(Online) ISSN 2744-1741
Defense and Security Studies *Review Article*
Vol. 5, No. 1, 2024, pp. 10-19
https://doi.org/10.37868/dss.v5.id261

Insider threat mitigation through human intelligence and counterintelligence: A case study in the shipping industry

Anastasios-Nikolaos Kanellopoulos [1*],
[1] Department of Business Administration, Athens University of Economics and Business, Greece

*Corresponding author E-mail: ankanell@aueb.gr

Received: Jan. 30, 2024.
Revised: Mar. 1, 2024.
Accepted: Mar. 2, 2024.
Online: Mar. 7, 2024.

Abstract

This paper comprehensively examines the multifaceted motivations behind insider threats within organizations, elucidating driving forces such as financial gain, revenge, personal aspirations, ideological beliefs, coercion, and negligence. Understanding this spectrum is fundamental for crafting effective Counterintelligence strategies. The study delves into behavioral indicators crucial for identifying potential threats, emphasizing the significance of recognizing warning signs like unusual data access, unsanctioned software usage, escalated privilege requests, poor performance, disagreement with policies, and more.

Furthermore, the role of Human Intelligence (HUMINT) in Counterintelligence (CI) and insider threat detection is explored, highlighting its qualitative contribution to understanding human behavior. Plus, through a hypothetical case study in the Shipping industry, the paper illustrates the direct application of HUMINT principles in fortifying security against insider threats, considering the unique challenges of this dynamic sector. The case study strategically employs employee interviews, psychological assessments, social network analysis, and trust-building initiatives to proactively identify and mitigate potential threats, in an industry reliant on seamless global supply chain operations.

Keywords: Insider Threats, Human Intelligence, Counterintelligence, Organizational Security Risk.

1. Introduction

In contemporary organizational landscapes, the phenomenon of insider threats poses a formidable challenge to security practitioners and scholars alike. The present study embarks on an inquiry into the nuanced motivations underlying individuals' proclivity towards insider threat behaviors within organizational contexts. With a specific focus on the dynamic domain of the shipping industry, our research endeavors to achieve multifaceted goals aimed at elucidating the intricacies of insider threats and fortifying organizational resilience against such risks.

Foremost among our objectives is a comprehensive examination of insider threats within organizations, underpinned by an understanding of the unique challenges and operational dynamics prevalent in the shipping sector. This entails a meticulous dissection of the diverse motivations driving insider threats, encompassing a spectrum ranging from pecuniary interests to psychological predispositions, ideological affiliations, and instances of coercion or negligence. By delving into this multifaceted landscape of motivations, the paper

aims to provide a nuanced understanding that can inform the development of targeted Counterintelligence (CI) strategies capable of addressing the diverse array of human behaviors conducive to insider threats.

In addition to illuminating the underlying motivations, our study seeks to identify and elucidate behavioral indicators crucial for the detection and mitigation of potential insider threats. Recognizing that individual behaviors, while not invariably indicative of malicious intent, often serve as early warning signs, the paper endeavors to delineate common behavioral patterns indicative of insider threat activities. These may include anomalous data access patterns, unauthorized usage of software or systems, aberrant work practices, or unexplained alterations in behavior or lifestyle. By scrutinizing these behavioral cues, organizations can proactively bolster their defense mechanisms against insider threats and preemptively mitigate associated risks.

Moreover, the central aim is the acknowledgment of Human Intelligence (HUMINT) as a cornerstone in CI operations, particularly in the realm of insider threat detection. HUMINT, with its unique capacity to decipher the complexities of human behavior, motivations, and intentions, emerges as an indispensable asset in organizational security efforts. By supplementing technological solutions with qualitative insights gleaned through HUMINT methodologies, organizations can gain a holistic understanding of the human factor in security operations and thereby enhance their resilience against insider threats.

Lastly, to illustrate the practical application of the paper’s theoretical insights, it presents a hypothetical case study centered on a shipping company operating within the global supply chain milieu. Through this illustrative scenario, it demonstrates the strategic integration of HUMINT principles in fortifying the company's security posture against insider threats. Techniques such as employee interviews, psychological assessments, social network analysis, and trust-building initiatives are deployed synergistically to proactively identify and mitigate potential insider threats. By contextualizing its theoretical framework within a real-world scenario, it aims to provide tangible exemplars that underscore the practical relevance and applicability of its research findings.

In sum, the study endeavors to offer a comprehensive and academically rigorous exploration of insider threats, HUMINT, and CI operations within the context of the shipping industry. By illuminating the intricacies of motivations, delineating behavioral indicators, emphasizing the role of HUMINT, and providing practical insights through a hypothetical case study, it aspires to contribute meaningfully to the scholarly discourse and practical endeavors aimed at safeguarding organizations against the perils of insider threats.

2. Research method

The research methodology employed in this study is a comprehensive review of information, aiming to provide an in-depth exploration of the extensive literature surrounding insider threats, HUMINT, and CI. Recognizing the multifaceted nature of these topics, our approach involves synthesizing a diverse array of source materials, including academic studies, government reports, policy documents, and media sources.

This inclusive strategy is essential for cultivating a holistic comprehension of the intricate subject matter, offering a nuanced perspective on the motivations, behavioral indicators, and CI measures related to insider threats. By drawing upon a wide spectrum of scholarly and practical insights, this review aspires to contribute to a deeper understanding of the complex interplay between human factors and organizational security.

Additionally, the research methodology encompasses a hypothetical case study focused on the Shipping industry, delving into its unique challenges and potential applications for insider threat detection. Through the examination of real-world scenarios and industry-specific nuances, the case study serves to contextualize theoretical concepts within the practical realm, enhancing the relevance and applicability of the study's findings.

2.1 Insider threats: motivations and behavioral indicators

2.1.1 Insider threats motivations

The motivations underlying individuals becoming insider threats are nuanced and shaped by a confluence of personal, situational, and organizational factors. Delving into the multifaceted nature of these motivations reveals a spectrum of driving forces, each contributing to the complexity of insider threats. Specifically, the common motivations for becoming an insider threat are the following:

- Financial gain emerges as a predominant motivation, compelling individuals to exploit their access to sensitive information, systems, or resources for personal profit. In pursuit of financial motives, insiders may clandestinely steal or sell valuable data, trade secrets, or intellectual property. The allure of financial gain poses a significant risk, particularly in industries where proprietary information holds substantial market value [6].
- Revenge or resentment represents another compelling motivation, particularly among disgruntled employees who perceive mistreatment, neglect, or injustice within their organizational milieu. Seeking retaliation, these individuals may engage in malicious activities such as sabotaging systems, leaking confidential information, or deliberately disrupting operational processes. The emotional underpinnings of revenge or resentment can manifest as potent catalysts for insider threats, necessitating a comprehensive approach to employee well-being and conflict resolution [11].
- Personal gain, beyond mere financial considerations, propels some insiders to engage in malicious activities for self-benefit. This may include actions geared toward gaining a competitive advantage, advancing one's career within the organization, or seeking recognition and power. The pursuit of personal gain introduces an additional layer of complexity to insider threats, demanding a nuanced understanding of individual aspirations and ambitions [6].
- Ideological or political beliefs emerge as motivating factors, driving insiders to promote a cause or advance a particular agenda within their organizational context. This may involve leaking sensitive information, disrupting operations, or engaging in activist endeavors aligned with deeply held convictions [6]. The intertwining of personal ideologies with organizational dynamics underscores the importance of considering ideological motivations in the identification and mitigation of insider threats [11].
- Coercion or blackmail introduces a dimension of external influence, as insiders may be compelled into becoming threats through threats to their personal safety, reputation, or financial well-being. The vulnerability of individuals facing external pressures underscores the need for robust CI efforts aimed at identifying signs of coercion and intervening before insiders unwittingly become instruments of external manipulation [3].
- Negligence or carelessness represents a distinct, albeit unintentional, motivation for insider threats. In certain instances, individuals may breach security protocols, mishandle sensitive information, or inadvertently cause damage to systems or data due to negligence or carelessness. Recognizing that not all insider threats are driven by malicious intent is crucial for devising strategies that encompass both intentional and unintentional security breaches [25].

Eventually, understanding the diverse motivations behind insider threats is imperative for developing comprehensive and effective CI strategies [21]. Financial gain, revenge, personal aspirations, ideological beliefs, coercion, and negligence collectively contribute to the intricate landscape of insider threats. Organizations must adopt a multifaceted approach that addresses these motivations through a combination of preventive measures, employee support programs, and a robust security infrastructure to mitigate the risks associated with insider threats [25].

2.1.2 Insider threats behavioral indicators

Behavioral indicators serve as crucial elements in identifying potential insider threats within an organization, offering valuable insights into activities that may deviate from established norms. While individual behaviors are not unequivocal evidence of malicious intent, they can serve as warning signs necessitating further investigation [20]. The following elucidates some common behavioral indicators that may suggest insider threat activity:

- Unusual Data Access or Movement: Employees accessing or moving substantial volumes of data beyond the scope of their job responsibilities or normal patterns can raise suspicion [15]. An abrupt departure from established data usage patterns may signify potential unauthorized activities, necessitating a closer examination of the employee's actions [7].
- Use of Unsanctioned Software and Hardware: The use of unauthorized or unapproved software, applications, or hardware by employees can indicate attempts to circumvent security measures or conceal malicious activities [27]. Monitoring for such deviations from sanctioned tools becomes imperative for maintaining the integrity of the organization's security infrastructure [9].
- Increased Requests for Escalated Privileges: Frequent or abrupt requests for elevated access privileges, exceeding what is essential for an employee's role, may point to an effort to gain unauthorized access to sensitive information or systems. Organizations should scrutinize such requests to ensure they align with legitimate job responsibilities [27].
- Poor Performance or Disgruntlement: A decline in job performance, recurring conflicts with colleagues or supervisors, or expressions of dissatisfaction with the organization can be indicators of potential insider threats. Monitoring employee satisfaction and promptly addressing workplace concerns can mitigate the risk associated with disgruntled individuals [20].
- Voicing Disagreement with Policies: Consistent vocal disagreement with organizational policies, procedures, or security measures may suggest an increased likelihood of engaging in malicious activities. Organizations should foster open communication channels to address concerns constructively and minimize the potential for dissent to turn into insider threats [6].
- Working Outside Normal Hours or Accessing Systems Off-Hours: Employees consistently working late or accessing systems during non-business hours without a legitimate reason may raise suspicions of unauthorized activities. Monitoring access logs and establishing clear protocols for after-hours system usage can aid in identifying potential insider threats [20].
- Attempts to Bypass Security Measures: Deliberate efforts to bypass security controls, such as disabling security software or circumventing access controls, can indicate malicious intent [15]. Regular security audits and monitoring of system logs are essential for detecting and mitigating insider threats attempting to compromise security measures [6].
- Unusual Financial Transactions: Employees involved in suspicious financial activities, such as unauthorized financial transfers, unusual cash flow, or unexplained financial gains, may be engaging in insider threats for financial gain. Organizations should closely monitor financial transactions and implement robust controls to detect and prevent such activities [9].
- Changes in Behavior or Lifestyle: Sudden changes in an employee's behavior, lifestyle, or financial situation, such as excessive gambling, substance abuse, or financial difficulties, can be indicators of potential insider threats. Early intervention, through employee assistance programs and counseling, can address underlying issues and mitigate the risk of such behavioral changes leading to security breaches [9].

In short, recognizing and interpreting behavioral indicators is integral to the proactive identification and mitigation of insider threats. Organizations must implement comprehensive monitoring mechanisms, coupled with clear protocols for responding to potential indicators, to safeguard against the diverse array of behaviors that may signify malicious intent.

2.2 The role of human intelligence in counterintelligence

HUMINT is a cornerstone in the field of intelligence gathering, encompassing a multifaceted approach to collecting, analyzing, and interpreting information derived from interpersonal interactions [22]. At its core, HUMINT relies on human sources—spies, informants, and operatives—who engage in direct communication with individuals to extract valuable insights [18].

Unlike other forms of intelligence, such as signals or imagery intelligence, HUMINT is uniquely positioned to decipher the complexities of human behavior, motivations, and intentions [3]. In the realm of CI, where the focus is on identifying and mitigating insider threats, HUMINT emerges as a critical component [1], [24]. Understanding the human element behind potential security risks is paramount, and HUMINT provides the nuanced context necessary for effective decision-making [12]. Through interviews, debriefings, and other interpersonal methods, HUMINT specialists can gather information on individuals' backgrounds, affiliations, and potential vulnerabilities to coercion or manipulation [11], [24]. This depth of understanding enables CI professionals to proactively identify and neutralize insider threats before they materialize [1]. HUMINT's emphasis on the human element complements technological solutions by adding a qualitative layer to the intelligence spectrum, offering insights that algorithms and automated systems may struggle to discern [3].

The value of HUMINT in CI lies not only in its ability to uncover information but also in its capacity to contextualize data within the intricate tapestry of human behavior [1]. By tapping into the rich tapestry of interpersonal connections, motivations, and loyalties, HUMINT contributes to a comprehensive understanding of the human landscape within an organization, enhancing the capacity to identify and mitigate insider threats effectively [22]. As technology continues to evolve, HUMINT remains an indispensable tool in the intelligence toolkit, providing a human touch to the often intricate and subtle dynamics of CI operations [8].

3. Results and Discussion

3.1 Insider threats identification through HUMINT

HUMINT sources constitute a rich tapestry of methods that delve into the intricate realms of human behavior, motivations, and intentions, offering invaluable insights for organizations aiming to identify and counter potential insider threats before they materialize [18].

Employee interviews represent a cornerstone in the HUMINT toolkit, offering a direct and personalized approach to gathering critical information. Skilled interviewers play a pivotal role in navigating the intricacies of human interaction, employing a combination of empathy, intuition, and expertise to elicit valuable insights [11]. These interviews transcend superficial observations, allowing interviewers to delve deep into the layers of an individual's behavior, motivations, and intentions. By establishing rapport and trust, interviewers create an environment conducive to open communication, encouraging employees to share candid responses that may unveil subtle nuances in their demeanor or provide glimpses into their mindset [16]. The richness of employee interviews lies in their ability to explore beyond the immediate context, uncovering the individual's unique experiences, perspectives, and potential grievances. This holistic approach aids in constructing a comprehensive profile, shedding light on aspects that automated systems or technological solutions might overlook [11]. Understanding an employee's mindset is crucial for anticipating their reactions to various stimuli, identifying potential stressors, and assessing their susceptibility to external influences. Furthermore, employee interviews contribute to a proactive approach to recognizing any signs of dissatisfaction or potential alignment with insider threat indicators [4]. Organizations that embrace employee interviews as a core component of their HUMINT strategy demonstrate a commitment to understanding the human element within their workforce [21]. This method not only serves as an early warning system for potential insider threats but also fosters a culture of transparency, where employees feel heard and valued. In an era where the human factor remains pivotal in organizational security, the nuanced insights gleaned from employee interviews

empower decision-makers to make informed choices, thereby enhancing the overall resilience of an organization against emerging threats [2].

Besides, psychological assessments, as a potent source within HUMINT, introduce a layer of scientific precision to the evaluation process, offering organizations a sophisticated means of understanding an individual's psychological makeup. Employing a range of standardized tests, personality assessments, and behavioral analyses, organizations can delve into the intricacies of an individual's psyche. These assessments are designed to unveil aspects of personality, emotional well-being, and cognitive processes, providing a more profound understanding of an individual's behavioral patterns. By examining responses to specific stimuli and gauging reactions in controlled environments, organizations can identify predispositions, emotional triggers, and potential stressors that might influence an individual's decision-making process [11]. The ability to recognize indicators of stress, discontent, or susceptibility to external pressures is crucial for conducting a comprehensive risk assessment, especially in the context of insider threat detection [4]. Psychological assessments contribute to a proactive approach by uncovering potential vulnerabilities or areas of concern that may not be immediately evident through traditional means [7]. Insights garnered from these assessments enable organizations to tailor intervention strategies, implement targeted support mechanisms, and foster a healthier work environment [21]. By combining the empirical rigor of psychological assessments with other HUMINT methods, organizations can construct a multidimensional profile of individuals, enhancing their ability to detect, mitigate, and prevent insider threats. This holistic approach, leveraging both the subjective and objective dimensions of human behavior, underscores the significance of psychological assessments in fortifying an organization's security posture against evolving threats in an increasingly complex and interconnected world.

Additionally, social network analysis stands as a powerful augmentation to the HUMINT toolkit, offering a sophisticated means of unraveling the intricate web of relationships, affiliations, and communication patterns within an organization [1]. This method involves scrutinizing connections between individuals, allowing analysts to discern not only the formal organizational structure but also the informal networks that underpin it [11]. By mapping the interplay of relationships, analysts can identify potential influencers, individuals with an outsized impact on decision-making or group dynamics [5]. Moreover, social network analysis enables the identification of isolated or disgruntled employees, those on the fringes of the social fabric whose sentiments may harbor risks to organizational cohesion and security [7]. Further, this method allows organizations to gauge the strength of allegiances, unveiling the depth and nature of connections between employees. Understanding the social dynamics within an organization becomes pivotal in identifying potential insider threats [17]. Patterns such as sudden changes in alliances, unusual collaborations, or the emergence of cliques may signify shifts in employee loyalties that merit closer scrutiny [11]. By visualizing the human landscape through social network analysis, organizations gain the ability to identify potential insider threats early in their gestation, providing a proactive approach to security [1]. The power of social network analysis lies in its capacity to offer a comprehensive, visual representation of the human relationships that shape an organization. This method goes beyond individual assessments and unveils the collective dynamics that influence behavior and decision-making. By integrating social network analysis with other HUMINT methodologies, organizations can develop a holistic understanding of their workforce, enhancing their ability to detect and mitigate potential insider threats before they materialize [11]. In the ever-evolving landscape of organizational security, this multifaceted approach positions social network analysis as a vital tool for identifying and navigating the complexities of insider threats [5].

In due course, combining these HUMINT sources and technique approaches empowers organizations to construct a nuanced profile of individuals, allowing for a more informed assessment of the risk they may pose as potential insider threats. By integrating these diverse methods, organizations can proactively identify anomalies, behavioral deviations, or signs of discontent that might otherwise go unnoticed. This proactive approach positions HUMINT as a key ally in the ongoing battle against insider threats, providing decision-

makers with the tools to intervene before potential risks escalate [4]. As technological advancements continue to reshape the landscape of security, the human touch afforded by HUMINT remains indispensable, offering a complementary perspective that augments the capabilities of automated systems and algorithms. The synergy of employee interviews, psychological assessments, and social network analysis creates a robust framework for understanding the complex interplay of human factors within organizations [1]. In a rapidly evolving threat landscape, organizations that harness the power of HUMINT sources are better equipped to identify, mitigate, and prevent insider threats, safeguarding their assets, reputation, and overall security posture.

3.2 Building trust, relationships, and counterintelligence culture

Building trust, fostering positive relationships, and cultivating a robust CI culture are imperative components for the effective implementation of HUMINT within an organization or business [1]. At the core of HUMINT lies the fundamental necessity for reliable information gleaned through interpersonal interactions, where trust serves as the linchpin in this intricate process [2].

Establishing trust commences with the creation of an organizational culture that places a premium on transparency, fairness, and open communication [14]. This foundational framework is pivotal in instilling confidence among employees, assuring them that their concerns and observations will be handled with the utmost seriousness and without any fear of repercussion [8]. A significant deterrent to the reporting of suspicious behavior is the apprehension of retaliation, underscoring the critical need for organizations to actively cultivate an environment where individuals feel safe to come forward with potentially vital information [14]. Leadership plays a central role in this endeavor, with its approachability, empathy, and responsiveness setting the tone for an organizational culture that places a high value on the human element [2], [19].

In addition, leadership commitment to listening, understanding, and addressing employee concerns is integral to creating an atmosphere conducive to trust. By demonstrating empathy and responsiveness, leaders not only foster positive relationships but also lay the groundwork for a culture that prioritizes the well-being and contributions of its workforce [2]. This approach extends beyond mere rhetoric; tangible actions must accompany these principles to fortify the trust-building process.

Furthermore, implementing anonymous reporting channels and whistleblower protection programs further solidifies the commitment to creating a secure environment for reporting. These initiatives empower employees to share information without fear of reprisal, thus facilitating early detection and intervention in potential security threats. Such mechanisms serve as essential safeguards, allowing individuals to contribute valuable insights without compromising their well-being.

In essence, trust and positive relationships constitute the bedrock upon which HUMINT thrives. The seamless flow of valuable information, unencumbered by fears of retribution or mistrust, is foundational to the success of HUMINT strategies [21]. As technological advancements continue to reshape the security landscape, the enduring significance of the human factor becomes increasingly evident. The unique ability of individuals to discern, interpret, and contribute information remains irreplaceable, underscoring the indispensable role of trust-building and positive relationships in bolstering the effectiveness of HUMINT within the broader framework of organizational security.

Moreover, a robust CI culture must permeate the entire organization, fostering a collective commitment to vigilance and security [2]. This culture encompasses not only leadership initiatives but also the active participation of every individual within the organization [8]. Security awareness programs, regular training sessions, and clear communication of security policies contribute to instilling a sense of responsibility and ownership regarding CI measures [21]. Plus, a resilient CI culture involves continuous assessments of potential vulnerabilities, adapting strategies to evolving threats, and integrating CI into daily operations seamlessly [8]. Encouraging employees to stay informed about security best practices, promoting a sense of

collective responsibility for organizational security, and fostering a proactive mindset are essential components of this culture [2].

3.3 Case study on shipping industry

In a hypothetical case study of a Shipping company, the principles of HUMINT are directly applicable in fortifying the company's security posture against potential insider threats. The intricacies of the Shipping industry, which depend heavily on the timely and secure movement of goods across borders, underscore the imperative for safeguarding operations, sensitive information, and reputation [13], [23]. The operation of a Shipping company implies the need for a comprehensive security strategy that integrates HUMINT methodologies to address the unique challenges inherent in the industry [10], [26].

The initial step involves the implementation of employee interviews as a pivotal HUMINT strategy [21]. Trained interviewers engage personnel at various hierarchical levels within the organization, aiming to unveil subtle nuances in behavior that may indicate signs of discontent, stress, or anomalous activities. By conducting targeted interviews with key personnel responsible for logistics, information technology, and security, the Shipping company can acquire a nuanced understanding of potential vulnerabilities that may be exploited by insider threats.

Then, psychological assessments assume a critical role in this context, offering a systematic and empirical approach to evaluating the psychological well-being of employees, particularly those occupying critical roles within the organization. Subjecting individuals to standardized tests and behavioral analyses enables the Shipping company to gain insights into predispositions, emotional triggers, and potential areas of concern. For instance, employees tasked with handling sensitive cargo or managing vital communication systems may undergo assessments to ensure their psychological resilience against external pressures or coercive influences, thereby fortifying the organization against potential insider threats.

Furthermore, Social network analysis emerges as an indispensable tool for navigating the complex interpersonal relationships within the organization [1]. By mapping connections between employees, the Shipping company can identify influencers, detect isolated or disgruntled individuals, and gauge the strength of allegiances within the workforce. This method assumes particular relevance in an industry where collaboration and communication are paramount, and the dynamics of interpersonal relationships can significantly impact operational efficiency. Analyzing the social fabric of the company, through a HUMINT lens allows the Shipping company to proactively identify potential insider threats based on social dynamics and relationships.

Over and above the previous, in an industry like Shipping, where the potential for insider threats to compromise the security of cargo or sensitive information is a significant concern, initiatives centered around trust-building take center stage [10]. Establishing an organizational culture that encourages open communication, values transparency, and actively supports whistleblower protection is paramount [2]. Leadership within the Shipping company must foster an environment where employees feel safe reporting suspicious behavior without fear of retaliation. The implementation of anonymous reporting channels ensures that employees can share vital information about potential threats without compromising their own safety or job security.

4. Conclusions

In conclusion, this paper presents a comprehensive exploration of insider threats, HUMINT, and CI, with a focus on motivations, behavioral indicators, and the role of HUMINT in organizational security. The multifaceted motivations behind insider threats, including financial gain, revenge, personal aspirations, ideological beliefs, coercion, and negligence, underscore the complex landscape organizations must navigate. Recognizing these motivations is vital for developing effective CI strategies that address diverse arrays of

human behavior. Behavioral indicators, such as unusual data access and changes in behavior, serve as crucial warning signs for potential threats, necessitating proactive identification measures.

In due course, the pivotal role of HUMINT in CI operations is emphasized, highlighting its unique ability to decipher human complexities. HUMINT provides a qualitative layer that complements technological solutions, ensuring a holistic understanding of the human factor in security. Finally, the hypothetical case study on a Shipping company further illustrates the direct applicability of HUMINT principles, showcasing the strategic integration of employee interviews, psychological assessments, social network analysis, and trust-building initiatives to fortify security against insider threats in the dynamic Shipping industry.

Declaration of competing interest

The author declares that has no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] A. N. Kanellopoulos, "The Dimensions of Counterintelligence and Their Role in National Security", *Journal of European and American Intelligence Studies*, vol. 6, no. 2, 2023.

[2] A. N. Kanellopoulos, "The Importance of Counterintelligence Culture in State Security", *Global Security and Intelligence Note*, vol. 1, no. 5, 2022.

[3] A.N. Shulsky, and G.J. Schmitt, Silent Warfare: Understanding the world of Intelligence. Washington: Potomac Books, Inc., 2009.

[4] A. Barnea and A. Meshulach, "Forecasting for Intelligence Analysis: Scenarios to abort strategic surprise", *International Journal of Intelligence and Counterintelligence*, vol. 34, no. 1, pp. 106-133, 2020.

[5] A. Barnea, "Big Data and Counterintelligence in Western countries", *International Journal of Intelligence and Counterintelligence*, vol. 32, no. 3, pp. 433-447, 2019.

[6] B. Champion, "Spies (Look) Like Us: The Early Use of Business and Civilian Covers in Covert Operations", *International Journal of Intelligence and Counterintelligence,* vol. 21, no. 3, pp. 530-64, 2008.

[7] I. Cho and L. Kyungho, "Advanced Risk Measurement Approach to Insider Threats in Cyberspace", *Intelligent Automation & Soft Computing*, vol. 22, no. 3, pp. 405-13, 2016.

[8] F.L. Wettering, "Counterintelligence: The broken triad", *International Journal of Intelligence and Counterintelligence*, vol. 13, no.3, pp. 265-300, 2000.

[9] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting insider threat via a cyber-security culture framework", *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 706-716, 2021.

[10] N P. Petersson, S. Tenold, and N. J. White, Shipping and Globalization in the Post-War Era, Palgrave Studies in Maritime Economics, 2019.

[11] H.W. Prunckun, Counterintelligence theory and practice, London: Rowman et Littlefield, 2019.

[12] J. Ehram, "Toward a Theory of CI", *Studies in Intelligence*, vol. 53, no. 2, 2009.

[13] J. Harber, "Unconventional Spies: The Counterintelligence Threat from Non-State Actors", *International Journal of Intelligence and Counterintelligence*, vol. 22, no. 2, pp. 221-36, 2009.

[14] J. E. Sims and B. L. Gerber, Vaults, mirrors, and masks: Rediscovering U.S. counterintelligence, Washington, D.C.: Georgetown University Press, 2009.

[15] K. Dempsey, V. Yan Pillitteri, and A. Regenscheid, "Managing the Security of Information Exchanges" Publication 800-47, *National Institute of Standards and Technology - U.S. Department of Commerce*, 2021.

[16] K. Riehle, "A Counterintelligence Analysis Typology", *American Intelligence Journal*, vol. 32l, no. 1, 2015.
[17] K. Spielmann, "Strengthening intelligence threat analysis", *International Journal of Intelligence and Counterintelligence*, vol. 25, no. 1, pp. 19-43, 2012.
[18] L.K. Johnson, Handbook of Intelligence Studies, London: Routledge, 2010.
[19] M. Lowenthal, Intelligence: From secrets to policy. Washington, DC: CQ Press, 2009.
[20] M. Rudner, "Protecting Critical Energy Infrastructure through Intelligence", *International Journal of Intelligence and Counterintelligence*, vol. 21, no. 4, pp. 635-60, 2008.
[21] M. D. Stouder and S. Gallagher, "Crafting Operational Counterintelligence Strategy: A guide for managers", *International Journal of Intelligence and Counterintelligence*, vol. 26, no. 3, pp. 583-596, 2013.
[22] A. C. Magee, "Countering Nontraditional HUMINT Collection Threats", *International Journal of Intelligence and Counterintelligence*, vol. 23, no. 3, pp. 509-20, 2010.
[23] N. Giannakopoulou, E. I. Thalassinos, and T. V. Stamatopoulos, "Corporate governance in shipping: an overview", *Maritime Policy & Management*, vol. 43 no. 1, 2016.
[24] Of moles and molehunters: A review of Counterintelligence Literature, 1977-92. Center for the Study of Intelligence, 1993.
[25] R. M. Clark and W. L. Mitchell, Deception: Counterdeception and Counterintelligence, Washington, DC: CQ Press, 2019.
[26] T. Grammenos, The Handbook of Maritime Economics and Business. Lloyd's List, 2010.
[27] The National Infrastructure Advisory Council, The Insider Threat to Critical Infrastructures, 2008.