SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Travel intelligence as a tool for counterintelligence and border security

Anastasios-Nikolaos Kanellopoulos

ankanell@aueb.gr

[1] https://orcid.org/0009-0001-1875-9264

Department of Business Administration, Athens University of Economics and Business, Patision 76, 112 57, Athens, Greece

Abstract

Counterintelligence and border security are two cornerstones of national security protection processes. They utilise intelligence sources and procedures extensively to assist in decision-making regarding countermeasures against high-degree threats and risks. Both employ intelligence cycle activities and risk analysis models to combine information coming from the operational environment. At the same time, travel intelligence (TRAVINT) consists of the intelligence product arising from the collection and analysis of a wide range of travel companies and data and information from governments. In the modern and increasingly globalised security environment, TRAVINT products constitute growing trend for protecting state border, intelligence, and internal security. The paper aims to explore the potential of leveraging TRAVINT for enhancing counterintelligence efforts and bolstering border security measures. The research methodology combines empirical analysis with a comprehensive review of the US and EU public documents and academic papers. This study is necessary, as it is essential to examine the worthiness of TRAVINT as an emerging intelligence sector. TRAVINT appears to be an extremely important data, information, and intelligence source offering the required material input to law, security, and intelligence enforcement agencies for analysis. TRAVINT and its parts, such as passenger name records (PNR) data, are used in compliance with state legislation in respect of human rights and in accordance with the needs of Intelligence networks, where excessive threats to internal and border security are implied.

Keywords

national security, PNR, counterintelligence, border security, TRAVINT

Article info
Received: 1 October 2023
Revised: 23 October 2023
Accepted: 25 October 2023
Available online: 23 November 2023

Citation: Kanellopoulos, A-N. (2024) 'Travel Intelligence as a tool for counterintelligence and border security', *Security and Defence Quarterly*, 45(1), doi: 10.35467/sdq/174523.

Introduction

Counterintelligence refers to activities and measures taken to identify, assess, and counteract the threats posed by foreign intelligence services (FIS) or other malicious actors seeking to gather sensitive information or undermine the security of a country or an organisation. Border security is also the first-level approach against any threats and risks that attempt to enter a state's security environment (Bellanova and Glouftsios, 2020, pp. 4–6). Both intelligence and security functions utilise processes of data, information and intelligence collection, management, and analysis based on intelligence management models, such as the intelligence cycle and risk analysis models, for instance the European Common Integrated Risk Analysis Model (CIRAM) (Fernández-Rojo, 2021, pp. 14, 22–24; Frontex, 2012a, pp. 5–6).

Travel intelligence TRAVINT also functions as a common intelligence aspect for both travel companies and government security agencies. In this domain, passenger name records (PNR), play a significant role, offering the opportunity to locate any emerging security and intelligence threats (De Hert and Papakonstantinou, 2010, pp. 1–2; US Department of Homeland Security and US Customs and Border Protection, 2013, pp. 1–3).

This paper examines the aspects and components of counterintelligence and border security using a research approach to TRAVINT's role in both functions. Objectives of the research revolve around investigating the principles and the value of TRAVINT as an intelligence input for both counterintelligence and border security functions. The research methodology used in this study is a multifaceted approach that integrates empirical analysis, thorough examinations of academic papers, and the invaluable inclusion of expert insights gleaned from a meticulous examination of public documents from both the United States and the European Union (EU). This comprehensive methodology is designed to provide a holistic and well-rounded perspective on counterintelligence, border security, and the emerging field of TRAVINT. It is worth noting that the term "TRAVINT" does not seem to have been documented previously in any existing academic article or book. Instead, it emerges as a novel concept closely linked to the official documents released by the European Commission and Frontex, both of which are extensively referenced and cited in this study. This observation underscores the innovative and timely nature of the research, as it seeks to elucidate a concept that has not yet been widely explored in academic or literary sources. Later in the paper, the author strives to address a notable research gap by examining the underexplored intersection of TRAVINT with other intelligence and security sectors. These examinations endeavour to highlight the worthiness of TRAVINT as an emerging intelligence sector.

While the paper offers valuable insights into the emerging field of TRAVINT, it is important to acknowledge its limitations, one of which is its predominantly US- and EU-centric focus. The research heavily relies on data and academic papers from the United States and EU, which may inadvertently skew the findings and recommendations towards the specific dynamics of these regions. TRAVINT raises a global concern, and its implications are not limited to these areas alone. Consequently, the applicability of the research's insights in the regions such as Asia, Africa, or South America may require further exploration and adaptation. Furthermore, the paper's exclusive focus on public and academic sources might overlook valuable insights from non-traditional and on-the-ground intelligence sources. Therefore, to enhance the comprehensive applicability of TRAVINT, the future research should try to broaden its geographical scope and incorporate diverse perspectives and sources.

Counterintelligence Theory and Practice

Counterintelligence theory refers to the principles, concepts, and strategies used in the field of interfering malicious intelligence acts (Ehrman, 2009, pp. 4–5, 14–18; Prunckun, 2019, pp. 37–51). It is a discipline within intelligence and security that focuses on identifying, understanding, and countering threats posed by FIS, such as espionage, and covert activities. It involves efforts to protect a country's national security secrets and prevent the unauthorised acquisition of sensitive information (Melendez, 2019, pp. 1–4). Theoretically, it is a subject of interest for both former intelligence officials and security studies, strategic studies, and intelligence studies. In particular, relevant literature arising from former intelligence executives of western countries' agencies such the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), MI6, and MI5. The written efforts of John Ehrman, and Michelle K. Van Cleave set up the strategic and operational aspects of the matter but often lack an academic and structured approach (Cram, 1993, pp. 1–80; Ehrman, 2009, pp. 1–27; Van Cleave, 2007, pp. 1–44). Another publication that covers a wider range of counterintelligence is Johnson's (2010) handbook which approaches the subject comprehensively, focusing on historical aspects and emphasising its ever-increasing value. In the same direction, Sims and Gerber's (2009, pp. 34–36, 128–129) book, *Vaults, mirrors, and masks*: *Rediscovering U.S. counterintelligence*, offers a focus on decision-making and the denial deception features of the process.

Counterintelligence, much like the metaphorical "sword" and "shield" used in the Soviet parlance to refer the KGB (*Komitet gosudarstvennoy bezopasnosti*), consists of two distinct yet interconnected functions, the offensive and defensive functions (Prunckun, 2019, pp. 25–28; Richelson, 1986, pp. 1–10). The offensive function is equated to the "sword," as it involves proactive efforts to identify, infiltrate, and disrupt intelligence activities which may encompass espionage, cyber attacks, or covert operations (Prunckun, 2019, pp. 49–52). This proactive stance is focused on identifying adversaries, collecting intelligence on their intentions, and neutralising their efforts. The main component of offensive counterintelligence is counterespionage (Prunckun, 2019, pp. 55, 216–217). It is a multifaceted discipline composed of detection, deception, and neutralisation. Firstly, it involves the meticulous detection of espionage activities and covert intelligence threats directed against an organisation or nation (Melendez, 2019, pp. 14–17). This process entails constant monitoring and vigilance to identify potential spies and their tactics. Secondly, it utilises deception techniques to confound adversaries, misdirect their efforts, and protect sensitive information (Prunckun, 2019, p. 9). These tactics may involve creating false leads, disinformation campaigns, or covert operations to disrupt the plans of intelligence adversaries (Prunckun, 2019, pp. 9, 49). Finally, once detected, counterespionage focuses on the neutralisation of espionage threats, ensuring that the nation's secrets remain safe (Prunckun, 2019, pp. 49–50).

In contrast, the defensive function operates as the "shield," forming a protective barrier to prevent and mitigate espionage, sabotage, and other intelligence threats targeted at an organisation or nation (Melendez, 2019, pp. 20–23). This defensive aspect is the guardian of an entity's secrets, ensuring that sensitive information is protected, and critical assets remain secure (Prunckun, 2019, pp. 55–64).

Specifically, threat identification, a fundamental element of defensive counterintelligence, involves the systematic analysis and assessment of potential threats—whether they emanate from FIS, insider threats, or other sources (Melendez, 2019, pp. 12–14; Prunckun, 2019, pp. 65–74). It is a process that aims to recognise the vulnerabilities and risks (Prunckun, 2019, pp. 75–78). Information protection is also another pivotal aspect of

defensive counterintelligence. It encompasses the secure handling of sensitive data, ensuring it remains inaccessible to unauthorised parties (Prunckun, 2019, pp. 55–64; Sims and Gerber, 2005, pp. 226–228). Over time, the responsibility for overseeing the procedures and operations associated with counterintelligence is entrusted to the collaborative efforts of proficient intelligence officers specialising in border and national security. Success of counterintelligence depends on the collection of appropriate information, which will lead, through the use of analytical tools, to the identification of any security gap and threat (Melendez, 2019, pp. 17–19).

Border security

Border security theory refers to the concepts and strategies used to protect a country's borders and ensure the security of its territory (Frontex, 2012b, p. 12; Oliveira Martins *et al.*, 2022, pp. 1–3; Wagner, 2021, pp. 77–81). It encompasses various approaches and practices, including the deployment of physical barriers, surveillance technologies, law enforcement personnel, and immigration policies (Frontex, 2012a, pp. 5–6). The main objective of border security is to prevent unauthorized entry, detect and intercept illegal activities, such as smuggling and terrorism, and maintain the safety of a nation (Frontex, 2012a, pp. 27–30; Hansen and Pettersson, 2021, pp. 3, 10; Oliveira Martins *et al.*, 2022, pp. 8–11).

Border security management relies on risk analysis models in support of effective border surveillance and control (Frontex, 2012a, pp. 10–12; Jeandesboz, 2020, pp. 15–16; Wagner, 2021, p. 234). Risk analysis is a process used by border security agencies to assess potential threats and vulnerabilities at the border and prioritise their response accordingly (Shepherd, 2022, pp. 6–9). In the last decade, agencies such as Frontex in Europe and Customs and Border Protection (CBP) in the United States have developed their own risk analysis models such as CIRAM, including specific intelligence procedures in their daily functioning (Frontex, 2012a, pp. 36–37; Léonard, 2010, pp. 1–5; Liashuk and Tsaruk, 2021, pp. 2–4).

Specifically, procedures of risk analysis are employed to assess risks and identify potential threats (Frontex, 2012a, pp. 20–26; Wagner, 2021, pp. 337–339). Their data collection processes may encompass border and internal security relevant data and information, such as traveller data (e.g. PNR information), cargo manifests, intelligence reports, watchlists, and other sources of data, to develop a comprehensive understanding of potential threats from terrorism, smuggling, illegal immigration, and more (Morral *et al.*, 2011, pp. 23–24). The data mining and analysis of these sources of information lead to pattern recognition and predictive modelling that assist in modus operandi and identificationof relationships that may indicate potential security risks (Frontex, 2013, pp. 13–23; Liashuk and Tsaruk, 2021, pp. 4–6).

Furthermore, border and security agencies proceed to risk prioritisation by allocating their resources, focusing on the highest-risk areas or individuals, and promoting strategies to mitigate the most serious problems, such as dealing with serious organised crime and terrorism (Frontex, 2013, p. 33–35; Wagner, 2021, pp. 349–350). This allows them to optimise security measures and respond to potential threats more effectively by deploying advanced screening technologies or targeting specific routes or individuals for further inspections (Jeandesboz, 2020, pp. 15–16; Oliveira Martins *et al.*, 2022, pp. 4–5; US Department of Homeland Security Privacy Office, 2017, pp. 25–27; Wagner, 2021, pp. 319–321).

By combining border security intelligence and risk analysis, authorities can eventually proactively identify and address potential security threats while efficiently managing the flow of legitimate travellers and goods across borders (European Parliament, 2016, pp. 14–15).

Defining Travel Intelligence and Counterintelligence

TRAVINT plays a decisive role in ensuring national security and proper border security by providing valuable information about potential threats, risks, and suspicious activities related to those people and material that are, geographically, in transition. It involves the systematic collection, analysis, and utilisation of travel-related information and intelligence to enhance security measures and law enforcement efforts. It focuses on data generated by activities such as passenger travel, including PNR, advance passenger information (API), and the European Travel Information and Authorisation System (ETIAS) (European Parliament, 2016, pp. 30–33; Frizberg, 2023, pp. 1–4; Namazov, 2022, pp. 7–11; National Counterterrorism Center, 2013, p. 60; Priestley and Beauvais, 2021, pp. 3–6; Romanian Parliament, 2019, p. 1; Wagner, 2021, p. 362).

The history of TRAVINT in the context of the EU and the United States has evolved over the years in response to the growing need for enhanced security measures. In the EU, the Europol Travel Intelligence Center (ETIC) was established in 2019 as part of Europol's horizontal operational services. It represents a coordinated effort to use travel-related data to combat security threats within the EU (Frontex, 2020, pp. 1–10; Romanian Parliament, 2019, p. 1). The development of such capabilities is in line with the EU's commitment to the collection and sharing of travel data as outlined in the EU PNR directive 2016/681 (Priestley and Beauvais, 2022, p. 9). In the United States, similar efforts have been made through organisations, such as the transportation security administration (TSA) and the Department of Homeland Security (DHS), by gathering travel-related data for security and border protection purposes. Both regions have recognised the significance of TRAVINT in bolstering their security and law-enforcement efforts, making it a pivotal component of their national and regional security strategies.

Furthermore, intelligence products emerging from TRAVINT provide critical insights into traveller movements, patterns, and potential security threats (Frontex, 2020, pp. 1–10). These products are mainly utilised for the following activities:

- *Threat identification*: TRAVINT helps to identify individuals or groups who may pose a threat to national security. By monitoring travel patterns, conducting background checks and analysing passenger data (such as PNR information), authorities can identify individuals who have connections to terrorism, criminal activities, or other security concerns (National Counterterrorism Center, 2013, p. 6; US Department of Homeland Security Privacy Office, 2015, pp. 14–16, 2017, pp. 2–4).
- *Risk assessment*: TRAVINT provides insights for assessing the potential risks associated with certain destinations, travel routes, or transportation modes. This information helps authorities to determine the level of security measures required and allocate resources accordingly (National Counterterrorism Center, 2013, p. 5; US Department of Homeland Security Privacy Office, 2015, pp. 15–16; US Government Publishing Office, 2011, pp. 4–14).
- *Response to emerging threats*: TRAVINT enables authorities to respond promptly to emerging threats or security incidents. By continuously monitoring and analysing

travel-related information, agencies can detect potential trends, patterns, or changes in threat levels and adjust their security strategies accordingly (National Counterterrorism Center, 2013, p. 35; US Department of Homeland Security Privacy Office, 2015, p. 11).

- *Watchlist management*: TRAVINT is used to maintain and update watchlists, which include individuals who are security risks. These watchlists help border security agencies to identify and screen individuals who should receive extra focus during travel (National Counterterrorism Center, 2013, pp. 6–10; US Department of Homeland Security Privacy Office, 2015, p. 13, 2017, p. 8).
- *Intelligence-sharing*: Collaboration and sharing of TRAVINT among different national security agencies and international partners is crucial. By sharing relevant information, such as suspect profiles, travel itineraries, or suspicious activities, countries can enhance their collective ability to detect and prevent security threats (Frontex, 2020, pp. 1–10; US Department of Homeland Security Privacy Office, 2015, pp. 15–20, 2017, pp. 14–15).
- *Border control and screening*: TRAVINT supports the implementation of effective border control measures. By analysing travel data and intelligence, authorities can identify high-risk travellers and allocate resources towards those who require further scrutiny and monitoring (National Counterterrorism Center, 2013, pp. 43–46).

With regard to PNR, it is a specific record that contains information about a passenger's travel arrangements (De Hert and Papakonstantinou, 2010, pp. 1–4; European Union, 2016, pp. 1–4; Glouftsios and Leese, 2022, pp. 1–2; Namazov, 2022, pp. 10–12). It typically includes details such as the passenger's name, contact information, travel itinerary, ticket information, seat assignments, and other relevant data (Glouftsios and Leese, 2022, pp. 3–5; US Department of Homeland Security and US Customs and Border Protection, 2013, pp. 1–8). PNR data is collected by airlines and travel agencies as part of the booking process and can provide valuable information to intelligence and law enforcement agencies for various purposes, such as identifying potential threats, tracking individuals of interest, or identifying patterns of suspicious travel behaviour

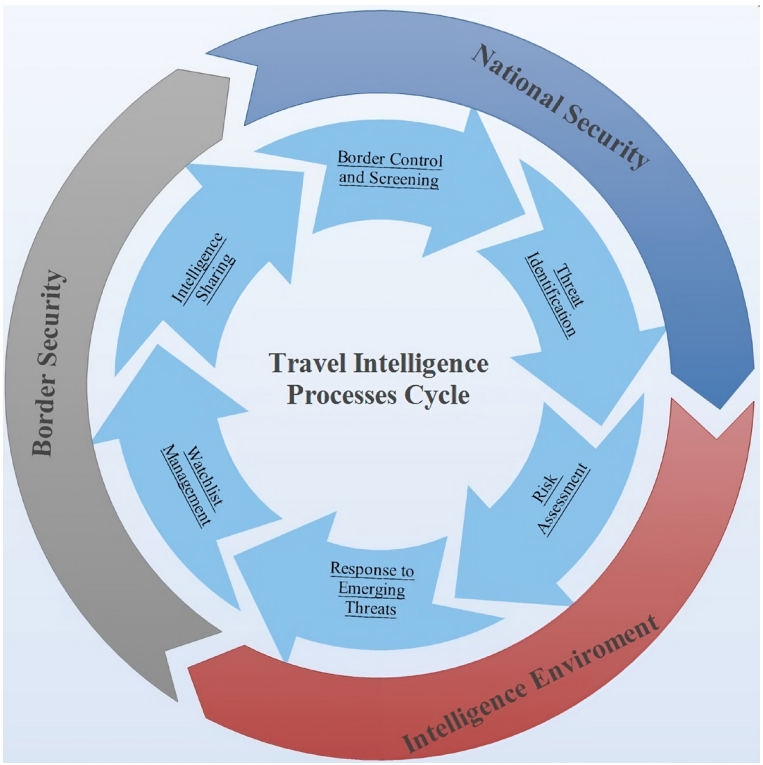

Figure 1. Main processes of travel intelligence.

(US Department of Homeland Security Privacy Office, 2015, p. 13). It's important to note that the collection and use of PNR data for intelligence purposes may have privacy implications and it is subject to legal and regulatory frameworks in different jurisdictions (De Hert and Papakonstantinou, 2010, pp. 1–4). Nonetheless, it is a critical part of the detection function within the domain of both defensive and offensive counterintelligence (Prunckun, 2019, pp. 121, 147, 178, 185). TRAVINT, in the context of PNR, also refers to the analysis and use of PNR data for intelligence and security purposes (De Hert and Papakonstantinou, 2010, pp. 1–4; European Union, 2016, pp. 1–4; Glouftsios and Leese, 2022, pp. 6–7). By analysing PNR data, intelligence agencies can detect anomalies or red flags that might indicate suspicious or illicit activity, such as individuals travelling to high-risk destinations, multiple individuals booking tickets on the same itinerary with no apparent connection, or other patterns that may warrant further investigation (Namazov, 2022, pp. 7–12). Overall, TRAVINT derived from PNR data can help enhance security, prevent terrorism, combat human trafficking, and support law enforcement efforts (Rudner, 2014). It can be used as part of a larger intelligence picture to assess and mitigate potential risks associated with travel (Barnea, 2019, pp. 9–10). That said, it does require considerable dedication to cooperation between all relevant defence and security agencies, as well as the commercial sector, to provide access to the data/information/intelligence for all.

In the context of border security, PNR has an important role in supporting the screening and vetting processes carried out by the authorities (European Union, 2016, pp. 1–4; Glouftsios and Leese, 2022, pp. 7–9; Namazov, 2022, p. 26; Van Dongen, 2010, p. 5). Border security agencies use PNR data to identify potential security risks and to facilitate the efficient and effective management of border control. By analysing PNR data, border security officers can determine whether any passengers on incoming or outgoing flights raise concerns or require additional scrutiny. Plus, PNR data allows border security agencies to identify individuals who may be on watchlists, such as terrorist watchlists or those involved in criminal activities (European Union, 2016, pp. 8–11; Glouftsios and Leese, 2022, pp. 12–15; Rudner, 2014; US Department of Homeland Security Privacy Office, 2017, p. 18). It can also assist with the identification of passengers with suspicious travel patterns, such as multiple one-way tickets or frequent travel to high-risk destinations.

Travel Intelligence, Border Security, and Counterintelligence

Counterintelligence and border security are two separate concepts, but they intersect and are mutually reinforcing within the context of national security. As counterintelligence refers to activities undertaken by a government or an organisation to identify, understand, and counter threats posed by FIS or other threat actors, it involves gathering information, analysing intelligence, and implementing measures to protect sensitive information and thwart espionage or sabotage attempts (Melendez, 2019, pp. 12–14; Riehle, 2015). Concurrently, border security focuses on protecting a country's borders and ensuring the integrity of its territory. It involves measures such as physical barriers, surveillance systems, patrols, and presence of law enforcement to prevent unauthorised entry, smuggling, trafficking, and other illegal activities (Oliveira Martins *et al.*, 2022, pp. 10–14). Several of these security measures are described by Prunckun (2019) within the context of defensive counterintelligence and typically as part of the defence counterintelligence tenet elaborating on defence-in-depth.

While counterintelligence primarily focuses on intelligence gathering and protection on a country's own territory, it can intersect with border security when there is concern about

FIS or threat actors attempting to exploit vulnerabilities at the border. In such cases, counterintelligence efforts may be integrated into border security strategies to identify and mitigate potential threats. Eventually, both counterintelligence and border security play important roles in maintaining national security, but they deal with different aspects of protecting a country's interests.

In the context of PNR, counterintelligence may involve the analysis of PNR data to identify suspicious travel patterns or activities that could indicate espionage, sabotage, or other threat activities conducted by FIS or individuals acting on their behalf. Certainly, detecting espionage and intelligence threats from PNR data can be a complex task that requires careful analysis and investigation. PNR data is primarily used by authorities for purposes, such as preventing terrorism and serious organised crime (Frontex, 2020, pp. 1–10). However, by analysing PNR data, intelligence agencies can potentially research for indicators, such as multiple individuals travelling together with no apparent connection, sudden changes in travel plans, unusual or high-risk destinations, or other suspicious patterns, that may suggest intelligence-related activities. Specifically, the tactical and operational approaches for detecting this pursuit are as follows:

- *Pattern intelligence analysis*: Analysing patterns in PNR data can help identify anomalies or suspicious activities. This can include looking for unusual travel itineraries and frequent changes in travel plans or connections to known espionage hotspots (European Commission, 2023; Frontex, 2020, pp. 1–10).
- *Social network analysis*: Conducting link analysis on PNR data can help identify connections between individuals or groups that may be involved in espionage activities. This can involve analysing shared travel patterns, common contacts, or other indicators of collaboration (Shulsky and Schmitt, 2009, pp. 11–18).
- *Travel behavioural analysis*: Examining the behaviour of individuals or groups in PNR data can provide insights into potential espionage activities. This can include analysing social behavioural and travel patterns, unusual booking behaviour, or other indicators of suspicious activity (European Commission, 2023; Frontex, 2020, pp. 1–10).
- *Integration with other intelligence sources*: Integrating PNR data with other intelligence sources, such as open-source intelligence or human intelligence (HUMINT), can provide a more comprehensive picture of potential espionage activities. This can help corroborate findings and provide additional context (European Commission, 2023; Frontex, 2020, pp. 1–10).

Considering the HUMINT sources, offensive counterintelligence efforts may involve monitoring and assessing the activities of FIS or suspected foreign agents who may be attempting to collect information or exploit vulnerabilities within a country or organisation (Stouder and Gallagher 2013, pp. 3–12). This may include tracking their travel patterns, understanding their contacts and associations, and identifying potential threats or vulnerabilities. On these occasions, watch-listing operational processes are promoted (National Counterterrorism Center, 2013, pp. 11–12; US Department of Homeland Security Privacy Office, 2017, p. 27; US Department of Homeland Security and US Customs and Border Protection, 2013, pp. 1–8).

The case of Alexander Yuk Ching Ma

The case of Alexander Yuk Ching Ma involves a former CIA officer who was arrested and charged on 14 August 2020 with espionage-related offences (Office of Public Affairs, 2022, pp. 1–5). Alexander Yuk Ching Ma was a naturalised US citizen born in Hong Kong, who worked as a CIA officer in the 1980s and later as a contract translator

for FBI in the 2000s and was charged with conspiracy to communicate, deliver, and transmit national defence information to the Chinese government for more than a decade. He allegedly provided information about CIA's personnel and tradecraft to Chinese Intelligence for personal gain (US Department of Justice, 2020).

Specifically, the case against him has been described as complex and there have been requests for a competency evaluation to determine his ability to stand trial. According to court documents, Ma expressed his desire for the "motherland" to succeed during conversations with an undercover FBI agent posing as a Chinese intelligence officer. Eventually, senior officials referred to Ma as a classic example of an insider threat. Their comments highlight the issue of former American intelligence officers who have betrayed their colleagues, country, and democratic values to support an authoritarian regime (US Department of Justice, 2020, pp. 15–19). It is important to note that Ma's wife travelled to Shanghai to deliver a laptop to Chinese intelligence, and Ma used to travel frequently to Hong Kong and China. Other open-source intelligence (OSINT) articles mentioned that he was "accused of stealing classified information and giving it to China in exchange for money, travel reimbursements and a set of golf clubs" (Boylan, 2023).

Furthermore, in addition to the official public statements and information concerning the examined case, it becomes evident that these sources are, in part, predicated upon the use of travel intelligence. This intelligence arises from the collation of data and information pertaining to Ma's travel patterns and operational methods (US Department of Justice, 2020, p. 15–19). His journeys to Asia, the intricacies of his travel arrangements, and the payment methods employed have plausibly contributed to the understanding of his associations with Chinese intelligence officers. It was also conceivable that his apprehension was linked to the implementation of specific watch-listing techniques as delineated in the documentation of American intelligence agencies, exemplifying a counterintelligence-oriented approach (US Department of Justice, 2020, pp. 15–19).

TRAVINT watch listing is a process where certain individuals are placed on watchlists to enhance security measures and prevent potential threats to national security. Subsequently, types of individuals or circumstances that might lead to watch listing may be as follows:

- *Known or suspected terrorists*: Individuals who have been identified as being involved in or having ties with terrorist organisations might be placed on TRAVINT watchlists to prevent them from travelling freely.
- *High-risk individuals*: Individuals who are deemed to pose a potential security risk, such as those with a history of violence or criminal activity, may be watch-listed to ensure enhanced scrutiny is given to their travel patterns.
- *Suspected or known spies*: Individuals suspected or known to be involved in espionage activities may be placed on travel watchlists to monitor their movements and prevent unauthorised access to sensitive locations or classified information.

Conclusion

In conclusion, counterintelligence theory is a dynamically evolving field that adapts to emerging threats, technological advancements, and shifts in geopolitical landscape (Prunckun, 2019). The evolving theories and practices within counterintelligence continually respond to new challenges and vulnerabilities. Given the increasingly complex intelligence and security environment, there is a growing imperative for functional interconnections between various security processes, such as border security.

This paper has approached the security and intelligence functions of counterintelligence and border security by examining and discussing their shared aspects, with a particular focus on TRAVINT. The paper has also highlighted the increasing demand for and importance of TRAVINT, emphasising its processes and tactical and operational co-approaches in conjunction with counterintelligence and border security.

From this perspective, TRAVINT emerges as an invaluable source of information, providing the legal, intelligence, and security enforcement sectors with necessary intelligence inputs to address national threats and risks. It is essential to highlight that the utilisation of PNR data should always occur in strict compliance with state legislation and with full respect for relevant human rights. Furthermore, it is evident that further academic and operational research is required to delve into the specific use of information and intelligence related to TRAVINT, with the aim of establishing a new sector within academic intelligence research.

Last but not least, the paper presents a visionary perspective on the future applications of TRAVINT, highlighting its crucial role in safeguarding global security. In an increasingly interconnected world, countries serving as international travel hubs, such as the Emirates (Dubai), the Netherlands (Amsterdam), Germany (Munich), the United Kingdom (London), and key African cities such as South Africa's Johannesburg and Cape Town, face burgeoning challenges in terms of counterintelligence and border security. As these pivotal transit points continue to attract an influx of travellers, the need for advanced intelligence operations to thwart potential threats has become paramount. The insights derived from this research have the potential to reshape international travel security strategies, making these global transit hubs safer, and reinforcing the broader global security ecosystem.

Funding

This research received no external funding.

Data Availability Statement

The data presented in this study is available on request from the author.

Disclosure statement

No potential conflict of interest was reported by the author. The author obtained copyright permission for the images published in the paper. The author read and agreed to the published version of the manuscript.

References

Barnea, A. (2019) 'Big data and counterintelligence in western countries', *International Journal of Intelligence and Counter Intelligence*, 32(3), pp. 433–447. doi: 10.1080/08850607.2019.1605804.

Bellanova, R. and Glouftsios, G. (2020) 'Controlling the Schengen information system (SIS II): The infrastructural politics of fragility and maintenance', *Geopolitics*, 27(1), pp. 160–184. doi: 10.1080/14650045.2020.1830765.

Boylan, P. (2023) 'Alleged spy for China to stand trial in 2024', *Star Advertiser*. Available at: https://www.staradvertiser.com/2023/02/17/hawaii-news/alleged-spy-for-china-to-stand-trial-in-2024/ (Accessed: 27 September 2023).

Cram, C. (1993) *Of moles and molehunters: A review of counterintelligence literature, 1977–92*. Book Monograph. Washington, DC: Center for the Study of Intelligence.

De Hert, P. and Papakonstantinou, V. (2010) 'The EU PNR framework decision proposal: towards completion of the PNR processing scene in Europe', *Computer Law and Security Review*, 26(4), pp. 368–376. doi: 10.1016/j.clsr.2010.05.008.

Ehrman, J. (2009) 'Toward a theory of CI', *Studies in Intelligence*, 53(2). Central Intelligence Agency. Available at: https://www.cia.gov/static/867934afc1db19abcfcc5ced4193b676/toward-a-theory-of-ci.pdf (Accessed: 27 September 2023).

European Commission (2023) *Passenger name record (PNR)*. Available at: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/passenger-data_en (Accessed: 19 October 2023).

European Parliament (2016) *Regulation establishing a European travel information and authorisation system (ETIAS) and amending regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0731 (Accessed: 9 November 2023).

European Union (2016) *EU directive 2016/681*.

European Union Agency for Law Enforcement Training (CEPOL) (2022) *Passenger name record (PNR) executive summary.* Available at: https://www.cepol.europa.eu/api/assets/Executive%20Summary%20PNR%20v2_with%20image.pdf (Accessed: 27 September 2023).

Fernández-Rojo, D. (2021) *EU migration agencies: The operation and cooperation of Frontex, EASO and Europol*. Cheltenham, UK: Edward Elgar.

Frizberg, D. (2023). *Advance passenger information (API): Revising the rules, European Parliament*. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)747429 (Accessed: 19 October 2023).

Frontex (2012a) *Common integrated risk analysis model a comprehensive update*. Warsaw: European Border and Coast Guard Agency.

Frontex (2012b) *Guidelines for risk analysis units: Structure and tools for the application of CIRAM version 2.0*. Warsaw: European Border and Coast Guard Agency.

Frontex (2013) *Border control in the information age*. Available at: https://frontex.europa.eu/media-centre/news/focus/border-control-in-the-information-age-udh57L (Accessed: 28 September 2023).

Frontex (2020) *Future group on travel intelligence and border management*. Available at: https://www.europol.europa.eu/publications-events/publications/future-group-travel-intelligence-and-border-management#downloads (Accessed: 28 September 2023).

Glouftsios, G. and Leese, M. (2022) 'Epistemic fusion: Passenger information units and the making of international security', *Review of International Studies*, 49(1), pp. 125–142. doi: 10.1017/s0260210522000365.

Hansen, F. and Pettersson, J. (2021) 'Contradictory migration management? Differentiated security approaches to visa overstay and irregular border crossings in the European Union', *European Security*, 31(1), pp. 117–134. doi: 10.1080/09662839.2021.1945038.

Jeandesboz, J. (2020) 'European border policing: EUROSUR, knowledge, calculation', *Global Crime*, 18(3), pp. 256–285. doi: 10.1080/17440572.2017.1347043.

Johnson, L.K. (2010) *Handbook of intelligence studies*. London: Routledge.

Léonard, S. (2010) 'EU border security and migration into the European Union: Frontex and securitisation through practices', *European Security*, 19(2), pp. 231–254. doi: 10.1080/09662839.2010.526937.

Liashuk, R. and Tsaruk, A. (2021) 'Experience of information and analytical activities in the field of border protection of the European Union', in *Proceedings of the International Conference on Economics, Law and Education Research* (ELER 2021), Series: *Advances in Economics, Business and Management Research*. Dordrecht, The Netherlands: Atlantis Press. doi: 10.2991/aebmr.k.210320.032.

Melendez, V.M. (2019) 'Counterintelligence: An asymmetric warfighting tool for the U.S. navy', *International Journal of Intelligence and CounterIntelligence*, 32(4), pp. 737–769. doi: 10.1080/08850607.2019.1621108.

Morral, A., Willis, H. and Brownell, P. (2011) *Measuring illegal border crossing between ports of entry*. Santa Monica, CA: RAND.

Namazov, R. (2022) *Application of advance passenger information (API) and passenger name record (PNR) security systems by using travel information*. State Customs Committee of Azerbaijan and Kanazawa University of Japan. Available at: https://www.border-security-report.com/wp-content/uploads/2022/07/API-PNR-Namazov-research.pdf (Accessed: 19 October 2023).

National Counterterrorism Center. (2013) *Watchlisting guidance*. Available at: https://www.eff.org/files/2014/07/24/2013-watchlist-guidance_1.pdf (Accessed: 27 September 2023).

Office of Public Affairs. (2022) *Former CIA officer arrested and charged with espionage*. Available at: https://www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage (Accessed: 23 October 2023).

Oliveira Martins, B., Lidén, K. and Jumbert, M.G. (2022) 'Border security and the digitalisation of sovereignty: Insights from EU borderwork', *European Security*, 31(3), pp. 475–494. doi: 10.1080/09662839.2022.2101884.

Priestley, A. and Beauvais, M. (2021) *International experience and good practices in API/PNR, OSCE*. Available at: https://www.osce.org/project-coordinator-in-ukraine/510575 (Accessed: 28 September 2023).

Priestley, A. and Beauvais, M. (2022) *International experience and good practices in API/PNR–Project coordinator in Ukraine*. Vienna: Organization for Security and Co-operation in Europe (OSCE).

Prunckun, H.W. (2019) *Counterintelligence theory and practice*. London: Rowman & Littlefield.

Richelson, J. (1986). *Sword and shield: The Soviet intelligence and security apparatus*. Philadelphia, PA: Ballinger.

Riehle, K. (2015) 'A counterintelligence analysis typology', *American Intelligence Journal*, 32(1), pp. 55–60. Available at: https://nationalmilitaryintelligence.app.box.com/v/ArchivesAIJ/file/226592331597 (Accessed: 9 November 2023).

Romanian Parliament. (2019) *IPEX|the platform for EU interparliamentary exchange*. Available at: https://secure.ipex.eu/IPEXL-WEB/download/file/082dbcc568e94e7e0168eba5046a0223. (Accessed: 9 November 2023).

Rudner, M. (2014) 'Intelligence-led air transport security: Pre-screening for watch-lists, no-fly lists to forestall terrorist threats', *International Journal of Intelligence and CounterIntelligence*, 28(1), pp. 38–63. doi: 10.1080/08850607.2014.962352.

Shepherd, A.J.K. (2022) 'EU counterterrorism, collective securitization, and the internal-external security nexus', *Global Affairs*, 7(5), pp. 733–749. doi: 10.1080/23340460.2021.2001958.

Shulsky, A.N. and Schmitt, G.J. (2009) *Silent warfare: Understanding the world of Intelligence*. Washington DC: Potomac Books.

Sims, J.E. and Gerber, B.L. (2005) *Transforming U.S. intelligence*. Washington, DC: Georgetown University Press.

Sims, J.E. and Gerber, B.L. (2009) *Vaults, mirrors, and masks: Rediscovering U.S. counterintelligence*. Washington, DC: Georgetown University Press.

Stouder, M.D. and Gallagher, S. (2013) 'Crafting operational counterintelligence strategy: A guide for managers', *International Journal of Intelligence and CounterIntelligence*, 26(3), pp. 583–596. doi: 10.1080/08850607.2013.780560.

US Department of Homeland Security and US Customs and Border Protection. (2013) *U.S. customs and border protection passenger name record (PNR) privacy policy*. Washington, DC: US Department of Homeland Security.

US Department of Homeland Security Privacy Office. (2015) *A report on the use and transfer of passenger name records between the European Union and the United States*. Washington DC: US Department of Homeland Security Privacy Office.

US Department of Homeland Security Privacy Office. (2017) *Privacy impact assessment update for the automated targeting system DHS/CBP/PIA-006(e)*. Washington DC: US Department of Homeland Security Privacy Office.

US Department of Justice. (2020) *Affidavit of FBI special agent Chris Jensen*. Available at: https://www.justice.gov/d9/press-releases/attachments/2020/08/17/download_ma_complaint_.pdf. (Accessed: 27 September 2023).

US Government Publishing Office. (2011) *Intelligence sharing and terrorist travel: How DHS addresses the mission of providing security, facilitating commerce, and protecting privacy for passengers engaged in international travel*. Available at: https://www.govinfo.gov/content/pkg/CHRG-112hhrg73736/html/CHRG-112hhrg73736.htm (Accessed: 27 September 2023).

Van Cleave, M.K. (2007) *Counterintelligence and national strategy*. Washington, DC: National Defense University (NDU) Press. doi: 10.21236/ada47148.

van Dongen, T. (2010) 'Mapping counterterrorism: A categorisation of policies and the promise of empirically based, systematic comparisons', *Critical Studies on Terrorism*, 3(2), pp. 227–241. doi: 10.1080/17539150903306170.

Wagner, J. (2021). *Border management in transformation: Transnational threats and security policies of European states*. New York City, NY: Springer.