Securing Borders Collaboratively to Prevent the Movement of Foreign Terrorist Fighters

Simon Deignan and Thomas Wuchte

The Collaborative Challenge

The phenomenon of terrorism is not new, although it has taken a new significance and magnitude over the past several years. Paris, Brussels, Berlin, Nice…the list can go on. Terrorists continue to avoid detection while crossing our borders. Since 2014, one of the major issues for international and national security has been the threat posed by Foreign Terrorist Fighters (FTFs). FTFs are defined as individuals who travel abroad to a State other than their State of residence or nationality to engage in, undertake, plan, prepare, carry out or otherwise support terrorist activity or to provide or receive training to do so. As Daesh lost territory, manpower, and finances, the flow of FTFs to conflict zones reversed. It is estimated that approximately 40,000 FTFs left their homes to fight for Daesh – although many have been killed or already returned home, over half of these are still unaccounted for today. Returning FTFs can pose a new terrorist threat to their home or third countries, including transit countries. The challenge for United Nations (UN) Member States is to ensure that these returnees are identified and detected. The international community continues to grapple with addressing the complex set of challenges posed by this threat and unanimously adopted UN Security Council Resolution (UNSCR) 2396 in December 2017. With the adoption of this Resolution, the UN Security Council identified a series of measures that will help States deal with the challenge of returning and relocating FTFs. UNSCR 2396 has three

* This paper was submitted on 10 June 2018.

key border security elements: (a) appropriate screening measures at the borders and enhancing identity management; (b) increasing the collection and use of passenger data and biometrics; and (c) improving our sharing of information, both among States and within States. This chapter will look at these three areas, where more efforts are required. It explains several issues counter-terrorism experts must address through promoting policy dialogue, exchange of experiences and capacity-building, all while upholding human rights and the rule of law to ensure measures are proportional to the threat.

Improving Risk-Based Border Screening and Identity Management

UNSCR 2396 obliges States to strengthen border security through more thorough checks on forged documents and enhanced identification management.

In January 2017, 14 people were convicted by a Belgian court of producing fake identity documents (IDs). Some of these documents had been sold to individuals who were involved in the November 2015 Paris attacks and in the 2016 Brussels bombings. This small group managed to forge more than 2,000 passports and IDs. Organised crime is actively involved in the production and distribution of fraudulent or stolen documents, some of which are at such a high level that they can only be detected using forensic equipment. Coupled with the 11,000 blank Syrian passports that were stolen by Daesh, there is an ever-present threat of such documents being used to carry out terrorist attacks.[1]

It is therefore of the utmost importance that States set up effective measures at the border to assess whether a traveller is using a fake identity or not, and whether a travel document is fraudulent or not. This is particularly relevant since at some border crossing points of certain States there are no passport readers or even electricity. In these areas, border security is totally reliant on the border guard's ability to assess the traveller and the travel document to recognise a fake.

---

[1] https://www.aljazeera.com/news/2017/09/isil-holds-11100-blank-syrian-passports-report-170910090921948.html.

Risk Assessments

A traveller's identity goes beyond the document they are carrying. The European Border and Coast Guard Agency has seen a marked rise in look-alike or impostor fraud – this increase is not just a European phenomenon but can be found globally.[2] The border official's role is not simply procedural and document-based, it requires investigation skills. The primary objectives of border officials are to ascertain whether the person presenting themselves at the border is who they claim to be, has authority to enter the territory by visa or otherwise, and does not represent a threat to the territory or anybody within it. Therefore risk-based assessments are required. In the context of borders this may include understanding the likely travel patterns of terrorists (the outbound route may differ from the inbound route), identifying suspicious travel activities, e.g., unnecessarily protracted routes and/or use of legitimately held or illegitimate multi-national passports, knowing the "hot-spots" for false and stolen travel documents and being able to recognise the signs. Where this information is not known, clearly defined "Intelligence Requirements" should be issued and disseminated to those who may be able to fill in the knowledge gaps.

UNSCR 2396 is clear in emphasising that risk assessments and screening procedures must be done without resorting to profiling based on any discriminatory ground prohibited by international law, and States have consistently reaffirmed that terrorism should not be associated with any nationality, religion or ethnicity. This is important because there is no single profile of a terrorist. Counter-terrorism measures that rely on broad profiles – which are based on stereotypical assumptions that a person from a certain national, ethnic or religious background is more likely to be involved in terrorism – are problematic for many reasons. They are contrary to equality and non-discrimination principles, which are cornerstones of the international human rights framework. They are counter-productive because they reinforce stereotypes, foster marginalisation and stigmatisation, create "suspect communities" and thereby undermine trust between those communities and the authorities; and they may even contribute to the terrorist radicalisation of individuals who perceive themselves to be unfairly targeted. But practice has also shown that discriminatory profiling

[2] https://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2017.pdf.

is ineffective in the short term because it can be easily circumvented. Indeed, terrorist groups have proven their ability to reduce the likelihood of detection, for example, by recruiting people who do not conform to the pre-determined profiles or by adapting appearance and behaviour accordingly.

The use of technology can support border guards to move from their own subjective opinions, which may be subject to bias, to a more rules-based objective analysis of a traveller, based on their route, travel history, and contact information. The subsequent section on Passenger Data will go into more detail on the use of such information.

Improving Identification Management

A couple of years ago, a United States (US) investigator managed to obtain four genuine US passports using fake names and fraudulent documents. In one case, he used the Social Security number of a man who had died in 1965. In another, he used the Social Security number of a fictitious five-year-old child created for a previous investigation, along with an ID showing that he was 53 years old.[3] The investigator then used one of the fake passports to buy a plane ticket, obtain a boarding pass, and make it through a security checkpoint at a major US airport.

In 2016, it was discovered that thousands of Indian citizens had paid a criminal gang for false birth and marriage certificates from the former Portuguese colonies of Goa, Diu and Daman. In Portuguese law, Indians born in these areas before 1961, or their children and grandchildren, can apply for Portuguese passports because these were colonies of Portugal until that year.[4] However, British and Portuguese police learned that this loophole was being systematically abused to obtain a genuine EU passport using false breeder documents.

Border controls are tightening, and we have highly secure passports with biometric chips, but the processes to acquire a genuine passport remain open to abuse by criminal and terrorist groups. Identity deceptions are particularly prevalent when there are disconnects between passport and civil registry identity management systems – with civil registry systems often being the weaker link. So-called breeder documents, such as

---

[3] http://edition.cnn.com/2009/US/03/14/passport.security/index.html.

[4] http://www.ipsnews.net/2004/02/portugal-india-crime-rings-sell-fake-portuguese-passports/.

birth/marriage/school certificates, are far easier to falsify than a travel document. However, building a false identity using such fraudulent breeder documents can allow for the fraudster to acquire a real passport under a false identity – making the falsification almost impossible to detect.

States have woken up to this reality and are now looking at ways to standardise security features in breeder documents. However, the gaps remain and will for some time to come.

Increasing the Collection and Use of Passenger Data and Biometrics

Both commercial and security priorities have led to great technological advances being made at formal points of entry to facilitate bulk movement of travellers and to detect potential threats. Although the technologies exist, they were often viewed as nice to have rather than necessities. UNSCR 2396 has changed that by mandating that all States collect Advance Passenger Information, Passenger Name Record, and biometric data.

Advance Passenger Information (API)

On 24 May 2014, four people were killed at the Jewish Museum in Brussels by a man armed with a Kalashnikov rifle. This man was Mehdi Nemmouche, the first Daesh returnee to carry out an attack in Europe. He managed to do so despite being on several terrorist watch-lists. Because his data was not checked against these watch-lists before he travelled, he managed to fly back to Europe undetected.[5] If his API data had been checked in advance against these watch-lists, he would likely not have been allowed entry.

But what is API? It is the biographic data contained in a passenger's travel document that is submitted to the airlines during check-in, as well as the flight information of that airline. When it is received in advance of a passenger's arrival it allows law enforcement authorities the time to do two things. Firstly, to check the name, date of birth, nationality and other travel document information in the MRZ (Machine Readable Zone) against watch-lists and databases. If the traveller appeared on one, like Mehdi Nemmouche, they would be stopped at the border for further questioning. Secondly, it allows law enforcement authorities to compare the traveller's

[5] https://www.counterextremism.com/extremists/mehdi-nemmouche.

details against risk profiles. For example, a young male, travelling alone, with no luggage, from Algeria to Madrid via Kiev, would be more suspicious than an old French couple travelling to Spain for the weekend.

Put simply, API allows States to check travellers against known suspects and known risks, as well as unknown suspects and known risks. API has been a global requirement since September 2014 when the UN adopted Resolution 2178 to prevent the movement of FTFs. Since then, ICAO, the International Civil Aviation Organisation, has established API as a binding standard, and many international and regional organisations are supporting States to overcome the technical, financial and legal issues to establish national API systems.

Passenger Name Record (PNR)

A second, more detailed type of border screening involves PNR, passenger name record data. This is the information a traveller gives to an airline when booking a flight – phone number, email address, home address, credit card details and so on. It is much more detailed information; hence there are more concerns regarding data privacy, particularly in Europe. Although the information is not backed by a government-issued travel document, like API, PNR data can be very useful for intelligence, analysis and border security because it can identify suspicious travel patterns by examining what other flights that person has booked using that credit card. This can flag threats that otherwise might have escaped attention. With the adoption of UNSCR 2396, all States are required to collect passenger data in advance and cross-check this information against watch-lists and databases.

Probably the most valuable use of PNR is to illuminate hidden connections between known threats and their unknown associates – the unknown unknowns. For example, if a flight for an unknown person is booked using a credit card that was previously associated with a known suspect – the person travelling immediately becomes a person of interest. Taking the example one step further, if that person uses a home address previously unknown to law enforcement officials, the other people living in that house may also be associated with a crime.

The United States Counter Terrorism Coordinator gives the real-life example of Faisal Shahzad. Faisal was a US citizen who had received explosives training in Pakistan. In 2010, he arrived at the US on a one-way ticket

from Islamabad. He matched a PNR targeting rule based on his travel pattern, and so was stopped but subsequently released. Three months later, a car bomb failed to detonate in Times Square. Investigators linked Faisal to the car, through his credit card. An alert for him was placed in its system. When he booked a flight to flee the country, the system flagged it.[6] He was arrested and is now serving a life sentence.

Biometrics

In November 2017, US authorities arrested Naif Abdulaziz M. Alfallaj, a Saudi citizen residing in Oklahoma who trained with Al Qaeda in late 2000. The FBI was able to identify the man when they matched his fingerprints against those taken from an application form for the terrorist group's Al Farouq training camp that was seized in Afghanistan.[7]

Biometrics can be a valuable tool for verifying that individuals are who they say they are. Terrorists and organised criminals will try to mask their identities in several ways: whether by using a fake passport or taking on another identity. However, it is a lot harder to fake, for example, fingerprints. Face recognition, eye recognition, fingerprints, all the way up to DNA – these are ways to identify someone using human characteristics.

The technology for biometrics already exists and is moving fast. The majority of countries in the world are now issuing biometric passports, which contain a photo and a fingerprint – when a traveller uses an e-gate, a live image of the traveller's face is compared with the photo in their passport. Apple uses fingerprint recognition technology in its iPhones, the United Kingdom uses fingerprints instead of library cards and even Disney World uses face recognition to ensure a three-day pass is not transferred to someone else. Some States have begun to collect fingerprints and facial scans of travellers to their country. This data can be used to validate the traveller's identity and their travel documents. Some States also have watch-lists with biometric data of known and suspected terrorists.

UNSCR 2396 mandates that all States "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist

---

[6] https://www.theguardian.com/world/2010/sep/19/times-square-bomber.

[7] https://www.nytimes.com/2018/02/06/us/naif-alfallaj-qaeda-camp-oklahoma.html.

fighters". Most States do not yet have the capacity or the means to do this; therefore, assistance from both international organisations and other States will be necessary.

Data protection considerations

The routine gathering, storing and sharing of large amounts of the personal data of potentially everyone who travels across borders may have a substantial impact on the enjoyment of individual human rights of ordinary people too – their right to privacy and freedom of movement or even their right to liberty and security.

In accordance with international privacy and data protection standards, the collection, storing and processing of personal information must be prescribed by law, strictly necessary for a legitimate purpose and proportionate towards that purpose. The information gathered must not be used for other purposes than those for which it was collected; and the law must also provide for appropriate procedural safeguards against abuse.

For API and PNR, there is a human rights backstop in place, as airlines, European ones, will not send the data to a country that does not first have the correct legal provisions in place to safeguard data privacy. However, more work will be needed to ensure that biometric information is collected responsibly for counter-terrorism purposes as this effort expands.

Improving Our Sharing of Information, Both among States and within States

In the aftermath of the November 2015 Paris attacks, we learned that Belgian intelligence services had known about the jihadi backgrounds of Salah Abdeslam and some of his associates for some months before the attacks. Unfortunately, this information was not shared among other European intelligence services.[8] Dealing effectively with transnational threats like terrorism requires constant cooperation and intelligence sharing between law enforcement authorities. This is the reason why UNSCR 2396 stresses the need to increase information exchange both within States and among States.

---

[8] http://www.newsweek.com/belgium-shelved-investigation-abdeslam-brothers-paris-attacks-460687.

Inter-State information sharing

INTERPOL, Europol and many national and international law enforcement and border agencies gather, collate and disseminate a broad range of data relating to stolen and fraudulent travel documents, watch-lists of suspects, and notices requiring actions, ranging from reporting sightings to immediate detention of individuals. As with all forms of information, the data coming out of the system is only as good as that going in. If States are not populating these databases with relevant and up-to-date data, their usefulness is severely diminished. A second problem is that not all border control points have access to these databases – some INTERPOL members have previously had no connection at their air, land, and sea ports of entry to the Stolen and Lost Travel Document (SLTD) and other databases, potentially allowing known terrorists and criminals to travel more freely.[9]

UNSCR 2396 also encourages States to share information through bilateral and multilateral mechanisms. The level of information sharing before and after the Paris attacks demonstrates the contrast in how effective the response can be. As pointed out above, the main protagonists were known to intelligence services beforehand, but this information was not shared outside of national borders. In contrast, after the Paris attacks, States actively cooperated and shared operational intelligence with one another much greater, leading to the arrest of many associates of the attackers across Europe.

Of course, this principle of sharing assumes that all States value privacy equally and do not misuse information to target individuals outside of the rule of law; and that information practices, including integrity, anonymity, and destruction as appropriate, are rule-of-law-based. In addition to sharing this information with one another, States need to ensure that appropriate safeguards against abuses in bilateral and multilateral information exchange and law enforcement cooperation are strengthened. States should also put in place appropriate safeguards to ensure that information received from other countries has not been obtained in contravention of international human rights standards, and that information shared with other countries is not used for purposes that do so. Those who are arbitrarily included in terrorism watch-lists or databases will face

[9] https://www.un.org/sc/ctc/wp-content/uploads/2017/04/20170405_INTERPOL-Statement-Panel-1-Mr.-Gottlieb.pdf.

serious consequences, including arrest and detention, when travelling across borders. Practice has shown that this is not a theoretical question; but remains a problem for too many human rights defenders, journalists, political activities and others who have been unfairly labelled "terrorists" by their governments.

Intra-State information sharing

Many State agencies still treat information as need to know rather than need to share. This results in multiple information silos where nothing comes in or out, leading to resource duplication and missed opportunities to identify potential terrorists. The US learned this after September 11 and progressed to a model where information is shared among a host of security agencies. Many European agencies are now following suit, although in most countries there remains more work needed to form interagency information sharing. Inadequate interagency processes severely impede a country's ability to provide frontline screeners and law enforcement agencies access to terrorism information, and to screen against this information and other key data at borders and ports of entry. Without such up-to-date operational information, a frontline border officer may allow the entry or exit of a terrorist being sought by another security agency.

In addition to information sharing between state agencies, we should look to increase information sharing with the private sector. In many countries the private sector owns and operates a vast majority of the nation's critical border infrastructure, such as information and communication technology (ICT), energy and traffic and transportation. There is then a further need to strengthen the sharing of best practices with the private sector on countering terrorism. Partnerships between the public and private sectors are essential to maintaining security and resilience. These partnerships create an environment to share critical threat information, risk mitigation, and other vital information and resources. In many countries, businesses have understood and taken responsibility for cooperating and collaborating with state security agencies.

"Intelligence-derived knowledge shared more widely beyond intelligence circles" is one of the Step Changes highlighted in the UK Anderson

Report.[10] Support and interaction among States, the public and private sectors, as well as international and regional organisations is paramount in tackling threats posed by terrorism. Recognising each other's roles and responsibilities and stronger collaboration will benefit all stakeholders in countering terrorism in all its forms.

Conclusion

Land, sea, air borders offer great opportunities to deter, detect and disrupt criminal and terrorist threats. This is particularly relevant in the current era of heightened international crime and terrorism threats and the transiting of borders by terrorists and returning fighters seeking safe havens or fresh terroristic opportunities. Firstly, the mindset of those personnel engaged in border and immigration roles should be investigative, i.e., to make no assumptions, accept nothing at face value but challenge and check everything. Secondly, they should be guided by being "intelligence-led", thus ensuring that resources are focused and utilised against prioritised threats. The sharing of intelligence-derived knowledge not only benefits first responders directly, but also can be used to raise awareness at borders where specialised personnel are not always present. Finally, border officials should be assisted in this task through awareness of, and access to, updated and enhanced technological tools and to specialist national and international support.

Terrorism remains a largely transnational phenomenon. Terrorists can move funds, fighters, and weapons across international borders, and can now enable, direct and support terrorists located in another country – the so-called homegrown terrorist. This means that countries must work together to prevent and defeat terrorism. Daesh's military defeats in Syria and Iraq means there will be an increase in the number of FTFs returning to their countries of origin or travelling to other regions. Fortunately, we see now with UNSCR 2396 that there is a corresponding reaction to: (a) improve appropriate screening measures at the borders and enhance identity management; (b) increase the collection and use of passenger data and biometrics; and (c) improve our sharing of information, both among States and within States.

---

[10] Published in December 2017 – focused on attacks in London and Manchester, March-June 2017 respectively.

Countering terrorism requires strengthening the security of not only travel documents, but also related issuance processes, their inter-linkages to modernised civil registries, and the use of travel documents as part of comprehensive and integrated border solutions. This is the ethos of UNSCR 2396. Terrorism is also about risk management. Managing a risk to which our societies are particularly averse. This is, after all, the aim of terrorists – manipulating public opinion and influencing policy by instilling fear. The temptation may therefore be very high to take drastic measures and impose blanket restrictions. Governments should take the time to weigh options and consider the long-term impact, not only the immediate security benefits but broader implications on society, human rights and cohesion. There is no doubt that data and intelligence gathering and surveillance are necessary to fight terrorism at our borders and to protect the right to life. The challenge is to ensure these operations are targeted, proportionate, and non-discriminatory. In the end, only through outstanding collaboration will we be able to find the right balance between security and the right to live with open borders.

Mr. Simon Deignan manages the Organization for Security and Co-operation in Europe's (OSCE's) Travel Document Security Programme within the Transnational Threats Department, work that includes document security, identity security, access to databases, training in the physical inspection of travel documents, and expanding the use of Advance Passenger Information. He has been working on OSCE issues since 2010 including as a Political Advisor for both the Irish and Swiss Chairmanships. Prior to the OSCE, Simon worked in the private sector for an international management consultancy.

Mr. Thomas Wuchte has been the Executive Director at the International Institute for Justice and the Rule of Law (IIJ) since 2017. Previously, he was the Head on Anti-Terrorism Issues in the Organization for Security and Co-operation in Europe (OSCE). Before the IIJ and OSCE, Mr. Wuchte received the United States Department of State's highest award for Excellence in International Security Affairs for his efforts to work collaboratively with international partners on UNSCR 1540. He is a graduate of West Point and received a post-graduate degree in International Relations from the University of Illinois.