

Leveraging competitive intelligence in offensive cyber counterintelligence: An operational approach for the shipping industry

Anastasios-Nikolaos Kanellopoulos¹, Antonios Ioannidis²

¹ankanell@aueb.gr

¹  <https://orcid.org/0009-0001-1875-9264>

^{1,2}Department of Business Administration, Athens University of Economics and Business, Patision 76, 112 57, Athens, Greece

Abstract

In the contemporary landscape of rapid digitalisation, the shipping industry is increasingly confronted with unparalleled cybersecurity threats, necessitating a transition towards proactive strategies to address these evolving risks. Traditional methodologies have proven inadequate, thereby necessitating the integration of competitive intelligence (CI) within offensive cyber counterintelligence (OCCI) frameworks. This paper investigates the interdependent relationship between CI and OCCI, underscoring their combined potential to safeguard organisational interests and enhance cybersecurity resilience. The primary objectives of this study are to elucidate the foundational principles and significance of CI within business contexts, to explore the theoretical underpinnings of OCCI, and to propose a structured framework for the integration of CI into OCCI operations specifically tailored to the shipping sector. Theoretical constructs highlight the critical importance of proactive measures in mitigating cyber threats and sustaining a competitive advantage in the digital era. Through a comprehensive analysis of the literature, this interdisciplinary approach provides practitioners with the opportunity to evaluate and implement the proposed framework. The insights garnered from this study hold significant implications for both academic research and industry practice, promoting ongoing collaboration in the development of robust frameworks for integrating CI within OCCI operations.

Keywords:

strategic management, competitive intelligence, offensive counterintelligence, shipping industry, organisational resilience

Article info

Received: 26 April 2024

Revised: 12 July 2024

Accepted: 14 August 2024

Available online: 25 October 2024

Citation: Kanellopoulos A-N. and Ioannidis A. (2024) 'Leveraging competitive intelligence in offensive cyber counterintelligence: An operational approach for the shipping industry', *Security and Defence*, 48(4). doi: [10.35467/sdq/192342](https://doi.org/10.35467/sdq/192342).

Introduction

In the contemporary era characterised by rapid digitalisation, the shipping industry faces an unprecedented spectrum of cybersecurity threats. Traditional approaches to cyber counterintelligence have proven inadequate, necessitating a proactive stance from stakeholders to counteract the evolving strategies of cyber adversaries. As cyberattacks become increasingly sophisticated, targeting critical infrastructure and sensitive data, organisations within the shipping industry are increasingly vulnerable to disruptions and financial losses. Recognising the imperative to strengthen defences against such threats, industry participants are adopting innovative strategies that leverage competitive intelligence (CI) to enhance their cyber counterintelligence capabilities. CI emerges as an essential tool in this context, facilitating the anticipation, mitigation, and neutralisation of cyber threats. This paper aims to elucidate the role of CI in augmenting offensive cyber counterintelligence (OCCI) strategies within the shipping industry. By providing a comprehensive review of the literature on CI and OCCI, it presents businesses with a strategic, tactical, and operational framework to more effectively address complex cyber threats. Through an analysis of conceptual frameworks and theoretical foundations, the paper clarifies the fundamental principles and contemporary significance of CI in business contexts. Finally, it proposes that the integration of these insights can enhance the strategic capabilities of businesses in the shipping industry.

Competitive intelligence Competitive intelligence definitions

Competitive intelligence stands as a linchpin in contemporary business strategy, intricately interwoven with the dynamic and multifaceted macro business environment. Its roots can be traced back to military intelligence practices, where it initially served as a strategic tool for gaining advantage (Franco *et al.*, 2011, pp. 1–3; Greene, 1966, pp. 1–25). Over time, CI has evolved into a legal framework extensively utilised by businesses to gather, process, and analyse qualitative data pertaining to specific industries and their competitive dynamics (Carvalho, 2021). This systematic approach enables organisations to glean profound insights into competitor behaviours, customer preferences, and broader market trends, facilitating astute decision-making processes crucial for sustaining competitiveness and achieving strategic goals (Dabrowski, 2018, pp. 1–8).

Initially, scholarly discourse surrounding CI has produced a plethora of definitions, reflecting its multifaceted nature and strategic significance within organisational contexts. Sawka (1996) defines CI as the acquisition of knowledge and foresight regarding the external operational environment, underscoring its pivotal role in shaping decision-making processes and furnishing a comprehensive understanding of the business landscape. Calof (1997) elaborates on this, characterising CI as the timely dissemination of fact-based data pivotal for decision-making and strategy development. This encompasses a multifaceted approach encompassing industry analysis, competitive assessment, and benchmarking practices. Prescott (1999) extends this conceptualisation, portraying CI as an iterative process geared towards developing actionable insights into competitive dynamics and non-market forces, aiming to confer sustainable competitive advantages to organisations.

Moreover, Leibowitz (2006) underscores CI as a meticulously structured programme designed to capture, manage, and analyse intelligence, thereby enhancing the efficacy of strategic decision-making processes. McGonagle and Vella (2002) adopt a data-centric perspective, positing CI as the strategic utilisation of publicly sourced data to

glean insights into competitor behaviours and prevailing market conditions. [Dishman and Pearson \(2003\)](#) accentuate CI as a proactive endeavour aimed at amassing information and intelligence to pre-empt competitors in the cut-throat business environment. Bose (2008) portrays CI as an ongoing process of vigilantly monitoring the competitive landscape to inform strategic and operational manoeuvres effectively. In addition, within this academic tapestry, [Strauss and Du Toit \(2010\)](#) frame CI as an evolutionary assessment of business environment opportunities and developments, each carrying strategic implications for corporate decision-making endeavours. [Pellissier and Nenzhelele \(2013\)](#) contribute by conceptualising CI as a holistic process that synthesises actionable intelligence through meticulous data collection, processing, and analysis, both internally and externally. [Bouthillier and Jin \(2005\)](#) accentuate the value-added proposition of CI, emphasising its role in collecting, analysing, and disseminating intelligence within a legal framework conducive to strategic advantage.

Subsequently, the absence of a universally recognised definition of CI persists; its profound impact on organisational resilience and strategic acumen remains unequivocal, in both academic discourse and practical application. Additionally, contributions from various scholars, such as [Boncella \(2003\)](#), [Calof \(1997\)](#), and [Ettore \(1995\)](#), underscore the ethical and legal dimensions of CI, highlighting its role as a legitimate means of acquiring and leveraging CI for strategic decision-making purposes. This amalgamation of perspectives underscores the multifaceted nature of CI, illuminating its pivotal role in navigating the complexities of the contemporary business landscape and achieving sustainable competitive advantage ([Markovich *et al.*, 2022](#), pp. 8–14; [Strauss and Du Toit, 2010](#), pp. 4–8).

Competitive intelligence process

Competitive intelligence operates as a multifaceted framework designed to equip decision-makers with actionable insights essential for navigating the complexities of contemporary business environments ([Prescott, 1999](#), pp. 1–14). CI projects serve as invaluable assets in preserving organisational leadership amidst evolving landscapes by proactively identifying and managing emerging challenges and uncertainties through informed intelligence acquisition ([Aguilar, 1967](#), pp. 18–35; [Barnea, 2021](#), pp. 1–10; [Cloutier, 2013](#), pp. 1–16; [Du Toit, 2015](#), pp. 1–6; [Miller, 2001](#), pp. 1–14; [Stack, 1998](#), pp. 1–10; [Zha and Chen, 2009](#), pp. 1–5;). This process of disseminating intelligence and knowledge to executive stakeholders underscores the pivotal role of CI in shaping strategic business outcomes ([Boyd and Fulk, 1996](#), pp. 12–17; [Cottrill, 1998](#), pp. 2–5; [García-Madurga and Esteban-Navarro, 2020](#), pp. 2–16; [Pranjic, 2011](#), pp. 2–15; [Tahmasebifard, 2018](#), pp. 2–12). However, the integration of CI into organisational decision-making processes is often challenged by the reluctance of decision-makers to acknowledge the value of CI products, relying instead on personal knowledge and experiences ([Dabrowski, 2018](#), pp. 1–8; [Gaidelys and Meidute, 2012](#), pp. 1–6). Addressing the demand for CI expertise within corporations necessitates a collaborative approach, wherein CI practitioners and decision-makers actively engage in a bidirectional exchange of intelligence ([Miller, 2001](#), pp. 1–14). This symbiotic relationship hinges on management's willingness to gain insights into the business environment and CI practitioners' capacity to operate within a standardised framework ([Ghoshal and Westney, 1991](#), pp. 1–15; [Sewdass, 2012](#), pp. 1–12; [Tahmasebifard, 2018](#), pp. 2–12). Thus, CI should be conceptualised not merely as a discrete department but also as a strategic management tool integrated across organisational functions ([Ruhli and Sachs, 1997](#), pp. 1–9; [Viviers *et al.*, 2005](#), pp. 2–11).

Furthermore, CI collected from a broad spectrum of the business' external environment encompasses a range of scanning activities tailored to uncover specific market

characteristics and trends (Abraham, 2012, pp. 57–85; Babbar and Rai, 1993, pp. 1–10; Cloutier, 2013, pp. 1–16; Hedin, 2004, pp. 1–9). Gelb and Zinkhan (1985) characterise CI as a blend of defensive and offensive intelligence aimed at deciphering competitors' plans, strategies, weaknesses, and opportunities. At the heart of the CI process lie raw data and information collected for the organisation (Pirttimäki, 2007, pp. 15–23; Wright, 2010, pp. 3–6), which are transformed into actionable insights through rigorous analysis and utilisation of CI analysts' expertise (Boyd and Fulk, 1996, pp. 12–17; Cottrill, 1998, pp. 2–5; Kump et al., 2018, pp. 2–16; Sliton, 1998, p. 17; Tahmasebifard, 2018, pp. 2–12).

Moreover, CI is not solely about data collection but also about enhancing organisational value through proactive intelligence analysis that informs strategic decision-making (Auster and Choo, 1994, pp. 1–12; David, 2013, pp. 19–22; Johns and Van Doren, 2010, pp. 3–6; Johnson *et al.*, 2009, pp. 131–162; Prescott, 2001, pp. 2–14). This dynamic process involves generating intelligence products ranging from real-time alerts to strategic insights, thereby empowering organisations to anticipate market shifts and formulate informed strategies (García-Madurga and Esteban-Navarro, 2020, pp. 2–16; Porter, 1991, pp. 1–21; Seng Yap *et al.*, 2013, pp. 3–9). Additionally, the effectiveness of CI hinges not solely on resource allocation but also on the cultivation of a culture of intelligence analysis within the organisation, fostering knowledge-sharing and continuity irrespective of resource availability (Babbar and Rai, 1993, pp. 1–10; Frates and Sharp, 2005, pp. 2–10; Gaspareniene *et al.*, 2013, pp. 1–5; Miller, 2005, pp. 1–3; Peddie, 1992, pp. 1–4; Pranjic, 2011, pp. 2–15; TejAdidam *et al.*, 2009, pp. 3–15; Viviers *et al.*, 2005, pp. 2–11).

Ultimately, the success of CI processes relies on decision-makers' recognition of its value proposition and their commitment to integrating intelligence into strategic decision-making processes (Miller, 2001, pp. 1–14). By leveraging CI insights, organisations gain a competitive edge in swiftly adapting to market dynamics and making informed decisions that drive sustainable growth (Cottrill, 1998, pp. 2–5; Du Plessis and Gulwa, 2016, pp. 1–6; Kars-Unluoglu and Kevill, 2021, pp. 2–5; Tahmasebifard, 2018, pp. 2–12). The ongoing refinement of the CI process ensures that decision-makers are equipped with timely and relevant intelligence, enabling them to navigate the complexities of the business landscape with confidence and foresight (Fahey and Herring, 2007, pp. 2–8; Heppes and Du Toit, 2009, pp. 3–10; Sapkauskiene and Leitoniene, 2010, pp. 1–8). In essence, CI serves as a strategic imperative for organisations seeking to sustain a competitive advantage in an increasingly dynamic and uncertain business environment.

Understanding offensive cyber counterintelligence

Conceptual foundations

Counterintelligence operates on dual fronts, encompassing both defensive and offensive dimensions, with the overarching goal of safeguarding sensitive information and thwarting hostile activities perpetrated by adversaries (Barnea, 2017, pp. 715–726; Kanellopoulos, 2022, pp. 2–6; Prunckun, 2019, pp. 163–206; Wettering, 2000, pp. 265–300). In the realm of cybersecurity, counterintelligence assumes heightened importance, particularly due to the asymmetric nature of cyber warfare (Duvenage and Solms, 2014, pp. 5–6). On the defensive front, counterintelligence entails the implementation of robust security measures to fortify organisational defences against cyber threats (Kanellopoulos, 2023, pp. 1–6). This includes measures such as access controls, encryption protocols, and network monitoring systems aimed at detecting and mitigating potential intrusions.

By proactively identifying vulnerabilities and deploying defensive countermeasures, organisations can mitigate the risk of data breaches, espionage, and other malicious activities aimed at compromising their assets (Duvenage *et al.*, 2017, pp. 6–8).

However, defensive measures alone are insufficient to contend with the evolving threat landscape of cyber warfare. As adversaries employ increasingly sophisticated tactics to exploit vulnerabilities and infiltrate networks, a proactive approach is imperative (Sangher *et al.*, 2023, pp. 1–6; Sigholm and Bang, 2013, pp. 1–6). This is where the offensive dimension of counterintelligence comes into play. Offensive counterintelligence involves pre-emptive actions aimed at disrupting adversaries' operations, gathering intelligence on their activities, and neutralising their capabilities. This may include the infiltration of adversary networks, disinformation campaigns, and offensive cyber operations designed to degrade their infrastructure and disrupt their strategic objectives (Duvenage *et al.*, 2018, pp. 2–14).

In the context of cyber operations, offensive counterintelligence serves as a force multiplier, enabling organisations to turn the tables on adversaries and proactively defend their interests. By gathering intelligence on potential threats and adversaries' tactics, techniques, and procedures (TTPs), organisations can anticipate and pre-emptively counter malicious activities before they escalate into full-blown cyberattacks (Duvenage and Solms, 2014, pp. 7–15; Duvenage *et al.*, 2018, pp. 2–14; Svlicic *et al.*, 2019, pp. 2–12). Moreover, offensive counterintelligence allows organisations to disrupt adversaries' command and control structures, degrade their capabilities, and undermine their ability to execute coordinated cyber operations effectively (Sigholm and Bang, 2013, pp. 1–6).

For instance, real-world examples highlight the significance of OCCI in thwarting cyber threats. The Stuxnet malware, discovered in 2010, represents a paradigmatic case of offensive cyber operations deployed for counterintelligence purposes (Kaminska *et al.*, 2021, pp. 1–14). Jointly orchestrated by American and Israeli intelligence agencies, Stuxnet targeted Iran's nuclear enrichment facilities, sabotaging centrifuge equipment through sophisticated cyberattacks, showcasing how offensive cyber capabilities can disrupt adversaries' critical infrastructure (Pöyhönen and Lehto, 2022, pp. 1–9).

Moreover, OCCI incorporates elements of psychological warfare and strategic deception. Disseminating carefully crafted disinformation can sow confusion and mistrust among potential threat actors, disrupting their operations. For example, a financial institution might strategically leak false information about advanced security protocols to deter cybercriminals from targeting their systems, creating a perceived risk-reward imbalance (Cybersecurity and Infrastructure Security Agency (CISA), 2021, pp. 3–14; Kaminska *et al.*, 2021, pp. 1–14).

Additionally, the asymmetric nature of cyber warfare further underscores the importance of offensive counterintelligence. Unlike traditional warfare, where adversaries may possess comparable military capabilities, cyber warfare often pits technologically advanced actors against less equipped opponents (Jaquire and Solms, 2017, pp. 1–9). In such scenarios, offensive counterintelligence becomes a critical tool for levelling the playing field and deterring adversaries from targeting vulnerable assets (Duvenage *et al.*, 2018, pp. 2–14).

Discussion on the relationship between CI and OCCI

The interplay between OCCI and CI signifies a critical nexus within the realm of cybersecurity strategy, offering organisations a potent amalgamation to fortify their cyber

resilience. CI serves as a foundational element, providing organisations with a comprehensive understanding of their competitive landscape, encompassing the strategies, capabilities, and vulnerabilities of rival entities (Markovich *et al.*, 2022, pp. 8–14; Strauss and Du Toit, 2010, pp. 4–8). Fundamentally, the CI process entails the meticulous gathering of information and intelligence concerning the business environment, thereby forming the informational bedrock for OCCI endeavours. By leveraging insights gleaned from CI, OCCI operations can be intricately tailored to anticipate and counter emergent cyber threats effectively (Duvenage *et al.*, 2018, pp. 2–14).

To illustrate, consider a scenario where a leading technology firm invests substantially in CI efforts to ascertain the market strategies and technological advancements of its industry peers. Through its CI initiatives, the firm uncovers indications that a competitor is clandestinely engaging in cyber espionage activities, aiming to pilfer proprietary research and development data. Armed with this intelligence, the firm's OCCI team springs into action, implementing proactive measures to fortify its digital infrastructure and actively monitor for potential intrusions. Consequently, when the adversary launches a cyberattack targeting the firm's intellectual property, the OCCI defences swiftly thwart the incursion, preserving the integrity of the organisation's sensitive assets.

Moreover, the symbiotic relationship between CI and OCCI extends beyond mere defensive measures, fostering strategic advantages within competitive landscapes. By integrating CI insights into OCCI frameworks, organisations can gain a nuanced understanding of adversary tactics and methodologies, thereby pre-emptively adapting their business strategies to mitigate risks and capitalise on emerging opportunities. For instance, consider a global pharmaceutical company confronted with escalating cyber-espionage campaigns aimed at stealing proprietary drug formulas. Utilising CI, the company identifies specific threats posed by these cyberattacks and assesses their potential impact on ongoing research and product development initiatives. Armed with this intelligence, the company strategically adjusts its product development timelines, accelerating critical projects while reinforcing cybersecurity measures to safeguard its research pipeline. In response to these identified threats, the pharmaceutical company implements proactive measures, including enhanced monitoring of digital communications, robust encryption protocols, and advanced threat detection technologies. These efforts not only bolster the company's defensive capabilities against cyber threats but also enable proactive engagement with regulatory bodies to ensure compliance with data protection regulations. Subsequently, the integration of CI into OCCI frameworks allows the pharmaceutical company to more effectively anticipate competitive moves in the market. By understanding the tactics and methodologies employed by adversaries attempting to compromise their intellectual property, the company can pre-emptively adjust its market strategies. For example, insights gained from OCCI may inform decisions to expand partnerships with secure research facilities or to prioritise patent filings for new drug discoveries ahead of schedule.

Furthermore, OCCI operations can reciprocate by bolstering CI endeavours, providing valuable insights into the modus operandi of adversaries and elucidating emerging trends within the competitive landscape (García-Madurga and Esteban-Navarro, 2020, pp. 2–16; Porter, 1991, pp. 1–21; Seng Yap *et al.*, 2013, pp. 3–9). For example, a financial institution integrates OCCI findings into its CI analyses, uncovering indications of a coordinated cyberattack campaign orchestrated by a rival bank seeking to undermine customer confidence. Armed with this intelligence, the institution proactively fortifies its cybersecurity defences and enhances its customer outreach initiatives, thereby pre-empting reputational damage and consolidating its market position.

Shipping industry cyber threats

The contemporary shipping Industry exhibits an escalating reliance on interconnected digital infrastructures, rendering it inherently vulnerable to a diverse array of targeted cyber threats. These threats, ranging from ransomware attacks to phishing schemes and supply chain breaches, pose substantial risks to both shipping operations and the broader spectrum of global trade activities. The pervasive digitalisation and automation within maritime operations have rendered vessels, ports, and logistical networks particularly susceptible to exploitation by malicious entities seeking to exploit systemic vulnerabilities ([Grammenos, 2010](#), pp. 709–743). Consequently, cyber threats targeting the shipping sector can precipitate a spectrum of adverse outcomes, including the compromise of sensitive data and intellectual property as well as the disruption of critical supply chains and maritime logistics networks. Furthermore, the interconnected nature of contemporary global trade magnifies the potential ramifications of cyber incidents, as disruptions within the shipping domain have the propensity to cascade across multiple industries and economies worldwide ([Pettersson *et al.*, 2019](#), pp. 1–5). Hence, safeguarding the cybersecurity posture of the shipping industry emerges as an imperative mandate, indispensable for ensuring the resilience and continuity of international trade networks amidst the digital paradigm.

Cyber intrusions: The cases of the Automatic Identification System (AIS) manipulation and ethernet-based cyberattacks

Cyber intrusions in maritime systems, particularly the manipulation of AIS, pose significant threats to global shipping and navigation. AIS, a system designed to enhance maritime situational awareness by transmitting vessel location and identification information, is increasingly targeted by cybercriminals ([Androjna *et al.*, 2021](#)). AIS manipulation, also known as spoofing, involves transmitting false positional data to disguise a vessel's true location. This tactic is frequently employed for illicit activities, such as sanctions evasion and smuggling. The case of the Malaysian-flagged tanker *Shanaye Queen* exemplifies the dangers of AIS spoofing. In July 2023, the vessel appeared to make an impossible rapid diversion, only to later be revealed as part of a sophisticated deception to mask its loading of the US-sanctioned cargo from Iran. Such incidents expose the vulnerabilities in maritime cybersecurity, as traditional AIS systems are easily tampered with, leading to erroneous navigational data ([Lloyd's List Intelligence, 2023](#)).

Furthermore, ethernet-based cyberattacks present an additional layer of risk to shipping operations. Modern ships are equipped with numerous interconnected systems that rely on ethernet networks for communication and control, including navigation, engine management, and cargo-handling systems. These networks, if inadequately secured, provide an entry point for cybercriminals to launch attacks that can disrupt critical operations. For instance, malware introduced into a ship's ethernet network can corrupt navigational data, disable crucial systems, or even hijack control of the vessel, posing severe risks to safety and security ([Shinde and Mehta, 2023](#)).

Ransomware attacks: disrupting maritime operations

Ransomware attacks represent an enduring and formidable menace to the shipping industry, precipitating disruptive operational upheavals and profound financial repercussions. These pernicious cyber assaults entail the encryption of critical systems and data by

malevolent actors, who subsequently extort ransom payments in exchange for restoring access (Schwarz *et al.*, 2021, pp. 1–8). Notable among these incidents is the infamous 2017 NotPetya ransomware attack, which targeted Maersk, a preeminent entity within the global shipping landscape (Greenberg, 2018). This assault inflicted devastating blows upon Maersk's IT infrastructure, resulting in widespread operational disruptions across its extensive network of ports and supply chains. The reverberations of this attack extended far beyond Maersk's internal operations, reverberating across its ecosystem of partners, customers, and stakeholders reliant on its services (Estay, 2020, pp. 29–42). Port terminals grappled with protracted delays in cargo handling, vessels encountered scheduling disruptions, and supply chains grappled with acute logistical bottlenecks. Moreover, the financial toll exacted by the attack was staggering, with Maersk reporting colossal losses totalling hundreds of millions of dollars. This seminal event served as a poignant reminder of the susceptibility of maritime organisations to ransomware incursions and galvanised the industry to fortify its cybersecurity defences (CISA, 2021, pp. 3–14).

Data breaches: compromising confidentiality and integrity

The escalation of data breaches within the maritime sector presents a profound and pressing cybersecurity challenge, imperilling the confidentiality and integrity of mission-critical information essential for the industry's functioning (Ball, 2021, pp. 10–18). Of particular concern are the deleterious effects stemming from the compromise of sensitive data, encompassing cargo manifests and vessel schedules, pivotal for the seamless and secure facilitation of goods' movement (Grammenos, 2010, pp. 659–679). A notable exemplar accentuating the gravity of this threat is the 2015 breach of the US Office of Personnel Management (OPM), attributed to hackers purportedly affiliated with China (Finklea *et al.*, 2015, pp. 1–10). While the primary target of this breach was not the shipping industry *per se*, its repercussions resonated across sectors, elucidating the pervasive menace of cyber espionage and data exfiltration. The breach laid bare millions of confidential records, including background investigation files of government personnel, precipitating apprehensions regarding the susceptibility of digital infrastructures to sophisticated cyber penetrations. Although the motivations driving the OPM breach may diverge from those underpinning attacks on maritime infrastructure, such as espionage or geopolitical strategem, the fundamental cybersecurity susceptibilities underscore the interconnectedness of cyber threats spanning heterogeneous domains. Consequently, the incident serves as a poignant reminder of the imperative for maritime entities to bolster their cybersecurity resilience vis-à-vis evolving cyber adversaries.

Supply chain disruptions: impeding global trade

The interconnectedness inherent in global supply chains renders the shipping industry profoundly susceptible to supply chain disruptions orchestrated through cyber means (Alcaide and Llave, 2020, pp. 1–7). The 2017 NotPetya ransomware attack, in addition to its direct impact on Maersk, stands as a stark exemplar of the extensive repercussions of such disruptions (Estay, 2020, pp. 29–42). This incident vividly illustrated the ripple effect that cyberattacks can induce across the broader supply chain ecosystem, precipitating cascading disruptions and substantial financial losses. In the aftermath of the NotPetya attack, myriad companies reliant on Maersk's logistic services encountered severe disruptions to their operations. From manufacturing plants grappling with procuring essential components to retailers contending with delays in merchandise receipt, the reverberations resonated throughout the global economy.

Moreover, the maritime industry's dependence on interconnected networks for communication, navigation, and cargo tracking amplifies the potential impact of supply chain disruptions (Akpan *et al.*, 2022, pp. 1–10). Any disruption to these pivotal systems can precipitate cascading effects, resulting in vessel schedule delays, port congestion, and disruptions to cargo movements.

Insider threats: exploiting human vulnerabilities

Within the multifaceted and intricate realm of the shipping industry, insider threats present a formidable challenge, exploiting human vulnerabilities to compromise cybersecurity (Catrantzos, 2023, pp. 32–40). Employees across various roles, from seafarers responsible for vessel operations to administrative personnel overseeing logistics and security protocols, play pivotal roles in maritime operations but can inadvertently or intentionally compromise security (Cho and Lee, 2016, pp. 1–8). The unique nature of the maritime environment, characterised by remote locations, complex supply chains, and diverse workforce dynamics, magnifies the risk posed by insider threats (Kanellopoulos, 2024, pp. 3–9).

Social engineering tactics, such as phishing scams and pretexting, exploit human trust to gain unauthorised access to sensitive systems and information (Gelles, 2021, pp. 669–680). These tactics prey on individuals' innate desire to be helpful or their lack of awareness regarding cybersecurity's best practices (Stouder and Gallagher, 2013, pp. 2–10). For instance, a malicious actor posing as an IT technician may contact an unsuspecting employee and request their login credentials under the guise of performing urgent system maintenance or troubleshooting. In their attempt to be cooperative and helpful, the employee may unwittingly divulge sensitive information, such as login credentials or access codes, which the attacker can then exploit to gain unauthorised access to critical systems and data. Consequently, this could lead to data breaches, unauthorised access, or other security incidents, potentially compromising the integrity and confidentiality of sensitive information (Kanellopoulos, 2022, 2024, pp. 3–9).

Furthermore, infiltration by malicious insiders poses a significant risk to maritime cybersecurity (Guitton and Fréchette, 2023, pp. 2–10). In some cases, individuals may be deliberately placed within organisations by external threat actors, acting as moles to facilitate cyberattacks or espionage. Alternatively, disgruntled employees with insider knowledge and access to a shipping company's network may act independently to sabotage operations or steal sensitive data for personal gain or vendetta. These insiders may exploit their privileged access to critical systems or information to carry out malicious activities, such as stealing sensitive data, sabotaging operations, or assisting external adversaries in compromising cybersecurity defences (Kanellopoulos, 2024, pp. 3–9). For instance, a disgruntled employee with access to a shipping company's network may intentionally leak sensitive information to competitors, compromising the company's competitive advantage and reputation. Similarly, they may plant malware within the organisation's systems to disrupt operations, causing financial losses and reputational damage.

Discussion: Leveraging CI for OCCI in the shipping industry

In response to the mounting cyber threats facing the shipping industry, the development of a holistic strategy amalgamating CI and OCCI frameworks becomes imperative

(Duvenage *et al.*, 2018, pp. 2–14). This strategic blueprint entails a methodical approach at both tactical and operational levels, aimed at reinforcing cybersecurity resilience and protecting critical assets and operations within the maritime sphere (Morrow, 2021, pp. 2–10). Emphasising the pivotal role of CI, organisations delve into this domain to glean profound insights into adversaries' tactics, intentions, and capabilities (D'agostini *et al.*, 2019, pp. 1–7). Such insights serve as the cornerstone for proactive defence strategies, enabling organisations to anticipate and thwart emerging cyber threats effectively. In the following sections, we provide tactical and operational level examples of how CI could have assisted the OCCI capabilities of Maersk in response to the notorious attack against it. Within the dynamic maritime landscape, CI serves as the bedrock upon which robust offensive measures are constructed, empowering organisations to navigate the complexities of cyber warfare with precision and efficacy (Duvenage *et al.*, 2018, pp. 2–14).

Integrating threat intelligence for offensive operations

At the heart of an effective OCCI strategy lies the integration of comprehensive threat intelligence. Derived from diverse CI channels, threat intelligence provides critical insights into the TTPs employed by adversaries. This intelligence transcends the mere monitoring of an organisation's network, extending to a broader cyber sphere that includes adversarial forums, communication channels, and clandestine operations (Duvenage and Solms, 2014, pp. 7–15). Through meticulous analysis of this intelligence, organisations can uncover the underlying motives and strategies of adversaries, facilitating informed decision-making and proactive offensive measures.

In the context of the 2017 NotPetya ransomware attack on Maersk, the company could have significantly benefitted from integrating threat intelligence into its offensive operations. For instance, Maersk could have employed advanced systems, such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), to monitor and analyse incoming traffic for signs of ransomware activity. These systems, by detecting and preventing unauthorised access, also gather valuable intelligence on adversaries' behaviours and capabilities (BIMCO *et al.*, 2021, pp. 3–22). Additionally, deploying honey-client applications could have enabled Maersk to actively engage with the cyber threat landscape, luring adversaries into interacting with decoy systems, thereby revealing their tactics and tools. This proactive engagement would have allowed Maersk to identify and isolate threats more swiftly, mitigating the impact of attacks such as NotPetya.

Offensive configurations and deception strategies

One of the core components of OCCI is the strategic configuration of systems and networks to deceive and exploit adversaries. This involves setting up honeynets and other deceptive infrastructures that present false information to adversarial reconnaissance tools. For Maersk, deploying a honeynet could have diverted ransomware actors away from critical systems, channelling them into controlled environments where their actions could be monitored and analysed (Pawelski, 2023, pp. 1–7). By feeding adversaries misleading data, Maersk could manipulate their understanding of the network, causing them to make strategic errors that could be exploited.

Moreover, Maersk could have utilised honey-client applications to engage actively with adversarial tools and scripts. For example, if Maersk had deployed honey-clients that mimicked vulnerable systems, they could have attracted ransomware actors to reveal their methods and tools. This intelligence would have been invaluable for crafting targeted

countermeasures against the specific tools and techniques used by the attackers, thereby enhancing Maersk's ability to pre-empt and neutralise threats.

Recruitment and utilisation of virtual agents

A sophisticated OCCI strategy often involves the recruitment and handling of virtual agents within underground forums and adversarial networks. These agents operate under true or false flags, collecting intelligence and engaging in activities that further the organisation's objectives. For Maersk, deploying virtual agents could have involved infiltrating cybercriminal forums to gather real-time insights into adversarial plans and operations (Mraković and Vojinović, 2019, pp. 2–7). These agents could have also spread disinformation to confuse and mislead adversaries, thereby disrupting their operational effectiveness.

For instance, virtual agents could have posed as insiders within forums used by North Korean cyber actors, gathering intelligence about planned attacks and techniques. By obtaining such insights, Maersk could have pre-emptively bolstered its defences against specific threats. Additionally, these virtual agents could have influenced discussions to sow mistrust among adversaries, undermining their cohesion and operational planning. This approach has been effective in various contexts, such as countering North Korean cyber operations by proactively disrupting their communication and planning.

Cyber espionage and strategic exploitation

Cyber espionage is a critical element of OCCI, characterised by its focus on actively targeting and exploiting adversarial networks. Unlike defensive measures that protect an organisation's own systems, cyber espionage involves penetrating and gathering intelligence from adversaries' networks. For Maersk, employing cyber espionage tactics could have included monitoring North Korean cyber actors to uncover their strategic plans and operational capabilities (BIMCO *et al.*, 2021, pp. 23–25). This proactive approach would have enabled Maersk to develop targeted operations to disrupt and neutralise adversarial activities.

Effective cyber espionage requires a deep understanding of the adversarial landscape, achieved through continuous monitoring and analysis of CI. For example, Maersk could have employed advanced data mining techniques to extract valuable insights from adversarial communications, identifying patterns and correlations that reveal their intents and capabilities. This intelligence-driven approach ensures that offensive operations are precise and impactful, maximising their effectiveness in neutralising threats.

Crew management and recruitment

In the domain of crew management and recruitment within the shipping industry, utilising CI for OCCI objectives is crucial to uphold operational efficacy and safeguard security measures. Crew management is a pivotal facet of maritime endeavours, where adept personnel play a fundamental role in ensuring the seamless functioning and safety of vessels (Griffioen *et al.*, 2021, pp. 1–6). However, the recruitment process is vulnerable to cyber threats, such as those posed by Russian intelligence agencies, such as the Federal Security Service (FSB) and Sluzhba Vneshney Razvedki or Foreign Intelligence Service (SVR), which may exploit sensitive personnel data or weaknesses within recruitment platforms to infiltrate organisational networks (Kanellopoulos, 2024, pp. 3–9).

Through CI integration, Maersk could proactively address these challenges and fortify its operational resilience. For instance, by analysing competitor job postings and recruitment strategies, Maersk could identify potential vulnerabilities in their processes that adversaries might exploit. Additionally, continuous surveillance of industry trends and threat intelligence feeds would enable Maersk to anticipate and counteract cyber threats targeting crew management systems and recruitment platforms. In the event of a cyberattack on a competitor's recruitment platform, Maersk could use the insights gained to implement pre-emptive measures, mitigating the risk of similar exploitation within their systems.

Moreover, Maersk could utilise CI to counter industrial espionage by Russian state actors in the shipping industry. By monitoring and analysing the recruitment practices of competitors, Maersk could identify attempts by adversarial intelligence agencies to place operatives within the company. Implementing thorough background checks and leveraging CI to detect anomalous behaviours or affiliations would enhance Maersk's ability to safeguard against such threats.

Technology and infrastructure enhancement

The utilisation of CI guides organisations in making informed decisions regarding technology investments and infrastructure improvements. By leveraging nuanced insights derived from CI, organisations gain a comprehensive understanding of emerging cyber threats and technological advancements within the maritime sector ([Morrow, 2021](#), pp. 2–10). This knowledge empowers them to strategically employ offensive counterintelligence tactics, such as disrupting competitors' technology infrastructure or exploiting vulnerabilities in their digital systems.

For Maersk, this could have meant investing in advanced cybersecurity technologies and improving digital resilience based on CI insights. For example, understanding the specific techniques used by ransomware groups, Maersk could have enhanced its endpoint security and incident response capabilities. This strategic alignment underscores the company's proficiency in navigating the dynamic landscape of cyber threats while showcasing its commitment to maintaining a competitive edge in the industry ([ABS Group, 2021](#), pp. 2–9).

Legal and ethical considerations

As organisations venture into the domain of OCCI strategies, they encounter a plethora of ethical and regulatory complexities that necessitate careful deliberation and adherence ([VristRonn, 2016](#), pp. 2–22). Fundamental among these complexities is the obligation to uphold privacy rights and maintain rigorous data protection standards. Given that offensive cyber operations often entail the gathering and analysis of sensitive information, organisations are obligated to abide by ethical guidelines and legal frameworks to prevent unwarranted intrusions into individuals' privacy ([Duvenage and Solms, 2014](#), pp. 14–15).

Transparency emerges as a crucial component in fostering trust and ensuring accountability. Stakeholders must be informed about the nature and extent of offensive cyber activities undertaken by organisations. This openness not only builds trust but also ensures that actions taken are scrutinised and held accountable. Additionally, organisations face the challenge of navigating regulatory constraints imposed by different jurisdictions, each governed by distinct laws governing cybersecurity practices and offensive operations. Compliance with these regulations demands a meticulous approach to ensure that offensive cyber activities remain within legal and ethical boundaries ([Prunckun, 2019](#), pp. 207–218).

In grappling with these ethical considerations and regulatory hurdles, organisations must strike a delicate balance between fulfilling their cybersecurity objectives and respecting core rights and principles. Neglecting to address these considerations adequately not only exposes organisations to legal consequences but also poses risks to their reputation and undermines stakeholder's trust. Therefore, a proactive approach that integrates ethical considerations into offensive cyber strategies is imperative to mitigate risks and uphold ethical standards in the pursuit of cybersecurity goals.

This entails implementing robust mechanisms for ethical review and oversight to ensure that offensive cyber activities are conducted with due regard for ethical principles and legal requirements. Such mechanisms might include independent ethics committees, regular audits, and comprehensive reporting procedures. Moreover, organisations must prioritise ongoing education and training programmes to cultivate a culture of ethical awareness and responsibility among personnel involved in offensive cyber operations. This includes training on legal frameworks, ethical decision-making, and the potential consequences of cyber activities.

By embracing ethical considerations as integral components of offensive cyber strategies, organisations can navigate the intricate landscape of cybersecurity with integrity and accountability. This approach not only protects the organisation from legal and reputational risks but also promotes a sustainable and responsible practice of offensive cyber operations, aligning cybersecurity efforts with broader ethical standards and societal expectations.

Conclusions

This paper integrates two critical areas of literature: CI and OCCI. Through the examination of the Maersk attack case example, it initiates a broader discussion on how CI can enhance OCCI operations in the shipping industry. By analysing this specific incident, we highlight the practical application and impact of CI in real-world scenarios, illustrating how strategic intelligence gathering and analysis can significantly improve an organisation's defensive and offensive cyber capabilities.

The integration of CI within OCCI strategies is pivotal for bolstering cybersecurity resilience. Ethical principles and actionable insights from CI enable organisations to navigate the complex cyber threat landscape effectively. This study demonstrates the symbiotic relationship between CI and OCCI, highlighting their potential to safeguard organisational interests and maintain a competitive edge. The proactive use of CI allows organisations to anticipate and counter cyber threats before they materialise, thereby reducing vulnerabilities and enhancing their overall security posture.

Future research should delve deeper into the integration of CI and OCCI, exploring various cyber threat scenarios and assessing the effectiveness of different OCCI tactics. It is crucial to investigate how different industries, especially those with critical infrastructure such as shipping, can tailor these strategies to their unique threat environments. Moreover, understanding the limitations and potential risks associated with integrating CI into OCCI operations would be essential for refining these approaches.

Collaboration between academia, industry, and policymakers is essential to develop comprehensive strategies and ensure the ethical deployment of cyber counterintelligence measures. Such collaboration can facilitate the sharing of knowledge, best practices, and innovations, contributing to a more robust and resilient cybersecurity framework.

Policymakers play a vital role in establishing guidelines and regulations that support ethical practices while enabling organisations to defend against increasingly sophisticated cyber threats effectively.

Funding

This research received no external funding.

Author Contributions

Conceptualisation, A.-N.K.; formal analysis, A.-N.K.; project administration, A.N.-K.; and supervision, A.I.

Data Availability Statement

Data available on request from the authors.

Disclosure Statement

No potential conflict of interest was reported by the authors. The authors read and agreed to the published version of the manuscript.

References

- Abraham, S.C.** (2012) *Strategic planning: A practical guide for competitive success*. Leeds: Emerald Group Publishing.
- ABS Group.** (2021) *Safety, risk and compliance management – A primer in IMO cyber risk management guidelines*. Available at: https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf (Accessed: 27 March 2024).
- Adidam, P.T, Gajre, S. and Kejrival, S.** (2009) 'Cross-cultural competitive intelligence strategies', *Marketing Intelligence & Planning*, 27(5), pp. 666–680. doi: [10.1108/02634500910977881](https://doi.org/10.1108/02634500910977881).
- Aguilar, F.** (1967) *Scanning the Business Environment*. New York, NY: MacMillan.
- Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S. and Michaloliakos, M.** (2022) 'Cybersecurity challenges in the maritime sector', *Network*, 2(1), pp. 123–138. doi: [10.3390/network2010009](https://doi.org/10.3390/network2010009).
- Alcaide, J.I. and Llave, R.G.** (2020) 'Critical infrastructures cybersecurity and the maritime sector', *Transportation Research Procedia*, 45, pp. 547–554. doi: [10.1016/j.trpro.2020.03.058](https://doi.org/10.1016/j.trpro.2020.03.058).
- Androjna, A., Perkovič, M., Pavić, I. and Mišković, J.** (2021) 'AIS data vulnerability indicated by a spoofing case-study'. *Applied Sciences*, 11(11), 5015. doi: [10.3390/app11115015](https://doi.org/10.3390/app11115015).
- Auster, E. and Choo, C.W.** (1994) 'How senior managers acquire and use information in environmental scanning', *Information Processing & Management*, 30(5), pp. 607–618. doi: [10.1016/0306-4573\(94\)90073-6](https://doi.org/10.1016/0306-4573(94)90073-6).
- Babbar, S. and Rai, A.** (1993) 'Competitive intelligence for international business', *Long Range Planning*, 26(3), pp. 103–113. doi: [10.1016/0024-6301\(93\)90012-5](https://doi.org/10.1016/0024-6301(93)90012-5).
- Ball, K.** (2021) 'Electronic monitoring and surveillance in the workplace', Joint Research Center – European Commission. Available at: <https://publications.jrc.ec.europa.eu/repository/handle/JRC125716> (Accessed: 27 March 2024).
- Barnea, A.** (2017) 'Counterintelligence: Stepson of the intelligence discipline', *Israel Affairs*, 23(4), pp. 715–726. doi: [10.1080/13537121.2017.1333725](https://doi.org/10.1080/13537121.2017.1333725).
- 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: 27 March 2024).

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*. Available at: <https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf> (Accessed: 27 March 2024).

Boncella, R.J. (2003) 'Competitive intelligence and the web', *Communications of the Association for Information Systems (CAIS)*, 12(1), pp. 326–341. doi: [10.17705/1CAIS.01221](https://doi.org/10.17705/1CAIS.01221).

Bose, R. (2008) 'Competitive intelligence process and tools for intelligence analysis', *Industrial Management & Data Systems*, 108(4), pp. 510–528. doi: [10.1108/02635570810868362](https://doi.org/10.1108/02635570810868362).

Bouthillier, F. and Jin, T. (2005) 'Competitive intelligence professionals and their interactions with CI technology: A research agenda', *Journal of Competitive Intelligence and Management* (Special SCIP04 Conference Issue), 3(1), pp. 41–53.

Boyd, B.K. and Fulk, J. (1996) 'Executive scanning and perceived uncertainty: A multidimensional model', *Journal of Management*, 22(1), pp. 1–21. doi: [10.1177/014920639602200101](https://doi.org/10.1177/014920639602200101).

Calof, J. (1997) 'For king and country and company', *Business Quarterly*, 61(1), pp. 32–39.

de Carvalho, P.S. (2021) 'Fundamentals of competitive intelligence (CI)'. *IF Insight & Foresight*. Available at: <https://paulosoeirodecavvalho.medium.com/fundamentals-of-competitive-intelligence-ci-1-ebf07520746e> (Accessed: 27 March 2024).

Catrantzios, N. (2023) *Managing the insider threat no dark corners and the rising tide menace*. Boca Raton, FL: 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. doi: [10.1080/10798587.2015.1121617](https://doi.org/10.1080/10798587.2015.1121617).

Cloutier, A. (2013) 'Competitive intelligence process integrative model based on a scoping review of the literature', *International Journal of Strategic Management*, 13(1), pp. 57–72. doi: [10.18374/ijism-13-1.7](https://doi.org/10.18374/ijism-13-1.7).

Cottrill, K. (1998) 'Turning competitive intelligence into business knowledge', *Journal of Business Strategy*, 19(4), pp. 27–30. doi: [10.1108/eb039948](https://doi.org/10.1108/eb039948).

Cybersecurity and Infrastructure Security Agency (CISA). (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: 27 March 2024).

Dabrowski, D. (2018) 'Sources of market information, its quality and new product financial performance', *Engineering Economics*, 29(1), pp. 115–122. doi: [10.5755/j01.ee.29.1.13405](https://doi.org/10.5755/j01.ee.29.1.13405).

D'agostini, E., Nam, H.-S. and Kang, S.-H. (2019) 'Gaining competitive advantage at sea: An overview of shipping lines' strategic decisions', *International Journal of Transportation Engineering and Technology*, 5(4), p. 74. doi: [10.11648/j.ijtet.20190504.12](https://doi.org/10.11648/j.ijtet.20190504.12).

David, F.R. (2013) *Strategic management concepts and cases: A competitive advantage approach*. London: Pearson.

- Dishman, P. and Pearson, T.** (2003) 'Assessing intelligence as learning within an industrial marketing group: A pilot study', *Industrial Marketing Management*, 32(7), pp. 615–620. doi: [10.1016/s0019-8501\(03\)00030-0](https://doi.org/10.1016/s0019-8501(03)00030-0).
- Du Plessis, T. and Gulwa, M.** (2016) 'Developing a competitive intelligence strategy framework supporting the competitive intelligence needs of a financial institution's decision makers', *SA Journal of Information Management*, 18(2), pp. 2–8. doi: [10.4102/sajim.v18i2.726](https://doi.org/10.4102/sajim.v18i2.726).
- Du Toit, A.S.A.** (2015) 'Competitive intelligence research: An investigation of trends in the literature', *Journal of Intelligence Studies in Business*, 5(2), pp. 14–21. doi: [10.37380/jisib.v5i2.127](https://doi.org/10.37380/jisib.v5i2.127).
- Duvenage, P., Jaquire, V. and Solms, S.** (2018) 'Towards a literature review on cyber counterintelligence', *Journal of Information Warfare*, 17(4), pp. 284–297. Available at: <https://www.jstor.org/stable/26783824> (Accessed: 27 March 2024).
- Duvenage, P., Sithole, T. and Solms, S.** (2017) 'A conceptual framework for cyber counterintelligence – Theory that really matters', in *16th European conference in cyber warfare and security*. Available at: https://www.cybersecurity.org.za/docs/ECCWS_2017_DSV_Prof_MS.pdf (Accessed: 27 March 2024).
- Duvenage, P. and Solms, S.** (2014) 'Putting counterintelligence in cyber counterintelligence', in Adrew Liaropoulos and George Tsihrintzis (Eds.) *13th European conference on cyber warfare and security*. Available at: https://www.researchgate.net/publication/328732134_Putting_Counterintelligence_in_Cyber_Counterintelligence (Accessed: 27 March 2024).
- Estay, D.** (2020) 'Cyber resilience for the shipping industry', CyberShip Project. Available at: https://www.dendanske.maritimefond.dk/wp-content/uploads/2017/03/Cybership_Report_WP_5.pdf (Accessed: 27 March 2024).
- Ettore, B.** (1995) 'Managing competitive intelligence', *Management Review*, 10, pp. 15–19. Available at: <https://go.gale.com/ps/i.do?id=GALE%7CA17551795&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00251895&p=AONE&sw=w&userGroupName=anon%7E68ba059b&aty=open-web-entry> (Accessed: 27 March 2024).
- Fahey, L. and Herring, J.** (2007) 'Intelligence teams', *Strategy & Leadership*, 35(1), pp. 13–20. doi: [10.1108/10878570710717245](https://doi.org/10.1108/10878570710717245).
- Finklea, K., Christensen, M., Fischer, E., Lawrence, S. and Catherine, T.** (2015) 'Cyber intrusion into U.S. office of personnel management: In brief', Congressional Research Service. Available at: <https://sgp.fas.org/crs/natsec/R44111.pdf> (Accessed: 27 March 2024).
- Franco, M., Magrinho, A. and Ramos Silva, J.** (2011) 'Competitive intelligence: A research model tested on Portuguese firms', *Business Process Management Journal*, 17(2), pp. 332–356. doi: [10.1108/14637151111122374](https://doi.org/10.1108/14637151111122374).
- Frates, J. and Sharp, S.** (2005) 'Using business intelligence to discover new market opportunities', *Journal of Competitive Intelligence and Management*, 3(3), pp. 16–28. Available at: <https://www.sharpmarket.com/wp-content/pdfs/article-new-market-opps.pdf> (Accessed: 27 March 2024).
- Gaidelys, V. and Meidute, I.** (2012) 'Instruments and methods of competitive intelligence', *Economics and Management*, 17(3), pp. 971–977. doi: [10.5755/j01.em.17.3.2122](https://doi.org/10.5755/j01.em.17.3.2122).
- García-Madurga, M. and Esteban-Navarro, M.** (2020) 'A project management approach to competitive intelligence', *Journal of Intelligence Studies in Business*, 10(3), pp. 9–23. doi: [10.37380/jisib.v10i3.636](https://doi.org/10.37380/jisib.v10i3.636).
- Gaspareniene, L., Remeikiene, R. and Gaidelys, V.** (2013) 'The opportunities of the use of competitive intelligence in business: Literature review', *Journal of Small Business and Entrepreneurship Development*, 1(2), pp. 9–16.

- Gelb, B. and Zinkhan, G.** (1985) 'Competitive intelligence practices of industrial marketers', *Industrial Marketing Management*, 14, pp. 269–275. doi: [10.1016/0019-8501\(85\)90019-7](https://doi.org/10.1016/0019-8501(85)90019-7).
- Gelles, M.G.** (2021) 'Insider threat prevention, detection, and mitigation: Building an insider threat program', in J. Reid Meloy, Jens Hoffmann (Eds.) *International handbook of threat assessment*, 2 edn, New York: Oxford Academic, pp. 669–679. doi: [10.1093/med-psych/9780190940164.003.0037](https://doi.org/10.1093/med-psych/9780190940164.003.0037).
- Ghoshal, S. and Westney, D.E.** (1991) 'Organizing competitor analysis systems', *Strategic Management Journal*, 12(1), pp. 17–31. doi: [10.1002/smj.4250120103](https://doi.org/10.1002/smj.4250120103).
- Grammenos, Th. C.** (2010) *The Handbook of maritime economics and business*. Lloyd's list. London Informa Law PLC.
- Greenberg, A.** (2018, August 22) *The untold story of notpetya, the most devastating cyberattack in history*. 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: 27 March 2024).
- Greene, R.** (1966) *Business intelligence and espionage*. Homewood, IL: Dow Jones-Irwin.
- Griffioen, J., van der Drift, M. and van den Broek, H.** (2021) 'Enhancing maritime crew resource management training by applying resilience engineering: A case study of the bachelor maritime officer training programme in Rotterdam', *Education Sciences*, 11(8), p. 378–389. doi: [10.3390/educsci11080378](https://doi.org/10.3390/educsci11080378).
- Guitton, M.J. and J., Fr chette** (2023) 'Facing cyberthreats in a crisis and post-crisis ERA: Rethinking security services response strategy', *Computers in Human Behavior Reports*, 10, p. 100282. doi: [10.1016/j.chbr.2023.100282](https://doi.org/10.1016/j.chbr.2023.100282).
- Hedin, H.** (2004) 'Introduction to competitive intelligence (1/2004)', *GIA white paper*. Available at: https://www.academia.edu/33107462/INTRODUCTION_TO_COMPETITIVE_INTELLIGENCE (Accessed: 27 March 2024).
- Heppes, D. and Du Toit, A.** (2009) 'Level of maturity of the competitive intelligence function', *Aslib Proceedings*, 61(1), pp. 48–66. doi: [10.1108/00012530910932285](https://doi.org/10.1108/00012530910932285).
- Jaquire, V. and von Solms, S.** (2017) 'Towards a cyber counterintelligence maturity model', in Juan R. Lopez, Adam R. Bryant, Robert F. Mills (Eds.) *Proceedings of the 12th international conference on cyber warfare and security*. Available at: <https://adam.uj.ac.za/csi/docs/Jaquire%20&%20von%20Solms%20-%20Towards%20a%20Cyber%20Counterintelligence%20Maturity%20Model.pdf> (Accessed: 27 March 2024).
- Johns, P. and Van Doren, D.C.** (2010) 'Competitive intelligence in service marketing', *Marketing Intelligence & Planning*, 28(5), pp. 551–570. doi: [10.1108/02634501011066492](https://doi.org/10.1108/02634501011066492).
- Johnson, G., Scholes, K. and Whittington, R.** (2009) *Exploring corporate strategy*. Essex: Pearson Education.
- Kaminska, M., Broeders, D. and Cristiano, F.** (2021) 'Limiting viral spread: Automated cyber operations and the principles of distinction and discrimination in the grey zone', in *13th International conference on cyber conflict*. Available at: <https://ieeexplore.ieee.org/document/9468290> (Accessed: 27 March 2024).
- 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: 27 March 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), pp. 10–19. doi: [10.37868/dss.v5.id261](https://doi.org/10.37868/dss.v5.id261).
- Kanellopoulos, A.N. and Ioannidis, A.** (2023) 'The dimensions of counterintelligence and their role in national security', *Journal of European and American Intelligence Studies*, 6(2), pp. 85–104.
- Kars-Unluoglu, S. and Kevill, A.** (2021) 'Emotional foundations of capability development: An exploration in the SME context', *Journal of Management & Organization*, 27(4), pp. 1–20. doi: [10.1017/jmo.2020.38](https://doi.org/10.1017/jmo.2020.38).
- Kump, B., Engelmann, A., Kessler, A. and Schweiger, C.** (2018) 'Toward a dynamic capabilities scale: Measuring organizational sensing, seizing, and transforming capacities', *Industrial and Corporate Change*, 28(5), pp. 1149–1172. doi: [10.1093/icc/dty054](https://doi.org/10.1093/icc/dty054).
- Leibowitz, J.** (2006) *Strategic intelligence: Business intelligence, competitive intelligence, and knowledge management*. Boca Raton, FL: Auerbach Publications.
- Lloyd's List Intelligence.** (2023) *The case of the Shanaye queen*. Available at: <https://www.lloydslistintelligence.com/knowledge-hub/risk-and-compliance/the-case-of-the-shanaye-queen> (Accessed: 9 July 2024).
- Markovich, A., Raban, D.R. and Efrat, K.** (2022) 'Tailoring competitive information sources to the sequence of dynamic capabilities', *Journal of Management & Organization*, 28(3), pp. 480–501. doi: [10.1017/jmo.2022.35](https://doi.org/10.1017/jmo.2022.35).
- McGonagle, J.J. and Vella, C.M.** (2002) *Bottom line competitive intelligence*. Westport, CT: Quorum Books.
- Miller, S.** (2001) 'Competitive intelligence – An overview', *Society of Competitive Intelligence Professionals*, pp. 1–14.
- Miller, J.P.** (2005) 'Information science and competitive intelligence: Possible collaborators?', *Bulletin of the American Society for Information Science and Technology*, 23(1), pp. 11–13. doi: [10.1002/bult.33](https://doi.org/10.1002/bult.33).
- Morrow, A.B.** (2021) 'Information security and cyber threats and vulnerabilities', in Gordon G.A. and Young R.Y. (Eds.) *Intermodal Maritime Security: Supply Chain Risk Mitigation*, Amsterdam: The Netherlands, pp. 169–193. doi: [10.1016/b978-0-12-819945-9.00010-1](https://doi.org/10.1016/b978-0-12-819945-9.00010-1).
- Mraković, I. and Vojinović, R.** (2019) 'Maritime cyber security analysis – How to reduce threats?', *Transactions on Maritime Science*, 8(1), pp. 132–139. doi: [10.7225/toms.v08.n01.013](https://doi.org/10.7225/toms.v08.n01.013).
- Pawelski, J.** (2023) 'Cyber threats for present and future commercial shipping', *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 17(2), pp. 261–267. doi: [10.12716/1001.17.02.01](https://doi.org/10.12716/1001.17.02.01).
- Peddie, J.** (1992) 'The corporate culture and use of competitive intelligence', *Competitive Intelligence Review*, 3(1), pp. 7–10. doi: [10.1002/cir.3880030104](https://doi.org/10.1002/cir.3880030104).
- Pellissier, R. and Nenzhelele, T.E.** (2013) 'Towards a universal definition of competitive intelligence', *SJ Journal of Information Management*, 15(2), pp. 559–566. doi: [10.4102/sajim.v15i2.559](https://doi.org/10.4102/sajim.v15i2.559).
- Petersson, N.P., Tenold, S. and White, N.J.** (2019) *Shipping and globalization in the post-war era*. Palgrave Studies in Maritime Economics. New York, NY: Springer.
- Pirttimäki, V.** (2007) *Business intelligence as a managerial tool in large Finnish companies*. Doctoral thesis. Tampere: Tampere University of Technology (TUT). Available at: <https://trepo.tuni.fi/handle/10024/114315> (Accessed: 27 March 2024).
- Porter, M.** (1991) 'Towards a dynamic theory of strategy', *Strategic Management Journal*, 12(S2), pp. 95–117. doi: [10.1002/smj.4250121008](https://doi.org/10.1002/smj.4250121008).

- Pöyhönen, J. and Lehto, M.** (2022) 'Assessment of cybersecurity risks: Maritime automated piloting process', *International Conference on Cyber Warfare and Security*, 17(1), pp. 262–271. doi: [10.34190/iccws.17.1.18](https://doi.org/10.34190/iccws.17.1.18).
- Pranjic, G.** (2011) 'Influence of business and competitive intelligence on making right business decisions', *Ekonomiska Misao Praksa*, 20(1), pp. 271–288. Available at: <https://hrcak.srce.hr/69721> (Accessed: 27 March 2024).
- Prescott, J.** (1999) 'The evolution of competitive intelligence: Designing a process for action', *APMP Professional Journal*, pp. 37–52.
- Prescott, J.E.** (2001) 'Competitive intelligence: Lessons from the trenches', *Competitive Intelligence Review*, 12(2), pp. 5–19. doi: [10.1002/cir.1013](https://doi.org/10.1002/cir.1013).
- Prunckun, H.** (2019) *Counterintelligence theory and practise*. New York, NY: Rowman & Littlefield.
- Ruhli, E. and Sachs, S.** (1997) 'Challenges for strategic competitive intelligence at the corporate level', *Competitive Intelligence Review*, 8(4), pp. 54–64. doi: [10.1002/\(sici\)1520-6386\(199724\)8:4<54::aid-cir9>3.0.co;2-s](https://doi.org/10.1002/(sici)1520-6386(199724)8:4<54::aid-cir9>3.0.co;2-s).
- Sangher, K.S., Singh, A., Pandey, H.M. and Kumar, V.** (2023) 'Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for dark web forum content by identifying cybercrimes', *Information*, 14(6), p. 349. doi: [10.3390/info14060349](https://doi.org/10.3390/info14060349).
- Sapkauskiene, A. and Leitoniene, S.** (2010) 'The concept of time-based competition in the context of management theory', *Inzinerine Ekonomika (Engineering Economics)*, 21(2), pp. 205–2013. Available at: <https://epubl.ktu.edu/object/elaba:3041519/> (Accessed: 27 March 2024).
- Sawka, K.** (1996) 'Demystifying competitive intelligence', *Management Review*, 85(10), pp. 47–51. Available at: <https://go.gale.com/ps/i.do?id=GALE%7CA18730946&sid=googleScholar&v=2.1&it=r&link-access=abs&issn=00251895&p=AONE&sw=w&userGroupName=anon%7Efe57ae9&aty=open-web-entry> (Accessed: 27 March 2024).
- Schwarz, M., Marx, M. and Federrath, H.** (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: 27 March 2024).
- Seng Yap, C., Zabid Abdul Rashid, M. and Amat Sapuan, D.** (2013) 'Perceived environmental uncertainty and competitive intelligence practices', *VINE*, 43(4), pp. 462–481. doi: [10.1108/vine-11-2011-0058](https://doi.org/10.1108/vine-11-2011-0058).
- Sewdass, N.** (2012) 'Proposing a competitive intelligence (CI) framework for public service departments to enhance service delivery', *SA Journal of Information Management*, 14(1), pp. 1–13. doi: [10.4102/sajim.v14i1.491](https://doi.org/10.4102/sajim.v14i1.491).
- Shinde, S. and Mehta, H.** (2023) 'Defending marine ships against ethernet based cyberattacks', in *2023 Fifth international conference on electrical, computer and communication technologies (ICECCT)*. New York, NY: IEEE. doi: [10.1109/icecct56650.2023.10179830](https://doi.org/10.1109/icecct56650.2023.10179830).
- Sigholm, J. and Bang, M.** (2013) 'Towards offensive cyber counterintelligence', in *2013 European intelligence and security informatics conference*, pp. 166–171. doi: [10.1109/EISIC.2013.37](https://doi.org/10.1109/EISIC.2013.37).
- Sliton, P.** (1998) 'Society of competitive intelligence professionals, various proceedings and publications', *Competitive Review*, 9(2), pp. 4–9.
- Stack, K.P.** (1998) 'Competitive intelligence', *Intelligence and National Security*, 13(4), pp. 194–202. doi: [10.1080/02684529808432511](https://doi.org/10.1080/02684529808432511).

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

Strauss, A. and Du Toit, A. (2010) 'Skills shortages and competitiveness in South Africa: The need for competitive intelligence skills', *Journal of Contemporary Management*, 7, pp. 307–324.

Svilicic, B., Kamahara, J., Rooks, M. and Yano, Y. (2019) 'Maritime cyber risk management: An experimental ship assessment', *Journal of Navigation*, 72(5), pp. 1108–1120. doi: [10.1017/s0373463318001157](https://doi.org/10.1017/s0373463318001157).

Tahmasebifard, H. (2018) 'The role of competitive intelligence and its sub-types on achieving market performance', *Cogent Business & Management*, 5(1), p. 1540073. doi: [10.1080/23311975.2018.1540073](https://doi.org/10.1080/23311975.2018.1540073).

Viviers, W., Saayman, A. and Muller, M.L. (2005) 'Enhancing a competitive intelligence culture in South Africa', *International Journal of Social Economics*, 32(7), pp. 576–589. doi: [10.1108/03068290510601117](https://doi.org/10.1108/03068290510601117).

VristRonn, K. (2016) 'Intelligence ethics: A critical review and future perspectives', *International Journal of Intelligence and Counterintelligence*, 29(4), pp. 760–784. doi: [10.1080/08850607.2016.1177399](https://doi.org/10.1080/08850607.2016.1177399).

Wettering, F. (2000) 'Counterintelligence: The broken triad', *International Journal of Intelligence and Counterintelligence*, 13(3), pp. 265–300. doi: [10.1080/08850600050140607](https://doi.org/10.1080/08850600050140607).

Wright, S. (2010) 'Capitalising on intelligence: Converting input to output to insight and competitive advantage', *Journal of Strategic Marketing*, 18(7), pp. 517–521. doi: [10.1080/0965254x.2010.529159](https://doi.org/10.1080/0965254x.2010.529159).

Zha, X. and Chen, M. (2009) 'Competitive intelligence monitoring in the risk prevention of SMES', *Journal of Service Science and Management*, 02(03), pp. 230–235. doi: [10.4236/jssm.2009.23028](https://doi.org/10.4236/jssm.2009.23028).