BORDER MANAGEMENT

In an increasingly interconnected world, it has become simple for people and goods to cross borders. This is also the case for terrorists. Effective border security is the first line of defence against the movement of terrorists across borders and the illegal cross-border movement of goods and cargo.

Maintaining secure maritime, land, and air borders is challenging for many Member States. Land borders, for example, can be tremendously lengthy and porous, and difficult to monitor. Other challenges derive from the lack of financial and human resources, equipment and specialist skills, or the lack of intra-State and inter-State cooperation.

The threat stemming from foreign terrorist fighters (FTFs) has increased the pressure on Member States and the international community to strengthen border security and prevent FTF travel. Following the Security Council’s adoption of resolution 2178 (2014), aimed at stemming the flow of FTFs, the Council’s Counter-Terrorism Committee and its Executive Directorate (CTED) have been engaged in analysing States’ counter-terrorism capacities, including in relation to border security. A preliminary analysis conducted by CTED at the end of 2014 (S/2014/807) revealed major gaps in many States’ implementation of the border-security requirements of resolutions 1373 (2001) and 1624 (2005). This in turn presents additional obstacles to the effective implementation of resolution 2178 (2014).

A more recent analysis (S/2015/683) established that many States had taken steps to strengthen border security and prevent FTF travel. Those steps include passport confiscation, the introduction of a requirement for transit visas, and more effective use of the databases of the International Criminal Police Organization (INTERPOL) to screen for potential FTFs. Some States have extended access to the INTERPOL I-24/7 secure communications network beyond their national central bureaus (NCBs) to other relevant border authorities, such as immigration at the frontline, and increased the use of the INTERPOL database on stolen and lost travel documents; more States are also populating the INTERPOL database of suspected FTFs.

Important tools in enhancing border security are Advance Passenger Information (API) and Passenger Name Records (PNR). In its simplest form, API is an electronic communications system that collects biographical passenger data and basic flight details from airline carriers and transmits the data to border-security authorities in the destination country prior to the flight’s arrival. This gives border-security authorities additional time to perform enough checks of all in-bound passengers against relevant sanctions and watch lists while minimizing delays in the processing of inbound passengers. PNR are generated through the information provided by passengers as they book their airline tickets and check into their flights. This
information is held in the carrier’s reservation and departure control systems, and may include a broad range of information, including the passenger’s name, his/her travel dates, ticket information, contact details, name of travel agent, means of payment, seat number, and baggage information. Many States already use PNR for law enforcement and border control purposes, whether on the basis of specific legislation or general legal and administrative powers, including to combat cross-border crime.

In its resolution 2396 (2017), the Security Council decided that Member States shall: (i) establish API; (ii) require airlines operating in their territories to provide API to the appropriate national authorities; (iii) share this information with the State of residence or nationality or with the countries of return, transit, or relocation, and relevant international organizations; and (iv) ensure that API is analysed by all relevant authorities. States shall also develop the capability to collect and process PNR data and ensure that such data is used by, and shared with, all their respective competent national authorities. The Council further encourages airlines to share PNR with relevant or concerned States to detect FTFs returning to their countries of origin or nationality or travelling or relocating to a third country.

So far, only one-third of Member States have implemented API systems. Even fewer have put in place PNR. There is therefore an urgent need to strengthen the sharing of information by airlines and Governments through the use of API systems that enable States to detect the arrival or departure of FTFs. Compliance with existing international standards, supplemented by passenger name records (PNR), would greatly assist States in the detection of FTFs attempting to cross their borders. Further ways to prevent the movement of terrorists or terrorist groups include strengthening the control of issuing identity papers and travel documents, and the introduction of measures to prevent counterfeiting, forgery, or the fraudulent use of identity papers and travel documents. However, many States lack clear policies and measures to ensure the security and integrity of the identity and travel-document issuance process.

Biometric identification is an effective tool for countering the threat posed by suspected terrorists including FTFs who attempt to travel internationally and use falsified travel documents. In resolution 2396 (2017), the Council decided that States shall 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, in compliance with domestic law and international human rights law. The Council encourages States to share this data responsibly among relevant Member States, as well as with INTERPOL and other relevant international bodies. In the context of a terrorism-related investigation, forensic science can assist investigators and prosecutors by linking an individual to a specific activity, event, place, or material, or to another individual. Member States’ use of biometric systems continues to expand, and the technological advancements in this field are fast. Many Member States struggle to implement these capabilities and to keep pace with these developments. It is therefore essential to strengthen Member States’ capacities in this area.

Spaces between official border crossings are difficult to control, because they are often lengthy and consist of open spaces or difficult terrain. They therefore present risks and vulnerabilities for potential crossing by terrorists. The lack of equipment and professionally trained border-security personnel also continues to increase States’ vulnerabilities.

Coordinated Border Management (CBM) strategies, which require close coordination among the competent authorities at border locations, have proven to be a highly effective tool for efficiently and effectively managing national borders. CBM strategies provide for the coordination of policies, programmes, and delivery among cross-border regulatory agencies with the aim of strengthening the management of trade and travel flows, while also addressing security concerns.

Ensuring effective border security is an integral part of any comprehensive and integrated national counter-terrorism strategy, and it requires collective action by States and relevant international and regional organizations. The CTC and its Executive Directorate (CTED) can assist States to identify and share good practices in this area, and to facilitate the delivery of technical assistance and financial support to ensure implementation of the relevant Council resolutions and the Committee’s related recommendations.