Anastasios-Nikolaos Kanellopoulos
Ph.D. Candidate Department of Business Administration, Athens University of Economics and Business
Email: ankanell@aueb.gr

Dr. Anthony Ioannidis
Assistant Professor of Management at the Department of Business Administration, Athens University of Economics and Business
Email: ai@aueb.gr

DOI:
Review paper
Received: October 23, 2024
Accepted: December 15, 2024

EMERGING INTELLIGENCE OPERATIONAL THREATS FOR THE SHIPPING INDUSTRY

Abstract: *The shipping industry, driven by rapid technological advancement and digital transformation, faces an evolving landscape of threats to intelligence operations. This paper delves into the multifaceted challenges posed by information warfare, state-sponsored espionage, and corporate espionage, which are motivated by economic gain, geopolitical advantage, and the acquisition of critical data. These threats have profound security implications, extending from financial risks to vessel and cargo safety. In addition to external threats, the industry must confront the human element, with insider actions posing a formidable challenge. Insiders can be exploited through social engineering and infiltration, underscoring the need for security awareness and risk mitigation measures. Moreover, the geopolitical context further complicates the maritime sector's security landscape, with China's expanding presence in the South China Sea and Russia's assertiveness in key maritime regions. These actions have significant implications for global trade, regional security, and the balance of power. To address these emerging threats, the paper emphasizes the importance of a holistic counterintelligence approach. Cybersecurity measures, employee training, and regular audits form the foundation of defense. Competitive intelligence and risk analysis, focusing on monitoring geopolitical developments and cyber threat indicators, are crucial for crafting effective risk mitigation strategies.*

Keywords: *Intelligence operations, Shipping industry security, Counterintelligence, Insider Threat, Competitive Intelligence, Russia, China.*

Introduction

Amidst a backdrop of rapid technological advancement, the Shipping industry finds itself grappling with a transformative shift in intelligence operations. This transformation is underscored by the amalgamation of the digital age, espionage, geopolitical tensions involving state actors, and the persistent specter of insider threats (Kanellopoulos, 2024). These converging factors form a complex tapestry of challenges that demand urgent attention. As the maritime sector navigates this dynamic landscape, marked by the adoption of cutting-edge technologies to enhance efficiency, safety, and innovation, it also confronts newfound vulnerabilities. These vulnerabilities, stemming from the digital revolution, expose the industry to a spectrum of cyber threats emanating from state-sponsored actors and criminal organizations (Lorange, 2020; Guitton and Fréchette, 2023).

Delving into the intricate world of intelligence operations within the maritime domain necessitates a deep exploration of information warfare, state-sponsored espionage, and corporate espionage. These evolving tactics, driven by motives of economic gain and geopolitical advantage, pose significant security risks, extending from economic perils to the safety and security of vessels and cargo (Amiri et al., 2017; Munim et al., 2020). Moreover, the human element within the maritime sector emerges as both the industry's backbone and a potential Achilles' heel. Insider threats loom large as adversaries employ various stratagems, including social engineering and infiltration, to exploit insiders and gain illicit access to sensitive information and critical systems (Cho and Lee, 2016; Kanellopoulos, 2024).

Furthermore, as the industry traverses geopolitical waters, it encounters the expansive maritime presence of China and the assertive stance of Russia. The actions of these state actors raise concerns regarding the potential deployment of intelligence operations in key maritime regions. China's maneuvers in the South China Sea and Russia's activities in Eastern Europe and the Arctic carry significant implications for global trade, regional security, and the geopolitical balance of power (Amin and Rafique, 2021).

In response to these emergent challenges, the Shipping industry is compelled to adopt a holistic approach to counterintelligence. This approach encompasses a spectrum of cybersecurity measures, including the implementation of state-of-the-art firewalls, comprehensive employee training programs, and regular audits. Moreover, it underscores

the importance of competitive intelligence and risk analysis, emphasizing the need to monitor geopolitical developments and cyber threat indicators (Munim et al., 2020; Akpan, 2022).

As this paper sets out to explore the dynamic evolution of intelligence operations within the Shipping sector, it emphasizes the critical importance of vigilance, adaptability, and a comprehensive counterintelligence strategy (Španja et al., 2017; Ko and Song, 2022). It is structured into three main sections, each addressing distinct but interconnected aspects of the topic. The first section encompasses the changing landscape of intelligence operations in the digital age and cyber threats, along with espionage and information gathering, provides a comprehensive examination of the evolving challenges posed by technological advancements and espionage tactics. Within this section, particular emphasis is placed on the concept of insider threats, elucidating how human vulnerabilities, exacerbated by the digital revolution, can compromise security within maritime operations. It delves into various methods employed by adversaries, including sophisticated social engineering techniques and infiltration strategies, and scrutinizes their potential ramifications on industry integrity. The second section shifts focus to geopolitical tensions and the actions of state actors, particularly China and Russia, in the maritime domain. It explores China's expanding maritime presence and intelligence operations, as well as Russia's assertive posture in regions like the Black Sea and the Arctic, elucidating their motivations and potential impacts on global trade and security. Finally, the third section outlines countermeasures and mitigation strategies aimed at safeguarding the Shipping industry against intelligence threats. It discusses defensive and offensive counterintelligence measures, counterespionage tactics, insider threat detection, as well as the importance of competitive intelligence and business environment monitoring. This comprehensive approach aims to address the evolving landscape of intelligence operations while ensuring the integrity, safety, and security of maritime activities.

Eventually, the intricate interplay among rapid technological advancements, state-sponsored espionage activities, geopolitical tensions, and the persistent specter of insider threats underscores an imperative demand for proactive interventions within the maritime industry. This confluence of factors not only accentuates the vulnerabilities inherent in contemporary maritime operations but also accentuates the critical need for strategic fortification measures to safeguard industry integrity, optimize operational efficacy, and cultivate an environment

conducive to innovation. Amidst this dynamic landscape, the maritime sector stands at a pivotal juncture, compelled to confront the multifaceted challenges posed by the intersection of technological evolution and geopolitical maneuvering. Central to this discourse is the fundamental inquiry: How can the maritime industry strategically augment its counterintelligence frameworks to effectively mitigate the evolving array of threats? In response to this pivotal question, this paper endeavors to engage in a thorough examination, drawing upon an exhaustive synthesis of insights gleaned from a diverse spectrum of scholarly resources and empirical evidence. The answer is encapsulated in the formulation of a comprehensive counterintelligence and competitive intelligence framework. This framework encompasses various facets, including defensive and offensive counterintelligence, counterespionage, competitive intelligence, business environment monitoring, intelligence and security risk analysis, and insider threat detection and mitigation. By integrating these elements, the maritime industry can effectively address the multifaceted challenges posed by contemporary intelligence operations. Future studies can delve deeper into the implementation of this framework within Shipping companies, exploring the practical strategies and methodologies for its adaptation and integration into existing operational structures.

The Changing Landscape of Intelligence Operations

The Digital Age and Cyber Threats

The Shipping industry, mirroring the trajectory of numerous other sectors in our era of rapid advancement, has experienced a profound metamorphosis propelled by its escalating reliance on digital technology (Munim et al., 2020). This shift towards digitalization has presented opportunities for enhanced efficiency and innovation, equipping Shipping companies with the requisite tools to optimize fleet and cargo management (Gruner, 2021). Nevertheless, this surge in technological advancement has concurrently exposed the industry to a gamut of cybersecurity threats emanating from both state-sponsored actors and criminal syndicates (Giannakopoulou et al., 2016; Akpan, 2022).

In the landscape of modern logistics, Shipping enterprises have embraced cutting-edge technologies to refine their operations (Ichimura, 2022). Sophisticated communication systems now facilitate seamless real-time data and information exchanges among vessels, Shipping hubs, and onshore personnel, expediting decision-making processes and refining

route optimization strategies (Niknami et al., 2023). Integrating satellite navigation systems has revolutionized maritime navigation, elevating positional accuracy and bolstering safety and efficiency in marine transportation. Additionally, interconnected networks have streamlined fleet and cargo management, offering dynamic real-time tracking and monitoring capabilities (Durlik, 2023).

Nevertheless, this increased reliance on digital infrastructure comes with inherent risks (Alcaide and Llave, 2020; Gruner, 2021). The Shipping industry's digitalization has made it a prime target for cyber adversaries (Munim et al., 2020; Akpan, 2022). State-sponsored actors, often with vast resources and sophisticated capabilities, may attempt to infiltrate and compromise critical maritime infrastructure. Their motivations can range from collecting sensitive information about cargo or vessel movements for geopolitical or economic advantage to disrupting Shipping operations to serve strategic interests (Amiri et al., 2017; Emmanuelides and Tsavliris, 2019; Alcaide and Llave, 2020).

Criminal organizations, on the other hand, see the Shipping industry as an opportunity for illicit financial gain. These groups have turned to cyber tactics to exploit vulnerabilities within the Shipping sector. Hacking into ship navigation systems can jeopardize vessel safety by manipulating navigation data or causing system malfunctions. Furthermore, ransomware attacks targeting port authorities can bring entire ports to a standstill, leading to significant disruptions in the flow of goods and resulting in substantial financial losses (Ben Farah et al., 2022). Eventually, in 2017, Maersk, one of the world's largest Shipping companies, fell victim to the NotPetya ransomware attack. The malware infiltrated Maersk's computer systems, causing widespread disruption to its operations. The attack paralyzed Maersk's IT infrastructure, including its booking system, email services, and container tracking systems. As a result, Maersk was forced to shut down many of its port terminals worldwide, leading to significant delays in cargo shipments and financial losses estimated to be hundreds of millions of dollars (Greenberg, 2018). This incident highlighted the vulnerability of the maritime industry to cyber threats and underscored the potential for ransomware attacks to disrupt port operations and supply chains (Estay, 2020; Cybersecurity and Infrastructure Security Agency, 2021; Kaminska et al., 2021). Moreover, in 2018, the Port of San Diego in California, United States, experienced a ransomware attack that disrupted its IT systems. The attack targeted the port's administrative computer network, affecting various services such as email, document management, and other internal systems.

While the port's operational systems remained unaffected, the incident caused significant disruptions to administrative functions and forced the port to shut down several services temporarily. Although the port did not disclose the exact ransom amount demanded by the attackers, the incident highlighted the vulnerability of port authorities to ransomware attacks and the potential for such attacks to disrupt port operations and administrative functions (Schwarz et al., 2021).

Espionage and Information Gathering

Intelligence operations have evolved significantly, transcending the boundaries of the physical realm as we continue to witness the increasing connectivity and integration of maritime infrastructure with the digital world (Alcaide and Llave, 2020; Munim et al., 2020). Today, information warfare has emerged as a powerful tool that poses a substantial threat to the Shipping industry. This threat manifests in various forms, from state-sponsored espionage to corporate espionage, all aimed at gathering sensitive information that can have far-reaching consequences (Barnea, 2019).

Foreign governments and competing companies are increasingly engaged in intelligence operations that target maritime Shipping entities (Rupert et al., 2009). Their objectives can vary but commonly revolve around the acquisition of critical data related to cargo, routes, or the operational strategies of Shipping companies (Emmanuelides and Tsavliris, 2019). Such sensitive information can provide these entities with a competitive edge, a stronger geopolitical position, or even financial advantages (Herbert-Burns and Lehr, 2009; Amiri et al., 2017).

One primary motivation for espionage in the maritime sector is the quest for economic gain. Shipping companies control vast quantities of goods and operate within a complex global supply chain (Sodhi and Tang, 2014). Access to information about cargo manifests, shipment schedules, and routes can enable malicious actors to predict market trends, identify valuable cargo targets, or exploit pricing differentials for their economic benefit (Herbert-Burns and Lehr, 2009). This economic advantage can come at the cost of legitimate players in the industry, leading to unfair competition and financial losses for affected companies (Grammenos, 2010).

Geopolitical advantage is another driving force behind intelligence operations in the maritime domain. The maritime industry plays a pivotal role in global trade, as it is responsible for transporting goods from one part of the world to another (The Hague Centre for Strategic Studies, 2019). Consequently, information about the routes, cargo, or strategic decisions of Shipping companies can be leveraged to manipulate international trade dynamics (Munim et al., 2020). State actors, particularly those with geopolitical interests in specific regions or Shipping lanes, may engage in Intelligence operations to exert influence, monitor foreign vessels, or gather intelligence to advance their national security interests (Van Cleave, 2007).

The implications of such intelligence operations extend well beyond mere data acquisition. They can lead to considerable economic and security risks. Economically, the manipulation of market dynamics and disruption of trade routes can destabilize global commerce, potentially leading to increased costs for consumers, supply chain disruptions, and, in some cases, even economic recessions (Grammenos, 2010; Sodhi and Tang, 2014).

From a security perspective, the shipping industry's reliance on information and communication systems means that compromised data or infrastructure can threaten the safety and security of seafarers and valuable cargo. When state actors gain access to critical information or navigation systems, they may not only disrupt normal operations but also pose direct threats to maritime security by manipulating vessel movement routes or even staging cyber-attacks on ships (Ben Farah et al., 2022).

Insider Threats

In the multifaceted and intricate world of the Shipping industry, the human element plays a pivotal role, yet it can also be the weakest link in terms of security (Catrantzos, 2012). Within this expansive sector, a diverse array of employees, from dedicated crew members to diligent port workers and the staff of Shipping companies, are integral to its functioning (Cho and Lee, 2016). However, it is precisely this human factor that often presents a vulnerability, making it susceptible to security breaches (Kanellopoulos, 2024).

The employees in the shipping industry serve as the industry's backbone, and they are responsible for ensuring the smooth and efficient movement of goods across the world's oceans (Gelles, 2021). This includes the highly skilled and experienced seafarers who

operate the vessels, the dockworkers who manage the loading and unloading of cargo at ports, and the administrative personnel within Shipping companies who oversee logistics, cargo scheduling, and security protocols. Despite their essential roles, these individuals can inadvertently or intentionally compromise security, potentially jeopardizing the industry's integrity (Cho and Lee, 2016; Prunckun, 2019).

Furthermore, social engineering, for instance, is a technique that relies on psychological manipulation to deceive individuals into divulging confidential information or participating in harmful actions (Gelles, 2021). In the maritime context, adversaries may craft convincing pretenses to elicit information or cooperation from unsuspecting employees. For example, they could pose as fellow employees, contractors, or service providers to gain access to secure areas or systems (Kanellopoulos, 2024).

Infiltration, another method employed in intelligence operations, may involve individuals deliberately placed within an organization, such as a Shipping company or port authority (Gelles, 2021). These moles are tasked with acquiring sensitive information or facilitating cyber-attacks from the inside, often undetected by security measures (Guitton and Fréchette, 2023).

In due course, the implications of compromised security within the Shipping industry are significant. Adversaries who gain access to sensitive information or critical systems can disrupt operations, compromise safety, and facilitate the theft of valuable cargo. Whether through hacking navigation systems, manipulating cargo manifests, or compromising access control systems, the consequences can extend beyond financial losses to include damage to the industry's reputation and, in severe cases, threats to national security (Van Cleave, 2007; Cho and Lee, 2016).

Geopolitical Tensions and State Actors

China's Expanding Maritime Presence

China's remarkable rise as a global superpower has been accompanied by a substantial expansion of its naval capabilities and territorial ambitions, particularly in the South China Sea and surrounding regions (Raine, 2017). This growth has raised concerns among international stakeholders about the potential ways China might leverage its maritime power

for both intelligence gathering and coercive actions (Buzynski, 2021; US Department of Defense, 2023).

The South China Sea, in particular, has become a focal point of international attention due to China's expansive territorial claims, which often overlap with those of neighboring nations (Raine, 2017). These claims encompass strategic islands, reefs, and waters that have significant geopolitical and economic importance (Papasotiriou, 2013). China's actions in the South China Sea have triggered concerns that its maritime ambitions may extend beyond sovereignty disputes and territorial control (Kipgen, 2021). Chinese Intelligence Agencies, often working in tandem with the People's Liberation Army Navy (PLAN), have the capability to conduct intelligence operations aimed at monitoring foreign vessels and collecting data on maritime traffic routes (Ministry of National Defense of the People's Republic of China, 2019; US Department of Defense, 2023). This ability enables them to track the movements of both military and civilian ships, including those of foreign nations, further deepening concerns among neighboring countries and international observers (Luttwak and Carson, 2019).

One of the key objectives of China's intelligence operations in the South China Sea is to monitor foreign naval activities (Kipgen, 2021; US Department of Defense, 2023). By closely observing the movements of foreign military vessels, particularly those of the United States and other nations conducting freedom of navigation operations (FONOPs), China aims to maintain a real-time understanding of potential threats or challenges to its territorial claims (Fu, 2015). This also enables China to respond proactively and serves as a tool for deterrence. Additionally, it is noteworthy that foreign military vessels also engage in Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) operations in the region (US Department of Defense, 2023). Moreover, the implications of China's maritime Intelligence operations are manifold. They raise concerns about the potential militarization of the South China Sea and an escalation of regional tensions. Chinese actions could lead to disruptions in global trade as the uncertainty surrounding Shipping routes increases (Ko and Song, 2022). Furthermore, they pose questions about the sanctity of international waters and the balance of power in the Indo-Pacific region (Amin and Rafique, 2021).

The international community, with a keen interest in the developments unfolding in the South China Sea, is actively engaged in monitoring these evolving situations. Recognizing the significance of the region's stability for global security and trade, countries with stakes in the South China Sea have employed various strategies to address China's territorial ambitions and intelligence operations. Diplomatic efforts play a crucial role in navigating the complexities of the South China Sea disputes, promoting dialogue cooperation, and seeking peaceful resolutions. International arbitration, exemplified by the Philippines v. China UNCLOS arbitral ruling in 2016, serves as a means to address legal disagreements and uphold international law. Furthermore, the presence of military forces in the region serves as a tangible deterrent against assertive actions and coercion through maritime patrols, joint exercises, and alliances (Chubb, 2022). However, striking a delicate balance amidst competing interests and power dynamics remains a formidable challenge, necessitating nuanced diplomacy, strategic cooperation, and a commitment to multilateralism. Managing these complexities demands constructive engagement with all stakeholders, including China, to seek mutually beneficial solutions and prevent further destabilization of the region, fostering a conducive environment for peaceful coexistence, economic prosperity, and security in the South China Sea and beyond. (Papasotiriou, 2013).

Additionally, China's intelligence operations extend beyond mere surveillance and data collection. They are strategically designed to exert influence over global Shipping routes (Ministry of National Defense of the People's Republic of China, 2019). Given that a substantial portion of the world's trade passes through these waters, China's ability to shape and control maritime traffic has far-reaching implications (Buzynski, 2021; European Parliament, 2023). By leveraging its presence and surveillance capabilities, China can influence the movement of vessels, potentially favoring or obstructing the passage of specific ships or types of cargo. Through diplomatic channels and economic incentives, China can further solidify its influence, shaping the flow of trade to align with its strategic interests and geopolitical objectives. This comprehensive approach underscores China's determination to assert dominance in maritime affairs and secure its position as a key player in global trade dynamics (Calatayud, 2023; European Parliament, 2023; Sly and Ledur, 2023).

Moreover, China's Belt and Road Initiative (BRI) significantly enhances its maritime influence. The BRI, launched in 2013, aims to improve connectivity and cooperation

between China and other countries through infrastructure development and investment (Russel and Berger, 2020; European Parliament, 2023). One aspect of the BRI focuses on developing maritime infrastructure, such as ports and Shipping lanes, in strategically located regions. By investing in and controlling key ports along critical maritime routes, China can exert more significant influence over Shipping activities and trade flows. This allows China to enhance its economic interests and extend its geopolitical influence across various regions (Russel and Berger, 2020).

Additionally, in collaboration with countries like Iraq, China has embarked on substantial infrastructure projects, particularly in the energy sector, as part of the BRI (Çalışkan, 2023). These investments extend beyond mere port and transportation network development to encompass the establishment of energy infrastructure, such as oil and gas pipelines and power plants. China's involvement in Iraq's energy sector aims to strengthen bilateral economic ties while addressing China's growing energy demands. By investing in Iraq's energy infrastructure, China secures a stable source of energy imports, particularly oil, which is crucial for fueling its rapid industrialization and economic growth (Lixia, 2021). Additionally, these investments enhance China's access to the Middle East and the Mediterranean Sea, strategically positioning it to play a significant role in regional energy dynamics. Moreover, China's collaboration with Iraq in the energy sector aligns with Iraq's goal of diversifying its energy exports and attracting foreign investment to revitalize its economy. Through mutually beneficial energy collaborations, China and Iraq seek to foster long-term economic cooperation and strategic partnerships under the framework of the BRI (Lixia, 2021; Çalışkan, 2023).

Similarly, China's collaboration with Iran under the BRI encompasses a multifaceted approach, extending beyond port development and transportation infrastructure to include strategic investments in the energy sector (Osiewicz, 2018). These investments in energy collaboration hold significant importance for both China and Iran. China's interest in Iran's energy resources, particularly its vast oil and natural gas reserves, aligns with its goal of diversifying its energy sources and ensuring energy security. By investing in Iran's energy infrastructure, including oil and gas pipelines, refineries, and petrochemical facilities, China secures access to reliable energy supplies while also fostering long-term economic cooperation with Iran (Lixia, 2021). Moreover, these investments provide Iran with much-needed capital and technology to develop its energy sector, enhancing its capacity for oil

and gas production and export (Saraswat, 2022). Through mutually beneficial energy collaborations, China and Iran deepen their economic ties and strategic partnerships while also contributing to the broader goals of the BRI in promoting regional connectivity and economic integration (Osiewicz, 2018; Yazdani and Zeng, 2022).

Furthermore, the BRI has also fostered collaborations between China and the European Union (EU) countries. China's investments in European ports and transportation networks not only enhance connectivity between China and Europe but also strengthen China's influence in the region (European Parliament, 2023). By participating in joint infrastructure projects and promoting trade along the Maritime Silk Road, China aims to deepen its economic and strategic partnerships with EU countries, furthering its position as a global maritime power (Wu, 2020; Zhang and Lu, 2021).

Russia's Aggressive Posture

Russia's assertive actions in Eastern Europe extend into the maritime domain, particularly in regions such as the Black Sea, Mediterranean Sea, Red Sea, and the Arctic, reflecting its broader geopolitical ambitions and strategic interests (Capsaskis, 2022; Riddervold, 2023). The assertiveness witnessed in these regions aligns with Russia's history of employing intelligence agencies for various activities, including cyber-attacks and electronic warfare (Borozna, 2022). The Black Sea holds particular significance for Russia due to its access to vital sea routes and proximity to key geopolitical players like Turkey and Ukraine. By asserting control over maritime territories and enhancing its naval presence in the Black Sea, Russia aims to strengthen its influence in the region, safeguard its strategic assets, and project power beyond its immediate borders (Dalay and Sabanadze, 2024). Furthermore, Russia's activities in the Mediterranean and Red Seas are driven by its desire to establish a foothold in these critical maritime corridors, which serve as vital arteries for global trade and energy transportation. Through naval deployments, military exercises, and strategic partnerships with countries like Syria and Egypt, Russia seeks to assert its presence and influence in the Eastern Mediterranean and Red Sea regions, thereby bolstering its geopolitical position and countering Western influence (Capsaskis, 2022). Additionally, Russia's increasing presence in the Arctic reflects its ambition to exploit the region's vast natural resources, secure new Shipping routes, and assert sovereignty over strategic territories. By militarizing the Arctic and investing in infrastructure projects, Russia aims to

consolidate its control over the Northern Sea Route and establish itself as a dominant player in the emerging Arctic geopolitical landscape (Brady, 2014; Rumer et al., 2021). Overall, Russia's assertive actions in these maritime domains underscore its geopolitical aspirations and its efforts to shape regional dynamics in line with its strategic objectives.

Moreover, cyber-attacks pose a significant risk in the maritime realm, as they can target various digital systems that are integral to ship operations (Ichimura, 2022). Navigation systems, communication networks, and electronic control systems can be compromised, leading to safety concerns and potential operational disruptions (Gruner, 2021). Such disruptions may result in accidents, collisions, or navigational errors, affecting the safety of ships and seafarers. In addition, cyber-attacks can lead to significant financial losses, as Shipping schedules are delayed, and cargo delivery may be compromised (Munim et al., 2020). One notable example of a cyber-attack that affected the safety of ships and seafarers occurred in 2017 with the collision involving the USS John S. McCain, a United States Navy destroyer, and the Alnic MC, a Liberian-flagged oil tanker. The collision occurred near the Strait of Malacca, a crucial maritime chokepoint. Investigations revealed that the incident was partly caused by a cyber-attack on the USS John S. McCain's steering system. The cyber-attack led to a loss of steering control, contributing to the collision. This incident highlighted the vulnerability of maritime vessels to cyber threats and underscored the potential consequences on maritime safety when critical systems are compromised (National Transportation Safety Board, 2017).

Furthermore, electronic warfare, another concern in the maritime context, involves the use of electronic systems to jam or intercept communication and navigation signals. Russia's demonstrated capabilities in electronic warfare, such as jamming GPS signals, can disrupt the accurate positioning of ships and aircraft. This not only compromises navigation but can also create a climate of uncertainty in areas where maritime operations are conducted (Ko and Song, 2022). Such disruptions can hinder the efficient movement of goods and jeopardize the safety of ships. Subsequently, Russian Intelligence Agencies have been known to employ a wide array of tactics, including cyber-attacks and electronic warfare, in their operations. These activities often involve sophisticated techniques aimed at compromising digital and electronic systems, with the potential to disrupt navigation systems and compromise the security of ships (Gruner, 2021). Eventually 2017, a cyber-attack targeted Ukrainian ports, including the Port of Odesa and the Port of Mariupol,

disrupting operations and causing logistical challenges (Perlroth et al., 2017). Moreover, Russia's assertive stance in Eastern Europe, exemplified by the annexation of Crimea in 2014 and the war of 2022, has raised questions about how the nation may leverage its maritime power for intelligence operations. The Black Sea and the Azov Sea, in particular, have been the focal points of these tensions (Cross, 2015). Concerns regarding Russia's activities include potential disruptions to trade routes, threats to maritime infrastructure, and the broader implications for regional security and stability. These bodies of water are vital for trade and transportation, connecting Eastern Europe to global markets. However, Russia's actions, combined with its history of intelligence operations, have heightened apprehensions about the security of maritime activities in these regions.

Chinese and Russian Intelligence Threats Against Western Shipping

The possibility of China and Russia conducting intelligence operations against the Western Shipping industry has raised significant concerns recently. Both nations are vested in gathering intelligence related to maritime activities, as it offers insights into global trade patterns, supply chain vulnerabilities, and potential leverage points in economic and geopolitical negotiations. These intelligence operations extend beyond traditional espionage, encompassing various strategies such as cyber-attacks, disinformation campaigns, and geopolitical maneuvering, all aimed at securing their positions in the highly competitive realm of geopolitics.

One aspect of China's intelligence operations against the Western Shipping industry involves the country's extensive investment in port infrastructure around the world, particularly under the BRI (Russel and Berger, 2020; European Parliament, 2023). China's acquisition of ports and terminals in strategic locations provides it with a significant degree of influence over trade routes, cargo handling, and logistics (Russel and Berger, 2020; Calatayud, 2023; European Parliament, 2023; Sly and Ledur, 2023). While these investments are ostensibly commercial, they can be leveraged for intelligence-gathering purposes, as control over port facilities provides insights into the movement of goods, the companies involved, and potentially sensitive cargo (Van der Putten, 2019). Moreover, China's digital espionage capabilities, including cyber-attacks and data breaches, offer avenues to infiltrate Western Shipping companies and access proprietary information, including cargo manifests and Shipping schedules (Moreno, 2024).

In addition, Russia's intelligence operations in the Western Shipping industry take a different approach, often involving cyber-attacks. Russian state-sponsored hackers have been linked to cyber-attacks targeting Shipping companies and maritime infrastructure, seeking to disrupt operations and gain access to sensitive data (US Department of Justice, 2020). As was already mentioned, the most prominent example of such a cyber-attack is the NotPetya malware, which was attributed to Russian state-sponsored hackers. NotPetya caused widespread havoc across various industries, including maritime, by targeting critical infrastructure and disrupting operations (Greenberg, 2018). The malware infected systems globally, impacting Shipping companies like Maersk, as well as port facilities and logistics networks (Capano, 2023).

In due course, China and Russia's intelligence operations may extend beyond individual companies in the future, including geopolitical maneuvering that shapes maritime policies. This involves leveraging political and economic relationships to influence international Shipping regulations, maritime treaties, and the allocation of marine resources. For instance, both nations have contested the Arctic as a region of interest, where control over Shipping routes and access to natural resources is a key objective (Kuo, 2023; Fadeev et al., 2024). Intelligence gathering in this context could provide valuable insights into the strategies and positions of Western nations in the Arctic region, allowing China and Russia to pursue their goals effectively.

Countermeasures and Mitigation Strategies

In the complex and interconnected world of the Shipping industry, a comprehensive counterintelligence and competitive intelligence framework is crucial to safeguarding operations from myriad intelligence threats (Cloutier, 2013; Barnea, 2021). This framework extends across various facets of defensive and offensive counterintelligence, counterespionage, competitive intelligence, business environment monitoring, intelligence and security risk analysis, and insider threat detection and mitigation (Clark and Mitchell, 2019). By adopting a common counterintelligence and competitive intelligence strategy, the Shipping industry can effectively address the evolving landscape of intelligence operations while maintaining the integrity, safety, and security of its maritime activities (Cloutier, 2013; Barnea, 2021).

Counterintelligence, Counterespionage and Insider Threats

The first pillar of this comprehensive framework is defensive counterintelligence, which focuses on safeguarding the Shipping industry's digital infrastructure and sensitive information (Prunckun, 2019; Ichimura, 2022). Robust cybersecurity measures, such as state-of-the-art firewalls and intrusion detection systems, are deployed to defend against cyber threats that continue to evolve in sophistication (Clark and Mitchell, 2019; Guitton and Fréchette, 2023). Shipping companies, port authorities, and maritime service providers must fortify their defenses to protect critical digital assets (Cybersecurity and Infrastructure Security Agency, 2021). This includes employee training in cybersecurity best practices and conducting regular penetration testing and security audits to identify and rectify vulnerabilities proactively. By emphasizing a proactive defense, the Shipping industry can mitigate the risk of cyber-attacks that may target navigation systems, communication networks, and cargo manifests (Canepa, 2021).

On the contrary, offensive counterintelligence focuses on actively identifying and countering threats originating from hostile entities (Prunckun, 2019). In this context, Shipping Companies leverage threat intelligence to understand the tactics and capabilities of potential adversaries (Sims and Gerber, 2009). By proactively identifying these threats, organizations can develop countermeasures that disrupt or neutralize intelligence operations before they become a risk (Sims and Gerber, 2009). Offensive counterintelligence might involve penetration testing and covert operations, as well as the use of decoy information to mislead adversaries (Prunckun, 2019; Kanellopoulos, 2022). The goal is to create a hostile environment for intelligence operations and hinder the progress of would-be adversaries within the industry (Prunckun, 2019; Kanellopoulos, 2022).

A significant part of the offensive counterintelligence in the Shipping industry is counterespionage (Prunckun, 2019; Kanellopoulos, 2022). Its efforts are dedicated to detecting and countering espionage activities aimed at gathering sensitive information from the industry (Sims and Gerber, 2009). Monitoring for signs of espionage and implementing effective counterespionage measures are essential components of the framework. This includes the use of advanced technology to detect electronic eavesdropping or surveillance, identifying insider threats potentially working in collusion with external intelligence agencies, and scrutinizing communication networks for irregularities or potential leaks of confidential information (Cho and Lee, 2016). By employing robust counterespionage

tactics, the Shipping industry can better protect its trade secrets, operational strategies, and confidential cargo data (Dempsey et al., 2021).

Moreover, a function connected to counterespionage is insider threat detection (Prunckun, 2019; Kanellopoulos, 2024). It poses a significant challenge in the maritime sector, given the pivotal role of employees in ensuring smooth and efficient operations. A framework ensuring the detection and mitigation of insider threats is crucial for Shipping companies (Kanellopoulos, 2024). This entails implementing rigorous background checks and employee screenings to identify individuals who could potentially pose security risks. (Geman, 2009). Training programs in security awareness and best practices help employees recognize and respond to potential threats, including social engineering tactics employed by malicious actors (Sims and Gerber, 2009; Canepa, 2021). Subsequently, implementing role-based access controls and conducting regular security audits enable organizations to monitor and evaluate access patterns and privileges, thereby detecting and preventing unauthorized access. By adopting a comprehensive approach to insider threat mitigation, the Shipping industry can reduce the vulnerability of the human element to security breaches (Prunckun, 2019; Kanellopoulos, 2022; Kanellopoulos, 2024).

Competitive Intelligence and Business Environment Monitoring

Competitive intelligence and business environment monitoring stand as essential tools for companies navigating dynamic and ever-evolving industries, exemplified by the Shipping sector (Cloutier, 2013; Barnea, 2021). In an environment characterized by constant change, businesses must adopt a proactive stance in deciphering the intricate web of factors shaping their operations. Competitive intelligence, an integral facet of business environment monitoring, plays a pivotal role in this pursuit (Cloutier, 2013; Lee et al., 2014).

Going beyond a myopic focus on immediate competitors, competitive intelligence extends its reach to encompass a comprehensive analysis of the broader business environment, comprising political, economic, social, technological, environmental, and legal factors (as encapsulated in PESTEL analysis) (Cloutier, 2013; Carvalho, 2021). Within the shipping industry, this multifaceted approach has become indispensable. This intelligence pillar assumes critical importance, facilitating the anticipation of potential threats and the identification of avenues for growth and competitive advantage (Amiri et al., 2017; Emmanuelides and Tsavliris, 2019). In the increasingly interconnected world, Shipping

companies must enlist intelligence analysts to diligently track geopolitical developments (Emmanuelides and Tsavliris, 2019; Carvalho, 2021). The dynamics of geopolitics, changing trade agreements, and diplomatic relations exert direct influence over global Shipping routes and trade volumes. Adopting a proactive approach in response to these factors enables companies to refine their operational strategies, thereby improving optimization and mitigating risks (Emmanuelides and Tsavliris, 2019).

Conclusions

The changing landscape of intelligence operations in the Shipping industry underscores the critical need for a comprehensive and adaptive approach to security (Putter and Dov Bachmann, 2022). The integration of digital technology has ushered in an era of efficiency and innovation, but it has also exposed the industry to unprecedented cyber threats emanating from both state-sponsored actors and criminal organizations (Gruner, 2021). Moreover, espionage and information gathering, driven by economic and geopolitical motivations, have the potential to disrupt global trade and compromise maritime security. Insider threats further compound the complexity of safeguarding critical systems and information (Kanellopoulos, 2024).

The actions of state actors, such as China's expanding maritime presence and Russia's assertive posture, have raised significant concerns about the safety and efficiency of maritime trade in key regions. These geopolitical tensions underscore the need for a nuanced and multifaceted approach to security that combines robust cybersecurity measures, continuous employee training, and proactive risk analysis (Kallimani, 2018).

In this dynamic and interconnected maritime environment, vigilance and adaptability are paramount. Shipping companies must remain at the forefront of technology, intelligence, and security practices to protect their assets, maintain the integrity of global trade, and navigate the complex challenges of the evolving intelligence landscape. The maritime industry's ability to thrive and ensure the safe and timely delivery of goods across the world's oceans depends on its commitment to evolving countermeasures and mitigation strategies in the face of these emerging threats (Emmanuelides and Tsavliris, 2019; Putter and Dov Bachmann, 2022).

References

Abraham, S.C. (2012) *Strategic planning A practical guide for competitive success*. Bingley, U.K.: Emerald.

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

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

Amin, H., and A., Rafique (2021). 'The maritime rise of China in the Indo-Pacific and Indo-US counter balancing approach'. *Journal of Political Science and International Relations*, 4(1), 18. https://doi.org/10.11648/j.jpsir.20210401.13

Amiri, N., S., Shirkavand, M., Chalak, and N., Rezaeei (2017). 'Competitive Intelligence and developing sustainable competitive advantage.' *AD-Minister*, 173–194. https://doi.org/10.17230/ad-minister.30.9.

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

Barnea, A. (2021). 'Big Data Can Boost the Value of Competitive Intelligence'. *Competitive Intelligence Magazine*, 26(1). Available at: https://www.scip.org/page/Big-Data-Boost-Competitive-Intelligence (Accessed 24/09/2024).

Ben Farah, M., E., Ukwandu, H., Hindy, D., Brosset, M., Bures, I., Andonovic, and X., Bellekens (2022). 'Cyber security in the Maritime Industry: A systematic survey of recent advances and future trends'. *Information*, *13*(1), 22. https://doi.org/10.3390/info13010022.

Borozna, A. (2022). The Sources of Russian Foreign Policy Assertiveness. Europe-Asia Studies, 75(7), 1228-1229. https://doi.org/10.1007/978-3-030-83590-3.

Brady, A. (2014). 'Russia's Arctic strategies and the future of the Far North'. *The Polar Journal*, *4*(1), 223–223. https://doi.org/10.1080/2154896x.2014.913911.

Buszynski, L. (2021). Australia's geopolitics and the South China Sea. Security, Strategy, and Military Dynamics in South China Sea, Chapter in Security, Strategy, and Military Dynamics in the South China Sea, 267–286. https://doi.org/10.1332/policypress/9781529213454.003.0015. Available at: https://www.cambridge.org/core/books/abs/security-strategy-and-military-dynamics-in-the-south-china-sea/australias-geopolitics-and-the-south-china-sea/DE944B03538B9080A4838C7CC0A91D12. (Accessed 24/09/2024).

Calatayud, L. (2023). *The complex relationship between Europe and Chinese investment: The case of Piraeus. Lau China Institute*. King's College London, Available at: https://www.kcl.ac.uk/lci/assets/china-in-focus-piraeus-paper-final.pdf. (Accessed 24/09/2024).

Çalışkan, S. (2023, March 22). China's expanding influence in Iraq. *The Diplomat*. Available at: https://thediplomat.com/2023/03/chinas-expanding-influence-in-iraq/ (Accessed 24/09/2024).

Canepa, M., F., Ballini, D., Dalaklis, and S., Vakili (2021). *Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain*. INTED2021 Proceedings. https://doi.org/10.21125/inted.2021.0726.

Capano, D. E. (2023, September 30). Throwback attack: How notpetya ransomware took down Maersk. *Industrial Cybersecurity Pulse*. Available at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk (Accessed 24/09/2024).

Capsaskis, C., (2022). *Moscow's Strategic Obsession with the Eastern Mediterranean: Lessons from pre-Cold-War history*. Hellenic Foundation for European & Foreign Policy. Available at: https://www.eliamep.gr/wp-content/uploads/2022/06/Policy-paper-103-final.pdf (Accessed 24/09/2024).

Catrantzos, N. (2012). 'Insider Threats in the Shipping Industry'. *Maritime Security Review*, 8(2), 87-102.

Carvalho, P. (2021, June 30). Fundamentals of Competitive Intelligence (CI). *IF Insight & Foresight*. Available at: https://paulosoeirodecarvalho.medium.com/fundamentals-of-competitive-intelligence-ci-1-ebf07520746e. (Accessed 24/09/2024).

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

Chubb, A. (2022). *Dynamics of assertiveness in the south china sea China, the Philippines, and Vietnam, 1970–2015* (Vol. 99). Seattle, Washington: The National Bureau of Asian Research. Available at: https://www.nbr.org/publication/dynamics-of-assertiveness-in-the-south-china-sea-china-the-philippines-and-vietnam-1970-2015/ (Accessed 24/09/2024).

Clark, R. M. and W. L., Mitchell (2019). *Deception: Counterdeception and counterintelligence*. Washington, DC: CQ Press.

Cloutier, A. (2013). 'Competitive Intelligence Process Integrative Model based on a scoping review of the literature'. *International Journal of Strategic Management*, 13(1), 57–72. https://doi.org/10.18374/ijsm-13-1.7.

Cross, S. (2015). 'NATO–Russia security challenges in the aftermath of Ukraine conflict: Managing black sea security and beyond'. *Southeast European and Black Sea Studies*, 15(2), 151–177. https://doi.org/10.1080/14683857.2015.1060017.

Cybersecurity and Infrastructure Security Agency, (2021). *Defending Against Software Supply Chain Attacks*. Available at: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf (Accessed 24/09/2024).

Dalay, G., and N., Sabanadze, N. (2024, March 7). How geopolitical competition in the Black Sea is redefining Regional Order. *Chatham House*. Available at: https://www.chathamhouse.org/2024/03/how-geopolitical-competition-black-sea-redefining-regional-order (Accessed 24/09/2024).

Dempsey, K., V., Yan Pillitteri, and A., Regenscheid (2021). *Managing the Security of Information Exchanges*. Publication 800-47, National Institute of Standards and Technology - US Department of Commerce. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf (Accessed 24/09/2024).

Durlik, I., T., Miller, D., Cembrowska-Lech, A., Krzemińska, E., Złoczowska, and A., Nowak (2023). 'Navigating the SEA OF DATA: A comprehensive review on data analysis in maritime IOT applications'. *Applied Sciences*, *13*(17), 9742. https://doi.org/10.3390/app13179742.

Emmanuelides, G., and P., Tsavliris (2019). *Winning shipping strategies. theory and evidence from leading shipowners*. Economia Publishing.

Estay, D., (2020). *Cyber resilience for the shipping industry*. CyberShip Project. Available at: https://www.dendanskemaritimefond.dk/wp-content/uploads/2017/03/Cybership_Report_WP_5.pdf (Accessed 24/09/2024).

European Parliament (2023). *In-Depth Analysis, Security implications of China-owned critical infrastructure in the European Union*. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf (Accessed 24/09/2024).

Fadeev, A., A., Spiridonov, N., Kondratov, K., Zaikov, M., Kuprikov, and N., Kuprikov (2024). 'Energy cooperation of Russia and China in the Arctic: State and prospects'. *Polar Geography*, 1–17. https://doi.org/10.1080/1088937x.2024.2321143.

Fu, R. (2015). 'Correspondence: Looking for Asia's Security Dilemma'. *International Security*, 40(2), 181-204. https://doi.org/10.1162/ISEC_c_00220.

Gelles, M. G. (2021). *Insider threat prevention, detection, and mitigation*. Chapter in International Handbook of Threat Assessment, 669–679. https://doi.org/10.1093/med-psych/9780190940164.003.0037.

Geman Hélyette. (2009). *Risk management in commodity markets from shipping to agriculturals and Energy*. John Wiley & Sons, Ltd.

Giannakopoulou, E. N., E. I., Thalassinos, and T. V., Stamatopoulos (2016). 'Corporate governance in shipping: an overview'. *Maritime Policy & Management*, *43*(1), 19-38. https://doi.org/https://doi.org/10.1080/03088839.2015.1009185.

Grammenos, C. T. (2010). *The Handbook of Maritime Economics and Business*. Lloyd's List.

Greenberg , A. (2018, August 22). *The untold story of notpetya, the most devastating cyberattack in history*. Wired. Retrieved Available at: https://cyber-peace.org/wp-content/uploads/2018/10/The-Untold-Story-of-NotPetya-the-Most-Devastating-Cyberattack-in-History-_-WIRED.pdf (Accessed 24/09/2024).

Gruner, J. (2021). *Digital Transformation in shipping: The Hapag-Lloyd Story*. In: Seebacher, U.G. (eds) B2B Marketing. Management for Professionals. Springer, Cham. https://doi.org/10.1007/978-3-030-54292-4_23.

Guitton, M.J. and J., Fréchette (2023). 'Facing cyberthreats in a crisis and post-crisis ERA: Rethinking Security Services Response Strategy', *Computers in Human Behavior Reports*, 10, 100282. https://doi:10.1016/j.chbr.2023.100282.

Haralambides, H., E., Karakitsos, and S., Tenold (2019). *shipping and Globalization in the Post-War Era*. Palgrave Studies in Maritime Economics.

Herbert-Burns, R., and P., Lehr (2009). *Lloyd's Miu Handbook of Maritime Security*. Auerbach.

Ichimura, Y., D., Dalaklis, M., Kitada, and A., Christodoulou (2022). 'Shipping in the era of digitalization: Mapping the future strategic plans of Major Maritime Commercial Actors'. *Digital Business*, *2*(1), 100022. https://doi.org/10.1016/j.digbus.2022.100022.

Kallimani, J. G. (2018). 'The challenges of digitisation and data analysis in the maritime domain'. *Maritime Affairs: Journal of the National Maritime Foundation of India*, *14*(1), 36–50. https://doi.org/10.1080/09733159.2018.1478433.

Kaminska, M., D., Broeders, and F., Cristiano (2021). *Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone*. 13th International Conference on Cyber Conflict.

Kanellopoulos, A. N. (2022). *The Importance of Counterintelligence Culture in State Security*. Global Security and Intelligence. Note 5. Available at: https://www.buckingham.ac.uk/wp-content/uploads/2022/07/GSIN_5a.pdf (Accessed 24/09/2024).

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

Kipgen, N. (2021). *The Politics of South China Sea Disputes*. Routledge.

Ko, B., and D., Song (2022). *New Maritime Business: Uncertainty, Sustainability Technology and big data*. Springer Nature.

Kuo, M. (2023, December 20). Assessing China's and Russia's Arctic ambitions. *The Diplomat*. Available at: https://thediplomat.com/2023/12/assessing-chinas-and-russias-arctic-ambitions (Accessed 24/09/2024).

Lee, C. B., J., Wan, W., Shi, and K., Li (2014). A cross-country study of competitiveness of the shipping industry. *Transport Policy*, *35*, 366–376. https://doi.org/10.1016/j.tranpol.2014.04.010.

Lixia, Y. (2021). 'Belt and road initiative and China's energy security: Can China be more energy secured?', *Energy Security in Times of Economic Transition: Lessons from China*, 151–160. https://doi.org/10.1108/978-1-83982-464-720201007.

Lorange, P. (2020). *Innovations in shipping*. Cambridge University Press.

Luttwak, E. and B., Carson (2019, February 19). Jaw-Jaw: China's Great Power Disease. *War on the Rocks*. Available at: https://warontherocks.com/2019/02/jaw-jaw-chinas-great-power-disease (Accessed 24/09/2024).

Ministry of National Defense of the People's Republic of China, (2019). China's National Defense in the New Era, Ministry of National Defense of the People's Republic of China. Available at: https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html (Accessed 24/09/2024).

Moreno, J. E. (2024, February 22). China's hacker network: What to know. *The New York Times*. Available at: https://www.nytimes.com/2024/02/22/business/china-hack-leak-isoon.html (Accessed 24/09/2024).

Niknami, N., A., Srinivasan, K., Germain, and J., Wu (2023). 'Maritime Communications – Current State and the Future Potential with SDN and SDR'. *Network*. 3(4), 563-584. https://doi.org/10.20944/preprints202310.0880.v1.

Osiewicz, P. (2018). 'The belt and Road Initi Ati Ve (BRI): Implications for Iran-China relations. *Przegląd Strategiczny*, 11, 221–232. https://doi.org/10.14746/ps.2018.1.16.

Papasotiriou, H. (2013). *China from Heavenly Empire to the rising superpower of the 21st century*, Poiotita Publications. [in Greek]

Perlroth, N., M., Scott, and S., Frenkel (2017, June 27). Cyberattack hits Ukraine then spreads internationally. *The New York Times*. Available at: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html (Accessed 24/09/2024).

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

Putter, D. and S. D., Dov Bachmann (2022) 'Scoping the future counterintelligence focus', *International* Journal of Intelligence and CounterIntelligence, 36(2), 358–385. doi:10.1080/08850607.2022.2091414.

Raine, S. (2017). *Regional disorder the south china sea disputes*. Taylor and Francis.

Riddervold, M. (2023). 'The EU and the governance of the Maritime Global Space'. *Journal of European Integration*, *45*(8), 1143–1159. https://doi.org/10.1080/07036337.2023.2270615.

Rumer, E., R., Sokolsky and P., Stronski (2021). *Russia in the Arctic - A Critical Examination. Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/files/Rumer_et_al_Russia_in_the_Arctic.pdf (Accessed 19/03/2024).

Russel, D., and B., Berger (2020). *Weaponizing the Belt and Road Initiative. Asia Society Policy Institute*. Available at: https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf (Accessed 24/09/2024).

Saraswat, D., (2022). *Iran's Ties with China: Synergising Geoconomic Strategies*. Arab Center for Research & Policy Studies. Available at: https://www.dohainstitute.org/en/Lists/ACRPS-PDFDocumentLibrary/iran-ties-with-china-synergising-geoconomic-strategies.pdf (Accessed 24/09/2024).

Schwarz, M., M., Marx and H., Federrath (2021). *A Structured Analysis of Information Security Incidents in the Maritime Sector*. Cornell University Archives, Available at: https://arxiv.org/pdf/2112.06545.pdf (Accessed 24/09/2024).

Sims, J. E. and B. L., Gerber (2009) *Vaults, mirrors, and masks: Rediscovering US counterintelligence*. Washington, D.C.: Georgetown University Press.

Sly, L., and L., Ledur (2023, November 6). *China has acquired a global network of strategically vital ports*. The Washington Post. Available at: https://www.washingtonpost.com/world/interactive/2023/china-ports-trade-military-navy/ (Accessed 24/09/2024).

Sodhi, M. M. S., and C. S., Tang (2014). *Managing supply chain risk*. Springer.

Španja, S., A., Krajnović and J., Bosna (2017). 'Competitiveness and business strategies of shipping companies'. *Poslovna Izvrsnost - Business Excellence*, *11*(1), 123–137. https://doi.org/10.22598/pi-be/2017.11.1.123.

The Hague Centre for Strategic Studies (2019). *Geopolitics and Maritime Security*. Available at: https://hcss.nl/wp-content/uploads/2021/01/Geopolitics-and-Maritime-Security-web.pdf (Accessed 24/09/2024).

US Department of Defense (2023). *Military and Security Developments Involving the People's Republic of China*. Available at: https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF (Accessed 24/09/2024).

US Department of Justice. (2020, October 19). Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in Cyberspace. *Office of Public Affairs*. Available at: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (Accessed 24/09/2024).

US National Transportation Safety Board (2017). *Collision between US Navy Destroyer John S McCain and Tanker Alnic MC Singapore Strait, 5 Miles Northeast of Horsburgh Lighthouse August 21, 2017*. Available at: https://www.ntsb.gov/investigations/accidentreports/reports/mar1901.pdf (Accessed 24/09/2024).

Van Cleave, M. K. (2007). *Counterintelligence and national strategy*. https://doi.org/10.21236/ada471485. Available at: https://apps.dtic.mil/sti/pdfs/ADA471485.pdf. (Accessed 24/09/2024).

Van der Putten, F-P. (2019). 'European seaports and Chinese strategic influence'. *Clingendael Institute*. Available at: https://www.jstor.org/stable/pdf/resrep21415.4.pdf (Accessed 24/09/2024).

Yazdani, E., and J., Zeng (2022). 'China's Bri: A platform for Cultural Communications and exchanges with Iran'. *China and the World*, *5*(1). https://doi.org/10.1142/s2591729322500018. Available at: https://www.worldscientific.com/doi/epdf/10.1142/S2591729322500018. (Accessed 24/09/2024).