CTED Trends Alert

The weak link in border security: Maritime borders and use of passenger data

CONTENTS

Introduction

Terrorists continue to exploit border security vulnerabilities to move between countries, establish networks and connections, and ultimately conduct attacks against civilian populations.

In several resolutions, the Security Council calls upon Member States to implement effective border management frameworks to curtail terrorist travel. Robust international cooperation, including through information-sharing and the use of the International Criminal Police Organization's (INTERPOL) databases, has resulted in successful interdiction (and, at times, investigation and prosecution) of foreign terrorist fighters (FTFs) returning from conflict zones in the Syrian Arab Republic and Iraq.

One of the most important international information-sharing mechanisms is the transmission of advance passenger information (API)/passenger name records (PNR) data between departure and arrival States by airlines. These systems have been put in place to implement the passenger screening required in resolutions 2178 (2014) and 2396 (2017). They represent positive outcomes in States' efforts to enhance their border security.

However, terrorist organizations continue to adapt to counter-terrorism measures adopted by Member States by utilizing counterfeit documents, exploring alternative transportation methods, including maritime routes, leveraging encrypted communications to coordinate travel, and exploiting governance gaps in conflict zones and fragile States to establish safe havens.

The more effective border security at airports becomes, the more attractive alternative transportation methods will become. **Maritime border security has not received the same investment and attention that the aviation sector has received, and it therefore is at risk of becoming an exploitable weak link in the chain.**

Recognizing this emerging vulnerability, United Nations bodies continue to assess the scope and implications of maritime security gaps. The Counter-Terrorism Committee Executive Directorate (CTED) addresses issues related to maritime security in the counter-terrorism context during its country assessments conducted on behalf of the Counter-Terrorism Committee. CTED's dialogue with Member States and engagement with members of its Global Research Network indicate that terrorists, as well as illicit goods, move via maritime channels, including to cover specific segments of a broken travel journey that encompasses land, air and maritime transport. Through its assessments and dialogue with relevant stakeholders, CTED continues to highlight challenges to border security, including maritime security.

Vulnerabilities at maritime borders, including the lack of comprehensive passenger screening measures, among other challenges, represent a significant obstacle to the international community's counter-terrorism efforts. These vulnerabilities include increased FTF travel-related risks and risks associated with possible attacks in the maritime sphere. While the aviation sector's progress in implementing passenger screening systems demonstrates the effectiveness of coordinated international measures, addressing maritime security gaps requires a clear understanding of the existing frameworks to further prevent terrorist travel, as well as of the unique challenges of the maritime domain.

United Nations guidance on curtailing terrorist travel

Several Security Council resolutions provisions address relevant components of effective border management to curtail terrorist travel. The Council notes that all measures taken to counter terrorism must comply with Member States' obligations under international law, including international human rights law, international humanitarian law and international refugee law. Resolutions 2178 (2014), 2396 (2017), and 2482 (2019) set requirements for Member States on developing systems for managing border security, including collecting and analysing API and PNR data, with full respect for human rights and fundamental freedoms.[1] For Member States, the resolutions provide a framework for disrupting terrorist mobility by integrating basic border security measures with advanced data analytics, enhanced border controls, and international cooperation. API and PNR programmes enable the identification and tracking of FTFs across international borders and have proved beneficial for security, facilitation, and enforcement.[2,3]

- Drawing from these resolutions, international standards and recommended practices, the United Nations has developed a comprehensive capacity-building initiative under the Countering Terrorist Travel Programme that assists Member

---

[1] Guidance can be found in the Addendum to the Madrid Guiding principles, available at www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-on-foreign-terrorist-fighters.pdf , and in the International Civil Aviation Organization/International Air Transport Association (IATA)/World Customs Organization (WCO) API/PNR Toolkit.

[2] See Kunio Mikuriya (WCO News), "API and PNR: two key words on the global security agenda", 10 June 2015. Available at https://mag.wcoomd.org/magazine/wco-news-77/api-and-pnr-two-key-words-on-the-global-security-agenda/.

[3] Office of the United Nations High Commissioner for Human Rights, *Guidance to States on Human Rights-Compliant Responses to the Threat Posed by Foreign Fighters* (New York, 2018), pp. 33 and 34. Available at www.ohchr.org/sites/default/files/newyork/Documents/Human-Rights-Responses-to-Foreign-Fighters-web_final.pdf.

States in designing systems to prevent, detect and investigate terrorist offences and related travel[4]

- In addition, States may also develop a national system, procure a commercial solution, or adopt a donor-provided system to bolster border management. The IATA World Tracker shows that globally 100 Member States have implemented API while 67 have implemented PNR into border security. Meanwhile, 63 Member States have implemented both, 46 Member States have not implemented API and 91 have not implemented PNR.[5]
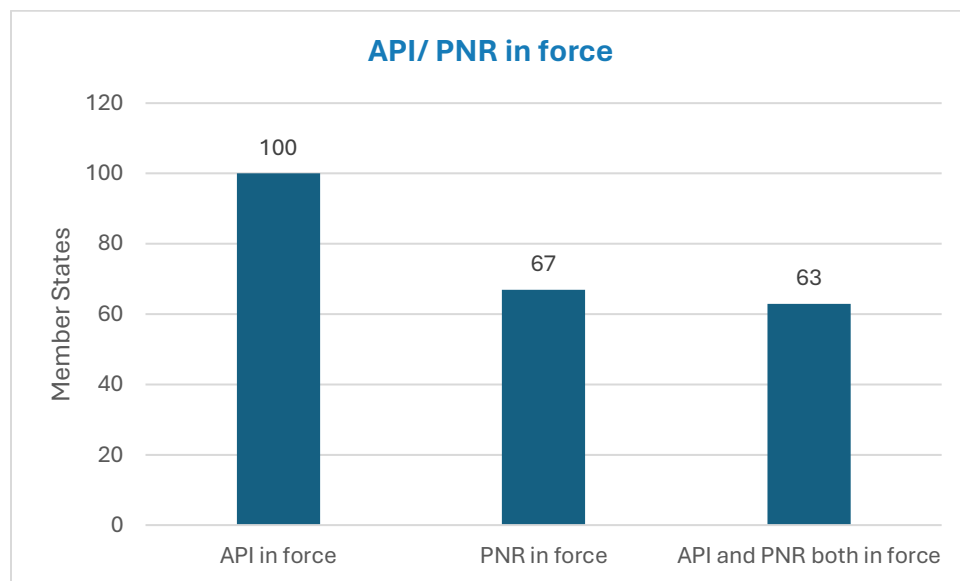

Figure I

API/ PNR authorized, not in force

Figure II

API/ PNR not implemented
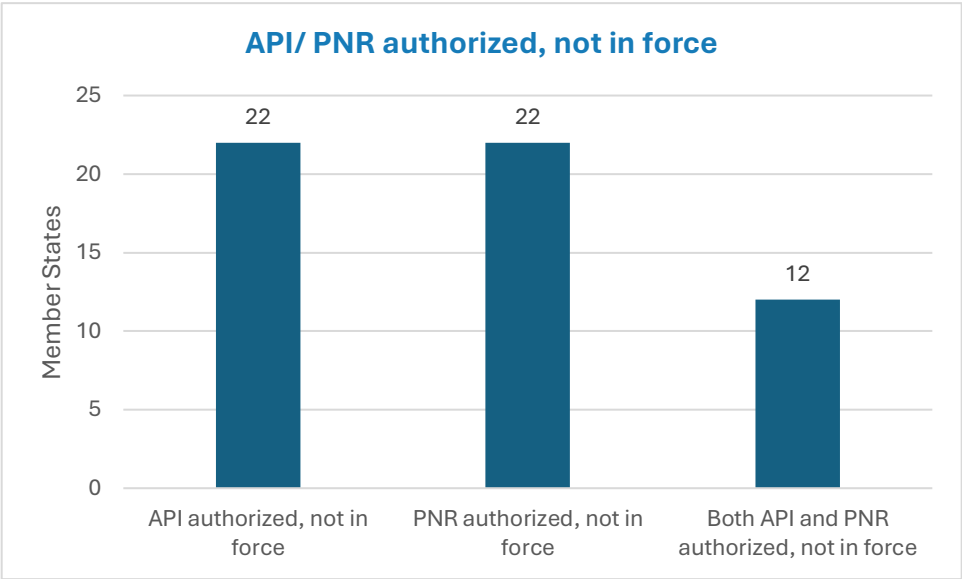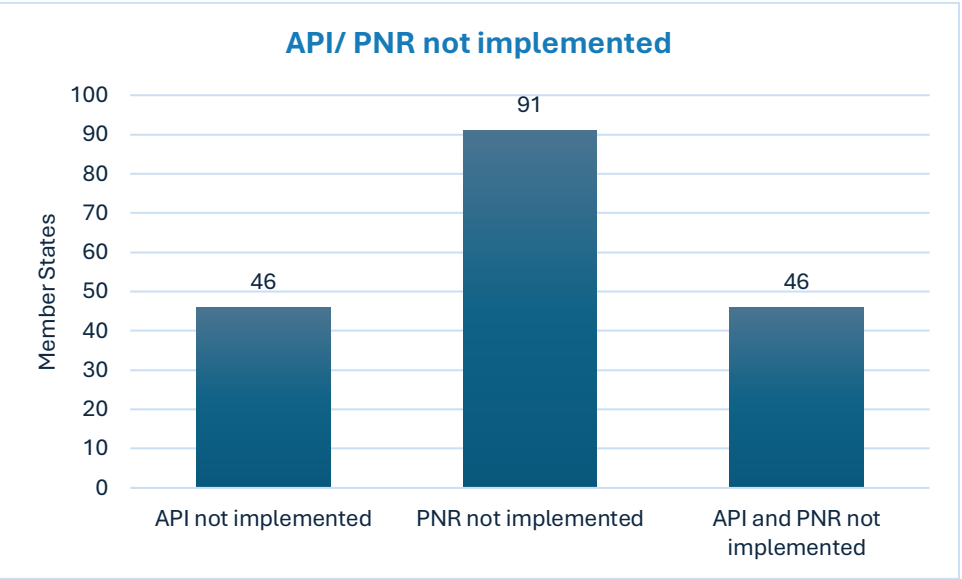
Figure III

Maritime border management challenges

While States have invested in advanced screening in the aviation sector, similar efforts have not been made for travel across maritime borders. Maritime travel can be exploited by terrorists to leave, transit or enter Member States' territories, including to perpetrate terrorist attacks. Loopholes in border and customs controls related to maritime travel and cargo transportation can also be abused for terrorism financing purposes (notably through cross-border transportation of cash and valuable goods) and circumvention of relevant sanctions, as well as for various forms of trafficking (including in weapons), whether at sea (mainly via container ships) or at port facilities.

Many Member States, in particular coastal States that lack equipment and capacity (at sea, on the coast, and in ports) to monitor and track the movements of vessels and to control and verify travel documents and goods, have reported to CTED that their lengthy and porous coastal regions and maritime zones are difficult to control.

INTERPOL's Operation Neptune I, II, and III has led to arrests of FTFs and highlighted that a significant number of FTFs travelled via Mediterranean ferry routes to the conflict zones of the Middle East and back to their countries of origin, compromising regional security in Europe and Africa. Routes in the eastern Mediterranean, together with those between North Africa and Southern Europe, have been utilized by terrorist groups, who use gaps in regulations to travel, transport, and move funds and illicit resources.

> ❖ FTFs have attempted to avoid detection and border controls on their way to conflict zones by using "broken travel" patterns, especially across maritime borders, that include passage aboard cruise ships, using falsified or stolen travel documents, exploiting **"weak links" in border management** measures to avoid surveillance.
>
> ❖ Increased security measures and the adoption of API/PNR in the aviation field can potentially incentivize terrorist **exploitation of maritime transport as a less risky option** to move undetected, with minimal risks.

During its assessment visits, CTED has observed the challenges many Member States face in effectively securing maritime borders. Member States also face gaps in implementing a whole-of-government approach to maritime security[6] and implementing

---

[6] See International Maritime Organization, "Whole of government approach to maritime security" (accessed 9 June 2025). Available at www.imo.org/en/OurWork/Security/Pages/Whole-of-Government-Approach-to-Maritime-Security.aspx.

the International Ship and Port Facility Security Code ([ISPS Code](#)) detailing maritime and port security-related requirements that International Convention for the Safety of Life at Sea Contracting Governments, port authorities and shipping companies must adhere to.

Other challenges include the lack of financial and human resources, equipment and specialist skills. A disconnect between maritime security and overall counter-terrorism policy can often result in gaps in information relevant to the development of security measures in the maritime domain, including protection of ports and other maritime assets as part of States' critical infrastructure.

This creates a security gap despite evidence that terrorists utilize maritime channels, particularly as part of "broken travel" routes combining multiple transportation modes.

The challenges of maritime border security, including resource constraints, technical limitations, and operational complexities, are multifaceted. These challenges, together with unique features of the sector, underscore some of the difficulties in integrating security measures in the maritime sector that are similar to aviation security measures. These challenges also highlight the urgent need for targeted solutions that can address the unique characteristics of maritime transportation.

However, the characteristics of maritime transport of passengers are different from those of air transport, which complicates the implementation of API and booking and reservation information (BRI) measures (the term PNR is not used in the maritime domain since it is specific to air transport). In particular, passenger ships may transport thousands of passengers in short maritime passages in a pressurized environment in peak season; for example "Operación Paso del Estrecho", also known as "Operation Marhaba" between Spain and Morocco, moved 3,442,770 passengers and 847,429 vehicles between 13 June and 15 September 2024, between the ports of Algeciras, Tarifa and Almería in Spain, Ceuta, and Nador and Tangier in Morocco.

Advance passenger information and booking and reservation information and maritime security

While CTED has observed significant investment in API/PNR for border crossings by air, it has not yet observed any State implement similar screening methods using BRI for passenger data or passengers using maritime modes of transport. CTED has observed one State that is investigating expanding API/PNR to rail and bus transport.

Ongoing efforts to curtail terrorists' ability to move across borders, find safe havens, and prevent illicit criminal activities, such as trafficking, can be strengthened by adopting comprehensive, human rights-compliant border security measures, including API/BRI,

implemented in the maritime domain. However, in addition to the lack of international standards in API/BRI use in the maritime sphere, there are additional unique challenges:

- The technical challenges of implementing standardized passenger data collection in the maritime sector are amplified by the diverse technical capabilities of maritime carriers, which have different types of infrastructure and of operations (cruise ships, ferries, cargo vessels carrying passengers) and varied data collection practices
- Unlike commercial airlines that typically use standardized reservation systems, maritime operators often employ varied booking methods ranging from sophisticated digital platforms to basic spreadsheets, making data collection inconsistent[7]
- Maritime transportation features less structured boarding processes than aviation, with passengers often able to purchase tickets shortly before departure, limiting pre-arrival screening opportunities, especially in the case of ferries
- The operational environment presents additional and unique difficulties – maritime vessels may visit multiple ports across different jurisdictions during a single journey, requiring compliance with varying regulatory frameworks and data formatting standards that create a complex compliance landscape, especially for smaller operators with limited resources
- While the foundations for the collection of API data appear to be in place in most countries for passenger and merchant ships involved in international travel, based on current Maritime Facilitation Regulations,[8] the concept of BRI is absent from the maritime sector, especially in the lack of an industry standard for the harmonization of booking information.[9]

Some steps have been taken to develop an international legal basis for the reporting of API and BRI data in the maritime sector and to ensure consistent, standardized and efficient approaches. A proposal for an amendment to the Convention on Facilitation of International Maritime Traffic (FAL Convention) was made in December 2024. That proposal is for the inclusion of new reporting requirements for API and BRI data for cruise ships or other maritime means of transport. The proposal received approval by

---

[7] Manu Niinioja (Border Security Report), "Maritime passenger targeting", 13 May 2022. Available at www.border-security-report.com/maritime-passenger-targeting/.

[8] The Regulations are part of legal framework established under the FAL Convention.

[9] The 2018 Addendum to the 2015 Madrid Guiding Principles states that States should ensure that national legislation clearly regulates the way in which States can collect, use, retain and transfer API and PNR data and that PNR data-processing and retention frameworks incorporate oversight and privacy protections, while also ensuring that precautions are taken against the misuse or abuse of the data by State authorities. Available at www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_1177.pdf .

the International Maritime Organization Facilitation Committee but is yet to be finalized.

At its forty-ninth session, in London from 10 to 14 March 2025, the Facilitation Committee of the International Maritime Organization (IMO) agreed the following principles on API/BRI:

- To include API as a new declaration in the FAL Convention, which would include a transition period to provide flexibility to Member States and industry to adapt their systems, before API declaration would replace the existing crew list and passenger list declarations;

- To not use the term "Passenger Name Record data (PNR)", since it is specific to air transport, and to use "booking and reservation information (BRI)";

In addition, the Committee established a Correspondence Group on Amendments to the Annex of the FAL Convention on API and BRI, coordinated by France, because it was not possible to finalize the amendments to the annex to the FAL Convention on API and BRI at the forty-ninth session.

For its fiftieth session, the Facilitation Committee of IMO will convene in London from 23 to 27 March 2026. If the amendments to the annex of the FAL Convention are approved, the Committee will adopt the amendments in its session in the first half of 2027, and API and BRI reporting would enter into force 1 January 2029.

Examining these dimensions reveals both the obstacles and the opportunities in strengthening global border security measures through comprehensive passenger screening across all transportation modes, including the maritime sphere, in accordance with domestic laws and international obligations, including in the area of international human rights law.

Key Insights:

In resolutions 2178 (2014) and 2396 (2017), the Security Council addresses the implementation of API and PNR in the context of civil aviation but not in the maritime sphere.

*The lack of a globally standardized use of API and PNR data for maritime borders creates potential weakness in the overall border management system, **representing a vital gap and vulnerability in the counter-terrorism architecture** to curtail terrorist travel, which needs to be addressed on an urgent basis.*

*During its assessment visits, CTED has noted that **Member States face ongoing challenges in collecting complete and reliable data to support risk assessments in the maritime sector**, including assessing risks stemming from foreign ports. Extending access to API and BRI/PNR data to screen maritime travelers would further strengthen maritime border protection.*