BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Counterintelligence Risks in Crew Management and Recruitment: The Role of Profiling and Screening in Shipping Companies

Anastasios–Nikolaos KANELLOPOULOS, Ph.D. Candidate*

*Athens University of Economics and Business
e-mail: ankanell@aueb.gr

Abstract

This paper examines the critical role of profiling screening in countering security threats within the maritime industry, focusing on crew management and recruitment processes. In light of the industry's susceptibility to espionage, terrorism, and sabotage, effective counterintelligence measures are imperative. By scrutinizing the vulnerabilities and best practices associated with profiling screening, shipping companies can fortify their security defenses, mitigate insider threats, and ensure the safety of their assets and personnel.

Keywords:

Counterintelligence; shipping companies; Shipping Crew Management; Profiling; Screening.

Article info
Received: 8 April 2024; Revised: 7 May 2024; Accepted: 3 June 2024; Available online: 5 July 2024

Citation: Kanellopoulos, A.N. 2024. "Counterintelligence Risks in Crew Management and Recruitment: The Role of Profiling and Screening in Shipping Companies. *Bulletin of "Carol I" National Defence University*, 13(2): 44-59. https://doi.org/10.53477/2284-9378-24-19

This research embarks on a comprehensive literature review to explore the effectiveness and suitability of Counterintelligence (CI) profiling and screening processes within the realm of shipping companies. The primary objective of this study is to delve into various methodologies and best practices, aiming to assess their potential applicability within the unique operational landscape of shipping companies. CI processes serve as crucial components of security frameworks, especially in industries where there is a substantial risk of compromising sensitive information and assets. This significance is particularly pronounced in the maritime sector, characterized by its dynamic and often hazardous operating environment. Given the nature of maritime operations, which involve the transportation of valuable goods across international waters, the implementation of robust CI measures becomes imperative to safeguard the integrity and security of shipping operations. Consequently, this research seeks to scrutinize existing literature to identify key strategies, challenges, and best practices associated with CI profiling and screening, focusing specifically on their relevance and effectiveness within the maritime domain. By examining scholarly works and practical case studies, this study aims to offer valuable insights and recommendations to inform decision-making processes within shipping companies regarding the adoption and implementation of CI profiling and screening procedures. In doing so, this research endeavors to contribute to the enhancement of security protocols within the maritime industry, thereby ensuring the protection of vital assets and the mitigation of potential security risks.

General Crew Management and Recruitment Risks

Crew management within the realm of shipping companies entails the holistic supervision of seafarers across the entirety of their employment trajectory, spanning from initial recruitment to eventual retirement. This multifaceted endeavor involves the comprehensive administration of various facets of seafarers' employment, including but not limited to recruitment procedures, training initiatives, scheduling arrangements, welfare provisions, performance evaluations, and career advancement opportunities (Caesar and Fei 2018). Central to the mandate of shipping companies is the assurance that seafarers possess requisite qualifications, certifications, and competencies essential for the safe and proficient execution of their duties aboard vessels (Grammenos 2010). Furthermore, shipping companies shoulder the responsibility of addressing the distinctive exigencies and adversities encountered by seafarers, such as protracted periods of separation from familial environments, isolation, and exposure to potentially perilous working conditions (Auster and Choo 1994; Grammenos 2010; Giannakopoulou, Thalassinos and Stamatopoulos 2016).

Recruitment Risks: Recruitment risks within the maritime sector present formidable obstacles for shipping companies in their quest to identify and recruit qualified seafaring personnel. Among these challenges, one of the most prominent is the restricted availability of suitably qualified candidates for specific roles, stemming from

a confluence of factors including demographic shifts, skill scarcities, and evolving job specifications (Caesar and Fei 2018). Furthermore, the endeavor to entice proficient seafarers is compounded by heightened competition from alternative industries that offer enticing incentives and promising career pathways. Complicating matters further, inadequate recruitment channels exacerbate the situation, as shipping enterprises may encounter difficulties in effectively reaching potential candidates. Additionally, the constrained access to diverse talent pools inhibits endeavors to assemble inclusive and adaptable crews capable of fulfilling the multifaceted demands of the maritime sector. Another significant risk lies in the accuracy and completeness of the information furnished by candidates during the sourcing phase. Erroneous or incomplete data may lead to incongruities between job prerequisites and candidate proficiencies, ultimately impinging upon the caliber of hires and the overarching efficacy of crew management initiatives. Mitigating these recruitment risks necessitates the implementation of proactive strategies by shipping companies, including the diversification of recruitment channels, the augmentation of outreach endeavors, the refinement of candidate screening mechanisms, and the allocation of resources toward talent development programs. These measures are indispensable for facilitating the effective attraction, retention, and integration of proficient seafaring personnel within shipping enterprises (Barnea and Meshulach 2020).

Training and Familiarization Risks: Training and familiarization risks represent pivotal concerns within the maritime industry, exerting profound implications on the safety, efficacy, and proficiency of crew operations conducted aboard vessels. Among these risks, a noteworthy challenge arises from the provision of inadequate training and preparation for newly recruited crew members, a deficiency often attributed to constraints such as time limitations, resource constraints, or deficiencies in training curricula. Such inadequacies may render recruits ill-prepared to navigate the demands inherent to their roles, thereby compromising their safety and impeding the collective performance of the crew. Additionally, the dearth of familiarity with vessel-specific procedures and equipment poses further obstacles, potentially impeding crew members' adeptness in maneuvering onboard systems and adhering to established protocols (Estay 2020). Furthermore, deficient knowledge regarding safety protocols and emergency response procedures exacerbates these risks, potentially undermining the crew's capacity to effectively address emergent or perilous scenarios. Another salient concern pertains to the crew's challenges in assimilating novel technologies or systems onboard, which may encumber operational efficiency and productivity. Finally, deficient communication and coordination amongst crew members pose consequential risks, engendering instances of miscommunication, errors, and operational inefficiencies. To mitigate these training and familiarization risks, shipping companies must accord precedence to comprehensive training initiatives, allocate resources towards advanced simulation and training infrastructures, cultivate a culture of safety and perpetual learning, and foster effective communication and collaboration amongst crew members (Georgiadou, Mouzakitis and Askounis 2021). Through proactive

risk management endeavors, shipping companies can enhance crew preparedness, alleviate operational disruptions, and uphold unwavering standards of safety and operational excellence aboard their vessels (Cho and Lee 2016).

Retention Targets Risks: Retention targets risks in the maritime industry present notable obstacles for shipping companies, impeding their capacity to retain competent and seasoned seafarers. A primary concern lies in the challenge of meeting retention objectives due to substandard working conditions experienced onboard vessels. Factors such as prolonged periods away from home, demanding work environments, and limited access to amenities contribute to seafarer discontentment and heightened turnover rates. Furthermore, the dearth of opportunities for career advancement and progression pathways poses a substantial risk, compelling seafarers to seek employment elsewhere in pursuit of professional growth and personal development. Inadequate acknowledgment and rewards for high-performing seafarers exacerbate the retention predicament, fostering sentiments of undervaluation and unappreciation among crew members. Moreover, deficient feedback mechanisms and performance evaluation systems impede the company's ability to preemptively identify and rectify issues, engendering diminished morale and motivation within the crew. A notable risk factor pertains to the imbalance between work and personal life, with prolonged durations at sea exacting tolls on seafarers' mental and physical well-being, precipitating burnout and dwindling job satisfaction levels. To mitigate retention target risks, shipping companies must accord primacy to seafarer welfare, furnish competitive remuneration and benefits schemes, offer avenues for professional advancement and skill enrichment, institute robust performance assessment frameworks, and advocate for a harmonious work-life equilibrium. Through these concerted efforts, companies can ameliorate seafarer retention rates, bolster crew morale and efficiency, and fortify the enduring prosperity and viability of their endeavors (Cho and Lee 2016).

Counterintelligence Risks

The intersection of CI risks with the overarching complexities inherent in crew management and recruitment exacerbates the intricacies of security challenges encountered by shipping companies (Grammenos 2010; Cho and Lee 2016). This amalgamation encompasses a spectrum of threats stemming from state-sponsored espionage, activities of non-state actors, and the potential of insider threats, thereby presenting formidable hurdles to the organization's security infrastructure (Greene 1966; Wettering 2000; Johnson 2010; Alcaide and Llave 2020). Effectively addressing these risks necessitates a holistic comprehension of the landscape coupled with strategic mitigation measures, which take into account factors such as the constrained availability of suitable candidates, deficiencies in training protocols, obstacles in retention initiatives, and vulnerabilities within recruitment channels (Johnson 2010; Duvenage and Solms 2014; Caesar and Fei 2018; Kanellopoulos 2023).

By acknowledging the interconnected nature of these risks, shipping companies can bolster their defensive mechanisms, thereby safeguarding the integrity of their operations and assets (Catrantzos 2023).

State and Non-State Actor Threats

State-sponsored espionage poses a significant and tangible threat to the maritime industry, as evidenced by numerous real-life incidents. For example, the "Cloud Hopper" operation, attributed to China's Ministry of State Security, targeted managed service providers (MSPs) to access the networks of their clients, including shipping companies. This extensive cyber espionage campaign aimed to steal sensitive data, intellectual property, and trade secrets from various industries, including maritime. By compromising MSPs' networks, the Chinese government gained access to a vast array of companies, allowing them to gather valuable intelligence on maritime trade routes, cargo shipments, and port operations (Cybersecurity and Infrastructure Security Agency 2017).

In addition to state-sponsored espionage, non-state actors also pose a significant threat to the maritime industry, exploiting vulnerabilities within crew management and recruitment processes for illicit activities (Caesar and Fei 2018). For instance, criminal syndicates engage in drug smuggling operations, targeting shipping vessels by coercing or bribing crew members to facilitate the transportation of illegal narcotics across international borders. An example of this is the discovery of large quantities of drugs hidden aboard a container ship, revealing a sophisticated smuggling operation orchestrated by a criminal organization. Such incidents underscore the vulnerabilities within crew management systems and highlight the need for enhanced security measures to prevent criminal exploitation of maritime personnel (Europol 2023).

Moreover, terrorist organizations have shown their intent to exploit weaknesses in the maritime sector for strategic and ideological purposes. For example, the Somali-based terrorist group Al-Shabaab has targeted commercial Shipping vessels in piracy-prone regions like the Gulf of Aden and the Indian Ocean. The hijacking of MV Maersk Alabama by Somali pirates in 2009 highlighted the security risks faced by shipping companies operating in these areas (Kantharia 2019). Although piracy incidents have decreased in recent years due to improved maritime security measures, the threat of terrorist attacks or hijackings persists, necessitating ongoing vigilance and collaboration among industry stakeholders to effectively mitigate risks (Cho and Lee 2016).

Insider Threats

Malicious insiders and negligent insiders pose significant risks to shipping companies, often leading to substantial financial losses, reputational harm, and compromised security (BIMCO, et al. 2021; Gelles 2021; Kanellopoulos 2024). Real-life incidents provide concrete evidence of the severity of these threats and underscore the

necessity for robust countermeasures (Johnson 2010; Clark and Mitchell 2019). In 2016, a disgruntled IT contractor at Maersk Line, one of the world's largest shipping companies, orchestrated a devastating cyberattack that disrupted global operations and incurred substantial financial losses. The contractor, employed to manage Maersk's shipping systems, utilized his privileged access to implant the NotPetya malware into the company's network. This malicious act quickly spread across Maersk's infrastructure, bringing down essential systems worldwide. As a result of this cyberattack, Maersk was forced to shut down key operations, including container terminals, booking systems, and email communications, severely impacting global supply chains. The financial toll was immense, with Maersk estimating losses of over $300 million due to halted operations and recovery costs (Leovy 2017). The examples vividly illustrate how malicious insiders, motivated by personal grievances or financial incentives, can exploit their insider status to inflict significant harm on shipping companies (Catrantzos 2023).

Furthermore, negligent insiders, while not acting with malicious intent, can still pose serious security risks to organizations through their careless actions or failure to adhere to security protocols (Catrantzos 2023). In 2017, a significant data breach occurred at FedEx due to the negligent actions of an employee, highlighting the serious security risks posed by careless insiders. An employee at FedEx Office, the company's retail arm, inadvertently left unsecured customer information in a publicly accessible location. This information included scanned passports, driver's licenses, and other sensitive documents that customers had submitted for printing or copying services. The exposed documents were discovered by a customer who notified the media and raised concerns about the potential for identity theft and fraud. The incident attracted widespread attention and scrutiny, leading to investigations by regulatory authorities and damaging FedEx's reputation for data security. Upon investigation, it was revealed that the employee had failed to follow proper procedures for handling sensitive customer data, including securely storing and disposing of documents (Shaikh 2018). This oversight resulted in a breach of customer confidentiality and exposed individuals to significant privacy risks. This instance demonstrates how negligent insiders, due to their lack of awareness or disregard for security practices, can inadvertently create vulnerabilities that malicious actors exploit for nefarious purposes (BIMCO, et al. 2021; Gelles 2021; Catrantzos 2023; Kanellopoulos 2024).

Methods of Exploitation

The issue of falsified credentials poses a significant challenge in crew management and recruitment within shipping companies, where individuals may resort to deceptive practices to enhance their qualifications or experiences to secure employment (Clark and Mitchell 2019). This deception spans a spectrum from minor embellishments on resumes to outright fabrications of certifications or educational backgrounds. For example, an applicant might falsely claim to possess specialized maritime licenses or certifications crucial for certain roles, thereby misleading recruiters and potentially

jeopardizing the safety and security of operations (Estay 2020). In extreme cases, individuals with malicious intentions may resort to identity theft or the production of counterfeit documents to substantiate their false claims (Clark and Mitchell 2019).

Similarly, undisclosed affiliations present a notable risk factor as applicants may intentionally withhold information about their connections to external entities that could pose a threat to the organization (Cho and Lee 2016). For instance, an individual with affiliations to a foreign government, extremist group, or organized crime syndicate might conceal these associations during the recruitment process to avoid scrutiny or suspicion (ENISA 2024). However, such undisclosed affiliations could leave the company vulnerable to exploitation, as these individuals may be susceptible to coercion, blackmail, or recruitment by external actors seeking to exploit their insider status for espionage or sabotage purposes (Greene 1966; Gelles 2021; Catrantzos 2023).

Furthermore, social engineering tactics represent a sophisticated and covert threat to the security defenses of shipping companies. By leveraging human psychology and interpersonal relationships, threat actors can manipulate employees or recruiters into disclosing sensitive information, granting unauthorized access to systems, or unwittingly executing malicious actions (Clark and Mitchell 2019). For instance, attackers might impersonate trusted colleagues or authority figures to deceive employees into revealing login credentials, providing access to confidential databases, or initiating unauthorized transactions. Additionally, phishing attacks, characterized by deceptive emails or messages aimed at tricking recipients into divulging sensitive information or clicking on malicious links, remain a pervasive threat in the maritime industry (Clark and Mitchell 2019). These social engineering tactics underscore the imperative for robust cybersecurity measures, comprehensive employee training programs, and vigilant monitoring to detect and thwart potential threats before they manifest into actual harm (Duvenage, Jaquire and Solms 2018; Alcaide and Llave 2020; Ball 2021; Akpan, et al. 2022).

Counterintelligence Profiling and Screening in shipping companies

CI profiling and screening procedures within shipping companies represent a critical endeavor aimed at identifying and mitigating potential security risks (Cho and Lee 2016). This comprehensive approach involves a series of meticulously designed steps intended to scrutinize individuals' backgrounds, behaviors, and affiliations to enhance security measures effectively. The subsequent discussion will outline the essential steps involved in this profiling screening process (Prunckun 2019).

Information Gathering: The foundational stage of the profiling screening process entails comprehensive information gathering, which is fundamental for shipping

companies to develop a comprehensive understanding of potential candidates. This phase involves a systematic and exhaustive examination of various facets of the applicants' backgrounds and credentials. Personal history scrutiny encompasses a detailed review of past addresses, familial connections, and significant life events to glean insights into the individual's character and integrity (Clark and Mitchell 2019). Verification of educational background entails thorough validation of academic credentials, degrees earned, and institutions attended to ensure the authenticity of claimed qualifications. Scrutiny of employment records involves a meticulous assessment of past work experiences, job roles, and performance evaluations to gauge the candidates' professional competence and suitability for maritime positions. Furthermore, evaluating references provides valuable perspectives on the candidates' character, work ethic, and interpersonal capabilities, offering valuable insights into their past behavior and reliability. Through rigorous documentation and verification protocols, shipping companies aim to construct a comprehensive profile of each candidate, facilitating informed evaluations of their potential contributions to the organization and their alignment with the company's values and objectives (Grammenos 2010).

Background Checks: Background checks constitute a fundamental component of the screening process, serving as a critical mechanism for validating the accuracy and integrity of the information provided by applicants. Through rigorous scrutiny and verification procedures, shipping companies aim to corroborate the veracity of candidates' credentials and assertions, thereby ensuring transparency and reliability in the recruitment process (Caesar and Fei 2018). In alignment with principles from Occupational Psychology, the verification of credentials involves a comprehensive examination of academic qualifications, professional certifications, and licenses, thereby confirming the candidates' eligibility and proficiency for the roles they aspire to fulfill (Barrick and Mount 1991). This process aligns with the concept of the psychological profile of the job, which emphasizes the importance of matching the psychological requirements specific to a job with the qualifications and attributes of the applicants. Furthermore, scrutinizing employment history entails validating the accuracy of past job titles, responsibilities assumed, and duration of employment with previous employers, enabling shipping companies to evaluate the candidates' relevant experience and suitability for maritime positions (Morgeson and Humphrey 2006). This aspect corresponds to the Individual psychological profile of the person, which encompasses various psychological characteristics of the individual being assessed, including their work history and experiences (Judge and Bono 2001). Additionally, the investigation of any criminal records or legal issues serves to uncover potential red flags or inconsistencies in the candidates' background, thereby mitigating risks associated with the recruitment of individuals with a history of misconduct or legal entanglements (Cho and Lee 2016). Understanding the psychological aspects of such records can provide insights into an individual's propensity for ethical behavior and compliance with organizational norms, aligning with the principles of Occupational Psychology. Eventually, by

conducting thorough and diligent background checks informed by principles from Occupational Psychology, shipping companies can uphold the highest standards of integrity and diligence in their recruitment processes, thereby safeguarding against potential liabilities and preserving the security and reputation of the organization (Clark and Mitchell 2019; Gelles 2021).

Risk Assessment: Upon the conclusion of background checks, shipping companies undertake a comprehensive risk assessment aimed at systematically evaluating the potential security threats and vulnerabilities associated with each applicant (Cho and Lee 2016). This rigorous evaluation process involves a meticulous examination of various factors, including but not limited to, past behavior, affiliations, and any indicators of concern identified during the background verification process (BIMCO, et al. 2021). Through a thorough analysis of the applicant's historical conduct and associations, shipping companies endeavor to discern any discernible patterns or inclinations that may suggest a propensity toward unethical, illegal, or malicious behavior (Barnea and Meshulach 2020). Moreover, the assessment considers any affiliations or connections the individual may possess with entities or organizations that could pose a potential security risk to the shipping company's operations or assets (ENISA 2024). Additionally, the risk assessment scrutinizes any red flags or warning signs identified during the background check phase, such as discrepancies in the applicant's employment history or unresolved legal issues, to assess the severity of potential risks posed by the individual (Clark and Mitchell 2019). Through the implementation of this comprehensive risk assessment process, shipping companies can effectively identify and mitigate potential security threats, thereby bolstering the integrity and security of their crew management and recruitment practices (Caesar and Fei 2018).

Behavioral Analysis: Integrating behavioral analysis into profiling screening protocols constitutes a pivotal element in discerning potential security threats inherent in the recruitment processes of shipping companies. This facet of screening aligns with principles from Occupational Psychology, emphasizing the importance of understanding human behavior in organizational settings (Spector and Jex 1998). Through the lens of the psychological profile of the job, shipping companies aim to identify the psychological requirements specific to maritime roles and assess applicants' suitability based on their behavioral traits and characteristics (Barrick and Mount 1991). During this phase, a comprehensive evaluation is undertaken, encompassing both verbal and non-verbal cues exhibited by applicants throughout the recruitment process. Verbal cues may entail scrutinizing the language used, tone of voice, and responsiveness during interviews, while non-verbal cues encompass aspects such as body language, facial expressions, and overall demeanor (Morgeson & Humphrey, 2006). This aligns with the concept of the Individual psychological profile of the person, which emphasizes the assessment of various psychological characteristics, including communication styles and interpersonal behaviors (Ones, Viswesvaran and Dilchert 2005). Furthermore, written communication,

including application materials and correspondence, undergoes scrutiny to discern any inconsistencies, discrepancies, or red flags that may signify potential security risks (Cho and Lee 2016). By leveraging behavioral analysis techniques informed by principles from Occupational Psychology, shipping companies can effectively identify subtle indicators of deception or malicious intent, thereby augmenting the reliability and integrity of their crew management and recruitment processes (Clark and Mitchell 2019; Gelles 2021).

Affiliation Verification: Affiliation verification represents a critical phase in the profiling screening process, designed to uphold the integrity and security of crew management and recruitment practices within shipping companies (Caesar and Fei 2018). This facet involves meticulous scrutiny and validation of applicants' associations with external entities, encompassing foreign governments, extremist organizations, or criminal networks. By rigorously assessing applicants' affiliations, shipping companies can evaluate the potential for loyalty conflicts or security threats that may jeopardize organizational interests or operations (Clark and Mitchell 2019). This verification process entails comprehensive inquiries, leveraging diverse sources of information, and scrutinizing applicants' backgrounds to accurately ascertain the nature and scope of their affiliations. Additionally, employing specialized investigative techniques and methodologies may be necessary to uncover any undisclosed or concealed connections that could pose security risks (ENISA 2024). Through diligent verification of applicants' affiliations, shipping companies can enhance their resilience against potential insider threats or external influences, thereby fostering a secure and conducive environment for crew management and recruitment activities (Gelles 2021; Catrantzos 2023).

Security Clearance Checks: Security clearance checks play a pivotal role in the profiling screening process, especially for positions requiring access to sensitive information or involvement in critical operations within shipping companies (Auster and Choo 1994). This rigorous procedure involves assessing individuals' eligibility to access classified data or engage in confidential activities based on a thorough evaluation of their background, trustworthiness, and allegiance to the organization (Barnea 2019). By subjecting applicants to comprehensive security clearance checks, shipping companies can determine the suitability and reliability of candidates for roles with heightened security responsibilities (ENISA 2024). This assessment delves into various aspects of the applicant's personal and professional history, including past affiliations, criminal records, financial stability, and overall integrity (Clark and Mitchell 2019). Additionally, security clearance checks may entail extensive interviews, background investigations, reference verifications, and character assessments to ascertain candidates' adherence to ethical standards and their ability to maintain confidentiality (ENISA 2024). Through meticulous scrutiny and adherence to established security protocols, shipping companies can effectively mitigate the risks associated with unauthorized access to sensitive information or potential breaches of security protocols (BIMCO, et al. 2021). By ensuring that

only individuals possessing the necessary qualifications, integrity, and loyalty are granted security clearances, organizations can enhance their resilience against internal threats and safeguard their critical assets from unauthorized disclosure or exploitation (Gelles 2021).

Continuous Monitoring: Continuous monitoring is an essential aspect of profiling screening, extending scrutiny beyond the initial hiring phase to encompass ongoing surveillance of employees' behavior and circumstances within shipping companies (Clark and Mitchell 2019). In line with principles from Occupational Psychology, this proactive approach acknowledges the dynamic nature of human behavior in organizational settings and emphasizes the importance of continuous assessment and adaptation (Spector and Jex 1998). Through systematic and vigilant monitoring mechanisms, such as surveillance systems, digital monitoring software, and periodic assessments, shipping companies can surveil employees' activities, communications, and interactions within the workplace environment (BIMCO, et al. 2021). This aligns with the concept of the psychological profile of the job, which emphasizes the identification of psychological requirements specific to maritime roles and the ongoing assessment of employees' alignment with these requirements (Morgeson and Humphrey 2006). Regular assessments and audits help identify potential red flags indicative of security vulnerabilities, such as sudden changes in behavior patterns, unauthorized access attempts, or suspicious communications (Gelles 2021). This corresponds to the Individual psychological profile of the person, which encompasses various psychological characteristics, including behavioral tendencies and communication styles (Ones, Viswesvaran and Dilchert 2005). Additionally, continuous monitoring facilitates the prompt identification and response to any deviations from established security protocols or compliance requirements, allowing organizations to intervene swiftly and mitigate potential threats before they escalate (ENISA 2024). By maintaining a vigilant stance and staying attuned to evolving security dynamics, shipping companies can bolster their resilience against internal threats and uphold the integrity and security of their operations and assets over the long term (Ball 2021).

Training and Awareness: Training and awareness initiatives are pivotal components in cultivating a culture of security and vigilance within shipping companies (Georgiadou, Mouzakitis and Askounis 2021). Through comprehensive training programs, employees acquire a deeper understanding of the importance of adhering to security protocols and remain alert to potential threats (ENISA 2024). These initiatives aim to equip staff with the requisite knowledge and skills to identify and respond effectively to suspicious activities or behaviors that could compromise the organization's security. Interactive workshops, seminars, and online modules are utilized to guide recognizing common indicators of security threats, such as anomalies in behavior patterns, unauthorized access attempts, or suspicious communications. Furthermore, training sessions offer practical advice on promptly and accurately reporting such incidents to designated authorities or security personnel for further investigation (ENISA 2024). By fostering a sense of ownership

and accountability for security among employees, these initiatives establish a robust frontline defense against both internal and external threats. Additionally, ongoing awareness campaigns and communication channels serve to reinforce key security messages and keep employees abreast of emerging risks or evolving security protocols. Through the cultivation of a culture of security consciousness and empowerment, shipping companies can bolster their resilience against potential threats and effectively safeguard their operations and assets (BIMCO, et al. 2021); (Georgiadou, Mouzakitis and Askounis 2021).

Adherence to Regulations: Ensuring adherence to regulations is fundamental to establishing robust security and CI practices within shipping companies. Organizations must rigorously comply with pertinent laws, regulations, and industry standards governing security protocols to uphold the integrity and credibility of their operations (Giannakopoulou, Thalassinos and Stamatopoulos 2016). By aligning profiling screening procedures with legal requirements and industry best practices, shipping companies manifest their dedication to maintaining security standards and mitigating potential risks proficiently (Cho and Lee 2016). This necessitates a comprehensive understanding and implementation of regulations such as the International Ship and Port Facility Security (ISPS) Code, which mandates stringent security measures for ships and port facilities globally (BIMCO, et al. 2021). Moreover, compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), ensures the lawful and ethical handling of sensitive information collected during screening processes (Auster and Choo 1994; Ronn 2016; Barnea 2019). shipping companies must also remain vigilant regarding evolving regulatory landscapes and adapt their security practices accordingly to effectively address emerging threats and regulatory modifications (ENISA 2024). By prioritizing compliance and regulatory adherence, organizations underscore their commitment to upholding the highest standards of security and integrity, thereby fostering trust and confidence among stakeholders and safeguarding the safety and security of maritime operations (Gelles 2021).

In conclusion, CI profiling and screening procedures in shipping companies encompass a thorough and methodical process aimed at evaluating the backgrounds, behaviors, and affiliations of individuals to mitigate security risks proficiently. Through adherence to these steps and the incorporation of robust security protocols, shipping companies can fortify their defenses against potential threats, thereby ensuring the protection of their operations and assets.

Potential Vulnerabilities in Counterintelligence Profiling and Screening

CI profiling and screening procedures in shipping companies are susceptible to significant vulnerabilities that necessitate careful attention and mitigation strategies.

A notable vulnerability arises from the reliance on potentially incomplete or inaccurate information during the screening process, which can lead to misguided assessments and compromise the overall efficacy of screening procedures (Kanellopoulos 2022). Additionally, biases present within the screening process pose another substantial vulnerability, as they may influence decision-making and result in unfair treatment or the overlooking of critical information (Lowenthal 2009); (Giannakopoulou, Thalassinos and Stamatopoulos 2016). Furthermore, the insufficient training of personnel responsible for conducting screenings constitutes another vulnerability, as it can diminish their proficiency and lead to oversight of crucial indicators or the failure to detect red flags effectively.

To address these vulnerabilities, the implementation of best practices in profiling screening is imperative. Leveraging multiple data sources for verification is paramount to enhance the accuracy and reliability of screening outcomes (Lowenthal 2009); (Barnea 2019). Cross-referencing information from various sources enables companies to validate applicant credentials more effectively and identify discrepancies (Auster and Choo 1994). Moreover, regular training and certification programs for screening personnel are essential to maintain competence and professionalism. Ongoing training ensures that personnel possess the requisite skills and knowledge to perform screenings accurately and impartially. Continuous evaluation and refinement of screening protocols are also crucial to address evolving threats and lessons learned from past experiences. Regular reviews and updates to screening procedures enable companies to adapt to emerging risks and bolster the effectiveness of their CI efforts (Clark and Mitchell 2019).

By prioritizing these best practices, shipping companies can mitigate vulnerabilities within their profiling screening processes and uphold the integrity and reliability of their security protocols. This proactive approach not only enhances the screening process's effectiveness but also contributes to overall organizational resilience against security threats in the maritime industry.

Conclusions

In summary, although CI profiling and screening procedures significantly contribute to enhancing security measures within shipping companies, they are susceptible to vulnerabilities that demand attention. Drawing from insights in Occupational Psychology, it is imperative to address challenges such as reliance on potentially inaccurate or incomplete information, biases in the screening process, and inadequate training of personnel to bolster the efficacy of these procedures.

By aligning with the psychological profile of the job, shipping companies can refine their screening processes by identifying and prioritizing the psychological requirements specific to maritime roles. This includes assessing the cognitive,

emotional, and behavioral attributes necessary for effective security screening (Barrick and Mount 1991).
Similarly, the individual psychological profile of the person plays a crucial role in ensuring the suitability of screening personnel. By considering factors such as personality traits, communication skills, and decision-making abilities, companies can select and train personnel who are well-equipped to handle the complexities of profiling screening (Judge and Bono 2001).

Nevertheless, by adopting best practices such as leveraging multiple data sources for verification, providing regular training and certification programs for screening personnel, and continuously evaluating and refining screening protocols, shipping companies can effectively mitigate these vulnerabilities (Barnea 2019).

Companies must remain vigilant and adaptable in the face of evolving threats, ensuring that their CI efforts remain robust and reliable (Kanellopoulos 2022). Through a proactive and comprehensive approach to profiling screening, shipping companies can fortify their security posture and mitigate potential breaches, thereby contributing to the overall safety and integrity of maritime operations.

References

Akpan, F., G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos. 2022. "Cybersecurity challenges in the Maritime Sector ." *Network* 2 (1): pp. 123–138. https://doi.org/10.3390/network2010009.

Alcaide, J.I., and R.G. Llave. 2020. "Critical infrastructures cybersecurity and the Maritime Sector ." *Transportation Research Procedia* 45: pp. 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.

Auster, E., and C.W. Choo. 1994. "How senior managers acquire and use information in environmental scanning." *Information Processing & Management* 30 (5): pp. 607–618. https://doi.org/10.1016/0306-4573(94)90073-6.

Ball, K. 2021. "Electronic Monitoring and Surveillance in the Workplace." *Joint Research Center – European Commission.* https://publications.jrc.ec.europa.eu/repository/handle/JRC125716.

Barnea, A. 2019. "Big Data and Counterintelligence in Western countries ." *International Journal of Intelligence and Counterintelligence* 32 (3): pp. 433–447.

Barnea, A., and A. Meshulach. 2020. "Forecasting for Intelligence Analysis: Scenarios to abort strategic surprise." *International Journal of Intelligence and Counterintelligence* 34 (1): pp. 106–133.

Barrick, M.R., and M.K. Mount. 1991. "The Big Five personality dimensions and job performance: A meta-analysis." *Personnel Psychology* 44 (1): pp. 1-26.

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo, Shipowners (INTERCARGO),

InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International, Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC). 2021. *The Guidelines on Cyber Security Onboard Ships.* https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pd.

Caesar, L.D., and J. Fei. 2018. "Recruitment and the image of the shipping industry." In *Managing Human Resources in the Shipping Industry*, pp. 18-36. Routledge. doi:10.4324/9781315740027-2.

Catrantzos, N. 2023. *Managing the Insider Threat No Dark Corners and the Rising Tide Menace.* CRC Press.

Cho, I., and K. Lee. 2016. "Advanced risk measurement approach to insider threats in Cyberspace." *Intelligent Automation & Soft Computing* 22 (3): pp. 405–413. https://doi.org/10.1080/10798587.2015.1121617.

Clark, R.M., and W. Mitchell. 2019. *Deception: Counterdeception and Counterintelligence.* Washington, DC: CQ Press.

Cybersecurity and Infrastructure Security Agency. 2017. *Awareness Briefing: Chinese Cyber Activity Targeting Managed Service Providers.* https://www.cisa.gov/sites/default/files/c3vp/Chinese-Cyber-Activity-Targeting-Managed-Service-Providers.pdf.

Duvenage, P., and S. Solms. 2014. *Putting Counterintelligence in Cyber Counterintelligence. 13th European Conference on Cyber Warfare and Security.* https://www.researchgate.net/publication/328732134_Putting_Counterintelligence_in_Cyber_Counterintelligence.

Duvenage, P., V. Jaquire, and S. Solms. 2018. "Towards a Literature Review on Cyber Counterintelligence ." *Journal of Information Warfare* 17 (4): pp. 284-297. https://www.jstor.org/stable/26783824.

ENISA. 2024. *Cyber Resilience Act Requirements Standards Mapping.* https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping .

Estay, D. 2020. *Cyber resilience for the shipping industry. CyberShip Project.* https://www.dendanskemaritimefond.dk/wp-content/uploads/2017/03/Cybership_Report_WP_5.pdf.

Europol. 2023. *New Modus Operandi: How organized crime infiltrates the ports of Europe .* https://www.europol.europa.eu/media-press/newsroom/news/new-modus-operandi-how-organised-crime-infiltrates-ports-of-europe.

Gelles, M. 2021. "Insider threat prevention, detection, and mitigation." In *International Handbook of Threat Assessment*, pp. 669–679. https://doi.org/10.1093/med-psych/9780190940164.003.0037.

Georgiadou, A., S. Mouzakitis, and D. Askounis. 2021. "Detecting insider threat via a cyber-security culture framework." *Journal of Computer Information Systems* 63 (4): pp. 706–716.

Giannakopoulou, E.N., E.I. Thalassinos, and T.V. Stamatopoulos. 2016. "Corporate governance in shipping: an overview." *Maritime Policy & Management* 43 (1): pp. 19-39.

Grammenos, T. 2010. *The Handbook of Maritime Economics and Business.* Edited by Lloyd's List.

Greene, R. 1966. *Business Intelligence and Espionage.* Homewood: Dow Jones- Irwin.

Johnson, L.K. 2010. *Handbook of Intelligence Studies.* London: Routledge.

Judge, T.A., and J.E. Bono. 2001. "Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis." *Journal of Applied Psychology* 86 (1): pp. 80-92.

Kanellopoulos, A.N. 2022. "The Importance of Counterintelligence Culture in State Security." *Global Security and Intelligence* Note 5. https://www.buckingham.ac.uk/wp-content/uploads/2022/07/GSIN_5a.pdf.

__. 2023. "The Dimensions of Counterintelligence and Their Role in National Security." *Journal of European and American Intelligence Studies* 6 (2): pp. 85-104.

__. 2024. "Insider threat mitigation through human intelligence and counterintelligence: A case study in the shipping industry." *Defense and Security Studies* (5) 1: pp. 10-19. https://doi.org/10.37868/dss.v5.id261.

Kantharia, Raunek. 2019. *The Story of Maersk Alabama Container Vessel.* https://www.marineinsight.com/marine-piracy-marine/the-story-of-maersk-alabama-container-vessel/.

Leovy, J. 2017. "Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks." *Los Angeles Times.* https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html.

Lowenthal, M. 2009. *Intelligence: From secrets to policy.* Washington, DC: CQ Press.

Morgeson, F.P., and S.E. Humphrey. 2006. "The Work Design Questionnaire (WDQ): Developing and validating a comprehensive measure for assessing job design and the nature of work ." *Journal of Applied Psychology* 91 (6): pp. 1321-1339.

Ones, D.S., C. Viswesvaran, and S. Dilchert. 2005. "Cognitive ability in selection decisions." *Handbook of employee selection* 3: pp. 431–468.

Prunckun, H.W. 2019. *Counterintelligence theory and practice.* London: Rowman et Littlefield.

Ronn, K.V. 2016. "Intelligence ethics: A critical review and future perspectives." *International Journal of Intelligence and Counterintelligence* 29 (4): pp. 760–784. https://doi:10.1080/08850607.2016.1177399.

Shaikh, R. 2018. "More spills... thousands of passports, driver's licenses, & Photo ids of fedex customers exposed." *Wccftech.* https://wccftech.com/thousands-passports-fedex-exposed/.

Spector, P.E., and S.M. Jex. 1998. "Development of four self-report measures of job stressors and strain: Interpersonal Conflict at Work Scale, Organizational Constraints Scale, Quantitative Workload Inventory, and Physical Symptoms Inventory." *Journal of Occupational Health Psychology* 3 (4): pp. 356-367.

Wettering, F.L. 2000. "Counterintelligence: The broken triad." *International Journal of Intelligence and Counterintelligence* 13 (3): pp. 265–300.