IGAD Member States meeting in Khartoum, Sudan in 2002. The Programme aims at building national capacity to resist terrorism and promoting regional security cooperation. The five main components of ICPAT are: enhancing judicial capacity; optimizing interdepartmental cooperation; enhancing border control; providing training, sharing information and best practices; and promoting strategic cooperation. ICPAT carries out studies and research with the objective of highlighting key steps required for safeguarding security; it convenes meetings within and between countries to promote information

[75] For more on the ATU, see OSCE’s website at http://www.osce.org/atu/.

sharing and cooperation; and it provides counter terrorism training for law enforcement officers.[76]

In 1998, the **Organization of American States (OAS)** established an **Inter-American Committee against Terrorism (CICTE)** to further hemispheric cooperation to combat terrorism. CICTE's objectives are to: enhance the exchange of information; formulate proposals to assist Member States drafting counter-terrorism legislation; promote universal adherence to international counter-terrorism conventions; enhance border cooperation and travel documentation security measures; and develop training and crisis management programmes.

On counter-terrorism issues, in recent years the CICTE has been guided by the principles set down in the Inter-American Convention against Terrorism adopted at a meeting of the OAS General Assembly in 2002. By 2008, the Convention had been signed by 33 OAS Member States and ratified by 24. In relation to protecting border control and migration regimes from the activities of terrorists, the key objectives of the CICTE include:

- enhancing information exchanges between the relevant authorities in CICTE member countries;
- establishing an Inter-American database on terrorism issues;
- developing capacity building programmes to help members draft relevant reforms for domestic legislation;
- facilitating a network of regional and subregional treaties based on international conventions which will harmonize counter-terrorism practices in key areas (including migration and border control);
- developing better capabilities to monitor irregular movements of people and the illegal use of fake identity and travel documentation.

In addition, CICTE has initiated a technical assistance programme involving specialized organizations such as INTERPOL, experts from government agencies outside the region, including Spain, for example, and international organizations such as the IOM. Within these programmes, emphasis has been placed on the management of lost or stolen travel documentation, particularly through a more comprehensive use of database technologies.

The **Security and Prosperity Partnership of North America (SPP)** is an initiative launched by the leaders of Canada, Mexico and the US in 2005. Although it does not deal exclusively with cross-border crime and terrorism, there is, nonetheless, a strong security focus within the SPP, with particular attention being paid to the need to work collectively to help secure the collective borders of the SPP members.

While review of the implementation of the programme is currently ongoing, key elements of the programme include:

- the establishment of standardized risk-based screening practices for goods and people through information sharing and a faster uptake of new technologies, especially in the area of biometrics;
- the development and implementation of interoperable electronic security processes across the supply chains so that the distribution of goods

[76] See ICPAT's website at http://icpat.org/index.php?option=com_content&task=view&id=163&Itemid=110.

throughout North America is not slowed or impeded by security screening;

- the implementation of common standards for identity documents to facilitate more efficient cross-border travel;
- a boost in the level of personnel exchanges between law enforcement agencies to foster capacity building in criminal and security investigations.

The **Asia-Pacific Economic Cooperation (APEC)** is a regional forum for economies on the Pacific Rim. Although its primary focus is on trade and investment issues, APEC has also developed security-related institutions, such as the Counter-Terrorism Task Force (CTTF), the Counter-Terrorism Action Plans (CTAP) and the Securing Trade in the APEC Region (STAR) initiative.

Since its creation in 1997, the **APEC Business Mobility Group (BMG)** has been leading regional developments in trade- and immigration-related security. Initiatives include standards on travel documents, arrangements relating to liaison officers, and advance passenger information. Another notable project has been the development of a regional watch list.

Watch lists are a commonly used instrument to control access to a country's territory by those who are wanted for, or suspected, of crimes. By law, consular officers must check the database prior to issuing a visa. The Australian Migration Alert List is an electronic lookout or early warning system that enables immigration authorities to check if there is any known problem that might affect the grant of a valid visa. Building on this, and in partnership with the US, Australia has played a leading role, through the BMG, in continuing development of a **Regional Movement Alert List** system **(RMAL)**. A fully functional RMAL system should strengthen the ability of participating countries to fight terrorism by monitoring the movement of people across borders. Following completion of a feasibility study undertaken by Australia and the US, APEC ministers agreed in November to pilot the RMAL in 2005. New Zealand joined in 2006.

RMAL allows APEC members with advanced passenger processing (APP) systems to access information made available by other participating members on a "real time" basis during the pre-boarding phase. In the case of Australia and New Zealand, RMAL works in parallel with the APP system, while in the case of the US, it works with the API system.

Under the pilot RMAL system, for example, if a passenger checks in for a New Zealand-bound flight with US travel documents, an automatic pre-arrival check is undertaken against current US records of lost, stolen or otherwise invalid travel documents. At the same time, the RMAL system also facilitates checks of the travel documents of New Zealanders travelling to the US via Washington's use of in-flight API checks.

Initial RMAL checks are limited to verifying the serial numbers and expiry dates of travel documents presented by incoming passengers against lists of stolen and otherwise invalid travel documents supplied by participating economies. This will be done without any exchange of biographical information, including names and dates of birth. Any detection through RMAL checks of an attempt to use a travel document previously reported as lost, stolen or otherwise invalid triggers collaborative investigation and remedial action by officials of the two countries concerned.

CHAPTER 5
DOMESTIC LAWS AND POLICIES

If there is an ever present tension between the human rights of the individual and the security of the state internationally, this conflict can also be thrown into sharp relief by domestic developments in security. With the recognition that keeping all potential threats out of the country is an impossible feat for any open state comes the need to enhance domestic security by ensuring that authorities have the resources and the capacity required to deal with threatening individuals. Sometimes, such measures will relate specifically to migrants (although that is not necessarily the case), and may involve legislation concerning the powers of authorities to detain and deport non-nationals who pose a threat to national security. They also involve measures to improve intelligence gathering, identification and tracking of non-nationals. Since many such measures providing national authorities with increased information and control also limit the right to privacy and freedom, it is crucial that they are justified by the current security climate. As with issues relating to border security, and perhaps more so, any security measures which may infringe on human rights and civil liberties must be proportionate to the security threat. In light of this, civil liberty groups who monitor new requirements brought in through anti-terrorism legislation have an important role to play. By issuing legal challenges on constitutional and proportionality grounds, they help to ensure that the proper balance is struck between national security and individual rights.

However, states are also engaging with migrants in more proactive and constructive ways, by developing programmes and policies aimed at integrating migrants in the host society. Integration policies help promote a cohesive, inclusive and tolerant society, where the immigrant population lives in harmony with the local population. Indeed, failure to promote tolerance in a society is often a precursor to discrimination, social exclusion and the rise of racism and xenophobia.[77] Socio-economic and political disaffection among immigrant communities can in turn breed social violence, even terrorism – or at least provide conditions conducive to recruitment to such destructive actions.

i) INTEGRATION POLICIES

An immigration integration policy is an umbrella concept for settlement policies targeting immigrants and their families. How, if at all, has terrorism affected the development of immigration integration policy?

National security is not the primary reason for integration, but there are aspects of it which can have an effect on security. There are two key security-related reasons why governments urgently need to ensure effective integration strategies:

- to ensure protection of migrants against a community backlash following terrorist attacks perpetrated by non-nationals, second-generation immigrants or others who may be seen as outsiders;
- to prevent migrants (and the general community) from being susceptible to recruitment to terrorism, e.g. through disaffection with or alienation from their host community.

[77] See IOM Policy Brief, "Integration in Today's Mobile World," July 2006, and European Commission, Communication to the Council and the European Parliament on *An Open Method of Co-ordination for the Community Immigration Policy*, COM (2001) 387 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0387:FIN:EN:PDF,11 July 2001, p.11.

Integration policies have existed in states with a long experience of immigration, and have primarily proven to be successful in ensuring improved social stability. Many immigrant-destination states have legislation on equal opportunities designed to promote cultural and racial harmony, and positive discrimination is used in some countries to secure equal representation in certain professions. A range of other measures are in place to improve access to social services and community activities. Key actors pushing such initiatives include community and ethnic support groups, as well as NGOs.

Integration policies in the traditional countries of immigration tend to focus on permanent migrants. Given, however, the long-term presence of temporary migrants in many parts of Europe, similar programmes could be explored for this sector in order to develop a more comprehensive approach to integration policy and involving more proactive integration strategies, beginning with wider consultation with social partners. A number of countries have various strategies in place to assist with the socio-economic integration of migrants, regardless of whether they are permanent. These include language training, translation services, information referral, migrant resource centres, improved access to health care, employment possibilities for spouses and the right of family members to accompany the migrant.

In **Canada**, new arrivals may benefit from various governmental settlement services abroad, upon arrival at ports of entry and at their final destination in Canada. These services include counselling and cultural orientation, loans to help with transportation to Canada, reception, information and orientation, referral to community resources, language training, translation and interpretation, and employment-related services. Under Canada’s Immigration Loans Program, loans are made to applicants for permanent residence – mostly refugees and members of humanitarian-designated classes – to cover the costs of medical examinations abroad, transportation to Canada and the Right of Permanent Residence Fee (RPRF). Assistance loans are also available to disadvantaged newcomers to cover expenses such as housing rental, telephone deposits or work tools.

Europe's economic prospects and demographic trends make immigration a necessity and a contributor to its development. Policy developments in recent years at the EU level reflect the need for clear and effective policies for the social integration of migrants. These may differ from one Member State to another due to prevailing cultural diversities. The principle of equality of rights and duties, however, should be a common denominator upon which integration practices, including the concept of citizenship, would be further built.

The **EU** is working towards a common European approach to social integration of third-country nationals, based on approximately equivalent rights to nationals,[78] their free movement within EU territory and some measures to enhance immigrants’ economic and socio-cultural position against xenophobia and racial discrimination. A number of EC initiatives and programmes are already in place to support actions in this field. For example, at the request of the EU’s Justice and Home Affairs Council, in 2003 the European Council moved to establish National Contact Points (NCPs) on integration and invited the Commission to present *Annual Reports on Migration and Integration* issues. The third *Annual Report on Migration and Integration* was

[78] The 1999 European Council in Tampere states the necessity to define a stronger involvement in designing a common integration policy in order to offer third-country nationals “rights and obligations *comparable to* all European Union citizens” [emphasis added].

presented by the Commission in September 2007.[79] Furthermore, 2004 saw the publication of the *Handbook on Integration for Policymakers and Practitioners,* a second edition of which was published in 2007. Also in 2004, the Hague Programme called on the EU to develop a long term strategy to resolve those deleterious social dynamics that are contributing to the radicalization of some individuals and their recruitment to terrorist networks.[80] The outcome of this call was released in 2005 in the form of the EU Common Agenda for Integration (CAI).

The strength of the CAI lies both in its acknowledgement of the importance of migration in ensuring Europe's continued economic and cultural growth and also its recognition that integration is "a dynamic, two-way process of mutual accommodation by all immigrants and residents of Member States."[81]To this end the CAI points out that the "practice of diverse cultures and religions is guaranteed under the EU Charter of Fundamental Rights and must be safeguarded, unless practices conflict with other inviolable European rights or with national law."[82]

In the **UK**, the Home Office is committed to integration as a vital part of the whole system process. It is considered necessary for all refugees who are invited to remain in the UK to be assisted to rebuild their lives, achieve their full potential and make a contribution to the social, cultural and economic life of the country. The successful settlement of refugees in the UK is considered a strategic factor in building stronger, more cohesive communities. A recent study noted the creation, in November 2007, of the Migration Directorate within the Department for Communities and Local Government, which is intended to coordinate work across the government relating to migration and the impact on local communities, thus providing for a more coherent overall policy on integration.[83]

Some initiatives have been underway for several years, while others are more recent and seek to respond to the concerns raised by the July 2005 London bombings. The **UK** has been revamping its nationality laws to require that immigrants seeking UK citizenship demonstrate sufficient knowledge of the English language and British history, culture, and customs, either by passing a short test or completing a government-approved citizenship and language class. The government has also introduced and made mandatory new citizenship ceremonies, during which those acquiring British nationality swear allegiance to the Queen and pledge respect for the UK's rights and freedoms. All of these measures took effect in 2004. Also, in the wake of the London attacks, the British government has sought to intensify contacts with the Muslim community. The Home Office established seven working groups of

[79] See European Commission, Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Third Annual Report on Migration and Integration*, COM (2007) 512 final, 11 September 2007, http://ec.europa.eu/justice_home/fsj/immigration/docs/com_2007_512_en.pdf.

[80] European Commission, Communication to the European Parliament and the Council, *Terrorist Recruitment: Addressing the Factors Contributing to Violent Radicalization*, COM (2005) 313 final, 31 September 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0313:FIN:EN:PDF, p. 3

[81] European Commission, Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *A Common Agenda for Integration: Framework for the Integration of Third-Country Nationals in the European Union*, COM (2005) 389 final, 1 September 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0389:FIN:EN:PDF, p. 5

[82] Ibid., p. 9

[83] UK Department for Communities and Local Government, *Review of Migrant Integration Policy in the UK*, 2008, p.8, available at: http://www.communities.gov.uk/documents/communities/pdf/838994.pdf

Muslim leaders and experts to provide advice on an informal basis to the government on ways to reduce disaffection and prevent radicalization of young Muslims.

In their efforts to ensure the creation of a cohesive society, some countries have made the continued resident status of migrants conditional on integration. For example, in **Germany**, the Residence Act 2004 introduced mandatory integration courses. Failure to follow these can result in reduced social benefits or refusal of continued residence. [84] In **France**, a law from 2003 stipulates that ten-year residence permits are only to be awarded if integration has occurred.[85] More recently, the 2007 "Contrat d'acceuil et d'integration", which imposes on aliens respect for the French Republic's values, stipulates that the stay permit will not be renewed in case of a violation of any the contract's clauses.

In **Finland**, a proactive approach by the government to the issue of cultural literacy includes an emphasis on the important contributions made to Finnish society by migrants, and appears to have resulted in a more positive embrace of Helsinki's immigration programme by ordinary citizens. A recent study, *The Attitudes of Finns towards Immigrants in 1987-2003*,[86] showed that the attitudes of Finns towards migrants and refugees have continued to improve in the post-9/11 period.

A recent undertaking relating to integration in the EU is the **Migrant Integration Policy Index (MIPEX),[87]** a collaborative initiative between universities, research institutes, think tanks, foundations and NGOs. Intended to spark debate and further discussions, the MIPEX measures policies to integrate migrants in 27 EU Member States and three non-EU countries, using over 140 indicators within six areas of policy:

- labour market access
- family reunion
- long-term residence
- political participation
- access to nationality
- anti-discrimination.

Standards for each area are set based on Council of Europe Conventions or European Community Directives, and countries are issued scores depending on how well they live up to these standards.

In late 2005, a pilot programme was introduced in two major **Australian** cities (Melbourne and Brisbane) whereby newly arrived clergy of all faiths were invited to a two-day seminar where they were provided with information on Australian politics, society and culture, and equipped with the information on how to utilize government services to address the economic, cultural and social concerns of their

[84] U. Davy (2006) "Immigration, Asylum and Terrorism: How do they Inter-Relate in Germany?" in A. Baldaccini and E. Guild (eds.), *Terrorism and the Foreigner: A Decade of Tension around the Rule of Law in Europe*, Brill, Leiden, p. 218

[85] C. Saas (2006) "The Changes in Laws on Asylum and Immigration in France in Response to Terrorist Fears" in A. Baldaccini and E. Guild (eds.), *Terrorism and the Foreigner: A Decade of Tension around the Rule of Law in Europe*, Brill, Leiden, p. 261

[86] M. Jaakkola (2005) "The Attitudes of Finns towards immigrants in 1987-2003", *Labour Policy Studies* 286, Helsinki

[87] MIPEX is available from http://www.integrationindex.eu/.

congregations.[88] The clergy were also encouraged to participate in existing interfaith initiatives in their communities and to create new multi-faith networks built upon the relationships established through the programme to counter ignorance, increase understanding, share problems and rely on each other in addressing the economic or social problems of their respective congregations.

Government action in the post-arrival integration of migrants has become critical in a post-9/11 world. Creating the right climate domestically, e.g. through policies promoting multiculturalism, can help achieve cohesion in societies that are increasingly diverse socially, ethnically, economically and religiously. Consequently, increased attention to the integration of new arrivals may be an important way of addressing international terrorism.

However, no amount of positive reinforcement by host governments implementing integration policies can entirely eliminate the possible development of terrorist, clandestine or subversive activity by extremists or disaffected individuals or groups within diasporas who may have succumbed to recruitment for terrorist activities. Therefore, integration policies are not a panacea for terrorism. Nonetheless, such policies can serve as an integral part of governments' overall efforts to build secure and cohesive societies.[89]

ii) DETENTION

In the wake of the 9/11 terrorist attacks in the US in 2001, many states pushed through with new anti-terrorism legislation, often expanding state powers of detention. Although not all states have actually increased their use of such powers, a number of states have done so, arguing that it is an essential instrument in the fight against terrorism.

The UK, which had adopted the Terrorism Act in 2000, responded to the events of 9/11 by passing the Anti-Terrorism, Crime and Security Act (ATCSA) in late 2001. Amongst other things, this legislation allowed for the detention for an indefinite period of non-citizens suspected of terrorism. Specifically, individuals who could be detained under this law were those designated as a (terrorist) threat to national security by the Home Secretary, but who could not be deported because they risked being killed or tortured in their home country. In order to detain such individuals, the UK had to derogate from obligations under the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights, by declaring "a public emergency threatening the life of the nation".[90] This derogation from the ECHR was heavily criticized by human rights organizations such as Amnesty International and the Islamic Human Rights Commission. In December 2004, the House of Lords ruled that Part 4 of the ATCSA (the part that deals with detention without trial) was incompatible with rights as set out in the ECHR, arguing that such detention powers were both disproportionate and discriminatory: disproportionate insofar as they

[88] School of Political and Social Inquiry, Monash University and The Australian Multicultural Foundation. *Introducing Australia: A Course for Clergy New to Australia*, Unpublished report for the Department of Immigration and Multicultural Affairs, 2006; see http://www.monash.edu.au/research/directory/?type=cref&query=2008002400.

[89] For a fuller discussion of integration, see "Integration in Today's Mobile World", IOM Policy Brief, July 2006 (http://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/policy_and_research/policy_documents/policy_brief_1.pdf).

[90] Schoenholtz, n. 2 above, p. 18

constituted a response beyond that justified by a public emergency; discriminatory insofar as they applied only to non-nationals.[91]

Detention without trial powers were repealed in April 2005. Instead, new regulations were implemented through the Prevention of Terrorism Act 2005, under which the Home Secretary can issue control orders restricting the movement and association of suspected terrorists. Notably, these control orders may be applied to British citizens as well as non-citizens.

The issue of detention has continued to be controversial in the UK, however. Under the Terrorism Act 2000, individuals suspected of terrorism could be detained for a maximum period of seven days before being charged with a crime. This period was subsequently extended to 14 days in 2003 and in the Terrorism Act 2006, introduced shortly after the July 2005 London bombings, it was extended further to 28 days. In an amendment to the bill, the government had proposed an extension to 90 days, but this was rejected by parliament.

France's special anti-terrorism unit can hold suspects for questioning for 96 consecutive hours, of which the first 24 hours may include not having any contact with a lawyer. In the UK, such incommunicado detention is limited to two days under the Terrorism Act 2000. In Australia, terrorism suspects can be held in incommunicado detention for seven days with extensions. Spanish authorities can detain suspects for up to 13 days incommunicado.[92] Critics have voiced concerns that such procedures are contrary to the human right of detainees to challenge the lawfulness of their detention.[93]

In the US, the USA Patriot Act introduced a number of changes, broadening the definition of what constitutes terrorism-related activity, and expanding the grounds for detention. In addition, a Justice Department rule, issued shortly after the 9/11 attacks, increased the permissible period of pre-charge detention for certain non-citizens from 24 to 48 hours, or for an undefined "reasonable period of time" in "an emergency or other extraordinary circumstances".[94]

In its report, *The September 11 Detainees*, the Inspector General of the US Department of Justice described the large number of arrests of immigrants as part of the investigations following the 9/11 attacks as "indiscriminate" and "haphazard". The long periods of detention were also pointed out as a problem.[95] In the US, some observers have also criticized abuse of the material witness law, claiming that authorities have used it to detain indefinitely those individuals they suspect of terrorism. [96]

[91] D. Bonner and R. Cholewinski (2006) "Immigration and Asylum Law: The Impact of Terrorism – The United Kingdom" in A. Baldaccini and E. Guild (eds.), *Terrorism and the Foreigner: A Decade of Tension around the Rule of Law in Europe*, Brill, Leiden, p. 150

[92] Schoenholtz, n. 2 above, p. 20

[93] Human Rights Watch, *Setting an Example? Counter-Terrorism Measures in Spain*, January 2005, http://www.hrw.org/reports/2005/spain0105/

[94] Schoenholtz, n. 2 above, p. 21

[95] US Department of Justice, Office of the Inspector General, *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks*, April 2003, http://www.usdoj.gov/oig/special/0306/full.pdf

[96] Human Rights Watch and the American Civil Liberties Union, *Human Rights Abuses under the Material Witness Law since September 11*, *17 Witness to Abuse*, June 2005, http://hrw.org/reports/2005/us0605/

iii) DEPORTATION

Much of the effort by governments in the last number of years has been devoted to preventing the entry of those who pose a threat to the country. However, since motives are difficult to predict and there are bound to be those who gain entry legally but subsequently abuse the conditions of stay, states have also put in place provisions for the deportation of non-citizens. Such legislation, concerning the exclusion[97] and deportation of non-citizens, has been expanded in a number of states since 9/11. A relatively recent development is the US Real ID Act of 2005, which defines support for terrorism in a broad manner, providing for the exclusion and deportation of those involved in, or supporting terrorism, in a variety of ways.[98]

Under international law, states are obliged to adhere to the principle of non-refoulement, which prohibits the exclusion or deportation of refugees. However, the Refugee Convention also contains parts which exclude from international protection individuals who have committed war crimes or crimes against humanity (Article 1F), or where there are "reasonable grounds" for regarding a refugee "as a danger to the security of the country in which (s)he is" (Article 33(2)). Some states have argued that these articles are applicable in the case of suspected terrorists, allowing for their deportation.

Those who argue that there is no exemption from the obligation of non-refoulement point to rulings by the European Court of Human Rights (ECtHR), which state that deporting non-citizens to a country where they might face a real risk of torture or degrading treatment contravenes the European Convention on Human Rights. In addition, the UN Convention against Torture and the International Covenant on Civil and Political Rights also lack any security exception to non-refoulement.[99] Indeed, it was in response to this that the UK, by attempting to derogate from the right to liberty in these two human rights instruments, devised its provision for indefinite detention, as discussed earlier. Since it could not deport certain non-nationals suspected of terrorism, it sought another way to ensure the safety of the state from the threat they were considered to pose. In Germany, proposals were put forward providing for indefinite detention for the same reason,[100] but these were not implemented, and the eventual result was similar to the UK control orders, in allowing for the restricted movement of suspects.

As indefinite detention was ruled contrary to human rights laws, but the threat posed by terrorists remains, states have made use of other instruments for the purposes of national security. Partly, this has involved increasing reliance on criminal prosecution and seeking diplomatic assurances from the receiving state that the deportee will not be tortured or otherwise subjected to degrading treatment.[101] However, as the UN Counter-Terrorism Committee stresses: "Whether or not States use diplomatic assurances, they must ensure that they comply with their obligations with regard to the principle of non-refoulement."[102]

[97] See the following section.
[98] Ibid.
[99] Schoenholtz, n. 2 above, p. 8
[100] Davy, n. 65 above, p. 227
[101] Schoenholtz, n. 2 above, p. 17
[102] The report of the Counter-Terrorism Committee on the implementation of Resolution 1373 (S/2008/379), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Terrorism%20S%20RES%20379.pdf

iv) EXCLUSION: TERRORIST-RELATED INADMISSIBILITY GROUNDS

The US Context

Among the general classes of aliens ineligible to receive visas or admission to the US, according to section 212 (a)(3)(B)(i) of the Immigration and Nationality Act, is an alien who:

(I) has engaged in a terrorist activity;

(II) a consular officer, the Attorney General, or the Secretary of Homeland Security knows, or has reasonable ground to believe, is engaged in or is likely to engage after entry in any terrorist activity (as defined in clause (iv));

(III) has, under circumstances indicating an intention to cause death or serious bodily harm, incited terrorist activity;

(IV) is a representative (as defined in clause (v)) of:

(aa) a terrorist organization (as defined in clause (vi)); or

(bb) a political, social, or other group that endorses or espouses terrorist activity;

(V) is a member of a terrorist organization described in sub-clause (I) or (II) of clause (vi);

(VI) is a member of a terrorist organization described in clause (vi)(III), unless the alien can demonstrate by clear and convincing evidence that the alien did not know, and should not reasonably have known, that the organization was a terrorist organization;

(VII) endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization;

(VIII) has received military-type training (as defined in section 2339D(c)(1) of title 18, United States Code) from or on behalf of any organization that, at the time the training was received, was a terrorist organization (as defined in clause (vi)); or

(IX) is the spouse or child of an alien who is inadmissible under this subparagraph, if the activity causing the alien to be found inadmissible occurred within the last 5 years, is inadmissible.

Since 2000, the US Congress has passed three major pieces of legislation concerning terrorist-related inadmissibility grounds that serve as bar (exclusion).The USA PATRIOT Act of 2001 expanded grounds of inadmissibility based on terrorism, broadened the definition of “terrorist activity”, added two definitions of “terrorist organization”, and added a separate ground of inadmissibility for those who have been associated with a terrorist organization. The Patriot Act also added a sub-section on membership in an undesignated terrorist organization to those grounds on which a person would not be eligible for asylum. The Immigration and Nationality Act (INA), as amended by the Patriot Act, allows those persons who fall under subsection (IV) of 212(a)(3)(B)(i) (representative of a terrorist organization) to be eligible for an exception to the bar, if it is determined that there are no reasonable grounds to believe that they are a danger to the security of the US.

The Real ID Act of 2005 introduces stricter laws governing applications of asylum and deportation of aliens for terrorist activity, purportedly to prevent terrorists from obtaining relief from removal. The legislation provides immigration judges with greater authority to make credibility determinations and to require corroboration of an asylum claim. More importantly, it further broadened the categories of persons who are inadmissible for terrorist activities by including those who have received military-type training from or on behalf of a terrorist organization. It also broadened the inadmissibility ground regarding espousing terrorist activity to no longer require that the individual hold a "position of prominence."

The 1951 Geneva Convention

The only significant international law regarding the exclusion of terrorists is found in the 1951 Refugee Convention. Terrorism is not explicitly mentioned, but Article 1F formally excludes from international protection any person "with respect to whom there are serious reasons for considering" that he has committed a crime against peace, a war crime, or a crime against humanity; acts contrary to the purposes and principles of the United Nations; or a serious non-political crime outside the country of refuge. The UNHCR Guidelines state that "acts commonly considered to be terrorist in nature are likely to fall within the exclusion clauses."[103] The other provision of this Convention, Article 33(2), provides for a security exception to the obligation of non-refoulement, where there are "reasonable grounds" for regarding a refugee as "a danger to the security of the country in which he is."

v) IN-COUNTRY IDENTIFICATION AND TRACKING

When they cross international borders, terrorists are subjected to an array of state controls and identification mechanisms. As states develop closer cooperation, secure travel documents and more advanced border control instruments, terrorists will find it increasingly difficult to avoid detection. However, a comprehensive strategy for preventing terrorism requires more than just border security. Therefore, states are also implementing measures for identifying and tracking suspected terrorists domestically. In light of the previous discussion concerning detention and deportation of terrorist suspects, it should be clear that access to accurate and timely information on suspected terrorists is crucial.

Many of the measures relating to in-country identification of non-citizens can be linked to the events of 9/11 and the way in which the terrorists entered the US on legitimately issued tourist and student visas.[104] While screening of visa applicants and the issuance of more secure travel documents can be important measures in the fight against terrorism, finding ways to track and identify dangerous individuals who have already entered the country is also a priority for states.

Many of the initiatives of recent years involve the use of biometrics to enhance identification systems. As previously noted, the insertion of biometric identifiers in passports is rapidly gaining ground in countries all over the world. A number of countries are also producing or considering the issuance of biometrically enhanced ID cards. This may mean that provisions have to be made for such measures in domestic law. For example, Germany's Anti-Terrorism Act 2002 allows for inclusion of biometric data in passports, ID cards, as well as residence permits for non-nationals.[105] The same legislation also allows the secret services to request

[103] 2003 UNHCR Guidelines on International Protection No. 5: Application of the Exclusion Clauses: Article 1F of the 1951 Convention Relating to the Status of Refugees

[104] Koslowski, n. 29 above, p. 3

[105] Davy, n. 65 above, p. 206

information from banks, airlines and telecom services, as part of the investigation of terrorist suspects. In Canada, non-citizen residents are issued with a Permanent Residence Card enhanced with biometric features, making it more fraud-resistant. The card is required for travel to and from the country.

The UK has started issuing ID cards for non-EEA foreign nationals. Issued at first only to certain categories of immigrants, the scheme is expected to cover 90 per cent of foreign nationals by 2014-15. It involves capturing fingerprints of card holders and will allow authorities to access information on the holder's immigration status, residence and work permits, and access to benefits.[106] From 2009, certain categories of UK citizens, working in sensitive areas, are also issued ID cards. However, the issue of identity cards, either for everyone or specific groups, will continue to be politically sensitive, particularly for countries which have no tradition of carrying identity cards such as Australia, Canada, the UK and the US. Concerns voiced in connection with such schemes involve privacy concerns and worries about stolen identities.

In addition to the use of biometrics in travel documents and ID cards, a number of systems also store such information for specific purposes. Among the measures already mentioned in this report is the **Visa Information System** (**VIS**), which will store fingerprint data on visa applicants wishing to travel to the EU for visits of up to three months. Although its primary function is to facilitate the development of a common visa policy, law enforcement access to the database is envisaged under certain conditions that ensure a high level of data protection and with the aim to prevent, fight and investigate terrorist offences as well as other serious crimes.[107] Thus, VIS can also be seen as providing an additional layer to the internal security of participating EU Member States. For the purposes of identification and tracking of criminals and terrorists, Member States, as noted earlier, also have access to the **Schengen Information System (SIS)**, currently being developed into the expanded **SIS II**, including biometric data on persons of interest to law enforcement authorities.

Another type of comprehensive measure facilitating the identification and tracking of foreign nationals is the entry-exit scheme pioneered by the US, through its **US-VISIT** scheme. By collecting biometric data and registering passengers upon entry and again upon departure (anticipated), authorities should better be able to detect those who overstay their visas, an issue which was of concern in relation to the perpetrators of the 9/11 attacks.

Although proposals have been put forward for a similar scheme in the EU, there are currently no plans to implement one.[108] Any EU-wide electronic entry-exit scheme would have to include a very large number of border controls and since the EU has more border crossing points than the US, this would prove practically difficult and costly. In addition, there would seem to be some overlap with other EU schemes, such as VIS.

[106] See "National identity scheme delivery plan published", UK Border Agency, Latest news, 6 March 2008, http://www.bia.homeoffice.gov.uk/sitecontent/newsarticles/2008/identityschemeplan).

[107] See "Visa Information System (VIS): The JHA-Council reaches a political agreement on the VIS Regulation and VIS", n. 44 above.

[108] See European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs, *Proposed New EU Border Control Systems*, Briefing Paper, June 2008, Doc. PE 408.296, http://www.europarl.europa.eu/document/activities/cont/200806/20080626ATT32854/20080626ATT32854EN.pdf.

Registration of certain categories of foreigners present in the country is required by a number of states around the world. In the UK, for example, foreign nationals from certain countries staying longer than six months are required to register with police authorities. Similarly, foreigners staying longer than six months in India must also register. In Japan, the corresponding time period is 90 days. Finally, the US runs the **Student and Exchange Visitor Information System (SEVIS)** which tracks and monitors more than one million students and scholars in the country. It requires universities and colleges to keep records on international students, informing authorities of any significant changes.

CHAPTER 6

CONCLUSION

While each theme addressed in this paper may have some application on an individual basis, a holistic approach to addressing the migration-related aspects of international terrorism seems to offer solutions that might better address the problem. It is one thing to have good border control, but the overall value of the process is lessened without appropriate entry and exit systems, improved data collection and sharing, secure travel documents and their issuance.

Furthermore, while a country can have implemented sophisticated measures to counter global terrorism it also needs to develop mechanisms for addressing the concerns of immigrant communities to comprehensively address this security issue. While it may not be possible to eliminate extremism, better understanding and accommodation of the specific needs of migrants is likely to lead to greater reciprocal cooperation. Dialogue is an essential part of this process.

In the exercise of its sovereignty, each state will necessarily consider its own circumstances and adopt policies, administrative structures and legislative measures considered best to protect its national interests and guarantee security from global terrorism. Countries that have lengthy land borders may well approach their immigration controls differently from those that do not. However, there are some concerns that all states grappling with international terrorism will face, including privacy and human rights issues. Privacy issues are particularly significant in the context of increased data gathering and information exchange. While the collection of pre-departure information and sharing of watch lists between agencies and countries can make a significant contribution to border management, both in terms of security and facilitation, it is crucial that any steps in this direction are carefully considered and proportionate to the security threat. In relation to internal security measures, similar proportionality requirements must be considered in accordance with the international law obligations of states. If present threat levels are considered high enough to motivate derogating from such obligations, it is vital that any arrangements made be subject to regular review and oversight.

At the same time, states and international organizations involved in areas of migration management must be aware of the limitations of migration policies in combating terrorism. Furthermore, migration is not limited to questions of security. Under the banner of migration management, countries have had to define and address human rights, economic growth and development, privacy and an overall balanced approach to border management. Most states and groups of states seek governance based on freedom, justice and security – as does the EU explicitly. Similar visions or goals are expressed, in different words, throughout the world. It would be counterproductive to achieve any one of those worthy goals at the expense of the others. As noted at the beginning of this paper, IOM considers migration not to be directly linked to terrorism. While these two fields intersect in a number of respects, and measures relating to migration can bring security benefits, there are numerous other areas of importance in the fight against terrorism.

In fact, there is even a risk that poorly calibrated immigration reforms might impose social and economic costs that far outweigh any corresponding benefits in terms of enhanced national security.

In terms of social costs, migration policies that are poorly implemented and/or have an excessive focus on security issues risk alienating the domestic immigrant community, which may consequently become isolated and susceptible to extremist influences. In the interest of national security, it is important that immigrant communities trust authorities and are willing to cooperate in preventing violence and terrorism. In this context, integration policies have an important role to play. In terms of economic costs, overly restrictive immigration policies run counter to global initiatives in the area of market liberalization. Obstacles to the migration of workers are not only a major impediment to the realization of higher levels of global growth, but also impede the capacity of labour-abundant countries in the developing world to offset the costs imposed by other areas of market reform.

These market distortions also carry ominous risks in terms of social costs. While labour mobility is important for maximizing the economic benefits generated by reforms to the international economy, structural obstacles to mobility are often a source of frustration and resentment. Faced with the passing of old economic practices and blocked from being able to benefit from the creation of new areas of economic activity, individuals risk developing hostile attitudes towards a “system” which they perceive to have disempowered and impoverished them. Evidence of the willingness of terrorist figureheads to fan this perception is clear in their rhetoric and in the targets of much of their violence. Therefore, there is an argument to be made for greater resort to organized labour migration as an active tool to improve security, which is imperative particularly in times of economic crisis that impacts severely on migrant workers.

Future developments in the field of migration management are likely to bring forth new challenges and opportunities for states and international stakeholders. In particular, developments in biometric technologies and identification systems are likely to continue at a rapid pace, calling for sustained international coordination in ensuring interoperability as well as the secure handling of data collected. These developments come along with the need to assist countries with limited resources in their equipment with these new tools. In addition, international cooperation and coordination relating to information exchange, capacity building and overall migration policy is set to continue growing. IOM strongly supports these developments by working closely with governments, international and civil society organizations with a view to promoting migration management approaches that attain an adequate balance between security concerns and increased facilitation of authorized and needed human mobility.

Last but not least, the inter-linkage is often portrayed as a conflict between state interests and human rights. Actions in the context of the fight against terrorism have sometimes challenged the integrity of the individual with regard to fundamental issues such as the right to seek asylum, the prohibition against torture and arbitrary detention and the right to a fair trial. A delicate balance must be struck between the interest of the state, the collective, and the human rights of the individual.

17 route des Morillons
1211 Geneva 19
Switzerland
Tel: +41.22.717 91 11 | Fax: +41.22.798 61 50
E-mail: hq@iom.int | Internet: http://www.iom.int