ENHANCING CYBER SECURITY AND COUNTERINTELLIGENCE IN THE SHIPPING INDUSTRY

DOI: https://doi.org/ 10.37458/nstf.25.1.6

Review paper

Anastasios-Nikolaos Kanellopoulos*

Abstract: The contemporary cyber threat landscape presents a complex tapestry of challenges, featuring diverse actors ranging from non-state entities like organized crime syndicates and terrorist organizations to state-sponsored operatives affiliated with nations such as China, Russia, and Iran. Motivations driving these actors span from financial gain to ideological pursuits and geopolitical objectives, resulting in a wide range of cyber operations aimed at individuals, businesses, and governments worldwide. These high-profile incidents underscore the disruptive potential, and strategic implications need of a comprehensive Shipping Industry's Cyber Counterintelligence approach, to safeguard critical assets and operations in an increasingly digitized environment.

Keywords: Cyber Counterintelligence, Shipping Industry, Cyber Threats, Maritime Security.

* Anastasios-Nikolaos Kanellopoulos is a PhD Candidate in Business Intelligence, Athens University of Economics and Business, Greece, MSc in International Relations, Strategy and Security, University Neapolis Pafos, Cyprus & BA in Business Administration, Athens University of Economics and Business, Greece, Frontex CIRAM Analyst Certified. He can be contacted at ankanell@aueb.gr

Introduction

The contemporary landscape of cyber threats presents a multifaceted array of challenges, characterized by the involvement of diverse actors ranging from non-state entities like organized crime syndicates and terrorist organizations to state-sponsored operatives affiliated with nations such as China, Russia, and Iran. Motivations driving these actors span from financial gain to ideological pursuits and geopolitical objectives, resulting in a wide range of cyber operations aimed at individuals, businesses, and governments worldwide. High-profile incidents such as the ransomware attack on the Colonial Pipeline and state-sponsored campaigns like the breach of the U.S. Office of Personnel Management underscore the disruptive potential and strategic implications of cyber operations conducted by both non-state and state actors. Moreover, the convergence of cyber and physical threats, exemplified by incidents like the Stuxnet worm attack, highlights the profound ramifications of cyber-physical attacks on critical infrastructure and public safety. Additionally, the proliferation of disinformation and cyber-enabled influence operations by state actors further complicates the cybersecurity landscape, posing challenges to democratic processes and societal cohesion.

Within the maritime domain, cyber threats manifest in various forms, including tampering with navigation systems, ransomware attacks targeting shipping operations, and theft of sensitive cargo information. Eventually, incidents such as the 2017 NotPetya ransomware attack on the Port of Rotterdam underscore the susceptibility of maritime infrastructure to cyber-attacks, with significant implications for global trade and supply chain integrity. Furthermore, the exploitation of digital technologies in shipping operations introduces novel attack vectors and vulnerabilities, necessitating comprehensive Cyber Counterintelligence (CCI) strategies.

In response, the adoption of CCI emerges as a cornerstone operational approach for safeguarding maritime operations against cyber threats. Leveraging continuous surveillance, proactive threat intelligence collection, systematic vulnerability assessments, and meticulous threat actor profiling, maritime organizations can bolster their resilience and readiness to mitigate cyber threats effectively. Employee training initiatives, incident response preparedness, and collaborative information-sharing frameworks further fortify cyber defense postures. By integrating these operational choices into a cohesive CCI strategy, maritime entities can navigate the intricate cyber threat landscape with enhanced resilience and adaptability, safeguarding critical maritime assets and operations in an increasingly digitized environment.

Cyber Threats Environment and Trends

The cyber threat landscape presents a multifaceted array of challenges, spanning from non-state actors such as hackers from Serious Organized Crime and Terrorist organizations like Albanian Organized Crime, Hezbollah, and Al-Qaeda to state-sponsored actors such as China, Russia, and Iran. Non-state actors, often motivated by financial gain, ideological motives, or geopolitical agendas, engage in a wide range of cyber-attacks, illustrating the diverse nature of cyber threats in the contemporary digital era (Bendovschi, 2015; Prunckun, 2018; Pöyhönen and Lehto, 2022).

For instance, the notorious hacker group known as "DarkSide" gained global attention in 2021 for their ransomware attack on Colonial Pipeline, disrupting fuel supplies along the East Coast of the United States (Congressional Research Service, 2021). This incident highlighted the significant risks posed by non-state actors, who exploit vulnerabilities in software and networks to infiltrate target systems, steal sensitive information, or

disrupt critical infrastructure, thereby posing a substantial threat to individuals, businesses, and governments worldwide (Rudner, 2008; Alcaide, and Llave, 2020).

In addition, state-sponsored cyber operations represent another dimension of the cyber threat landscape, with countries like China, Russia, and Iran leveraging their cyber capabilities for espionage, sabotage, and geopolitical influence. China, occasionally, has been implicated in numerous cyber espionage campaigns targeting intellectual property and sensitive government information (Jensen, 2023). One prominent case involved the breach of the U.S. Office of Personnel Management in 2015, where hackers believed to be linked to China stole millions of sensitive records, including background investigation files of government employees (Finklea et al., 2015). Similarly, Russia has gained notoriety for its aggressive cyber activities, ranging from interference in elections to disinformation campaigns and cyber-attacks against critical infrastructure in other countries. The 2017 NotPetya cyber-attack, widely attributed to Russian hackers, crippled computer systems worldwide, causing billions of dollars in damages to businesses and governments (Cybersecurity and Infrastructure Security Agency, 2021; Kaminska et al., 2021). Likewise, Iran has conducted cyber operations targeting government agencies, financial institutions, and critical infrastructure, often in response to geopolitical tensions or perceived threats to its national security. The 2012 Shamoon malware attack against Saudi Aramco, attributed to Iranian hackers, disrupted oil production by destroying thousands of computers (Alshathry, 2017).

Moreover, the intersection of cyber and physical threats presents additional challenges, as adversaries exploit vulnerabilities in control systems and industrial infrastructure to cause physical harm or disrupt essential services (Prunckun, 2018). Cyber-physical attacks, exemplified by

incidents like the Stuxnet worm, highlight the potential for malicious actors to manipulate physical systems through cyber means, with potentially catastrophic consequences for public safety and national security (Bendovschi, 2015; Kaminska et al., 2021). The Stuxnet worm, discovered in 2010, targeted Iran's nuclear enrichment facilities, causing physical damage to centrifuges by exploiting vulnerabilities in industrial control systems (Kaminska et al., 2021). This unprecedented cyber-physical attack demonstrated the ability of sophisticated adversaries to blend digital and physical warfare tactics, underscoring the evolving nature of cyber threats in the modern era (Pöyhönen and Lehto, 2022).

Furthermore, the proliferation of social media platforms and online communication channels has facilitated the spread of disinformation, propaganda, and cyber-enabled influence operations, with state-sponsored actors like China, Russia, and Iran exploiting these platforms to manipulate public opinion, sow discord, and undermine democratic institutions (Andriukaitis et al., 2021). These influence operations pose significant challenges to the integrity of democratic processes, public discourse, and societal cohesion, highlighting the need for robust countermeasures to combat disinformation and protect the integrity of online information ecosystems. The prevalence of state-sponsored disinformation campaigns, such as Russia's efforts to interfere in the 2016 U.S. presidential election through social media manipulation and propaganda, underscores the growing importance of addressing the weaponization of information in cyberspace (Mueller, R., 2019).

Implication of Cyber Threats on Shipping Operations

The Shipping Industry is increasingly reliant on interconnected digital systems, making it susceptible to a wide range of specific cyber threats that can have severe consequences for Shipping operations and global trade

(Grammenos, 2010; Petersson et al., 2019). One significant threat facing the industry is the potential for cyber-attacks targeting Shipping navigation systems, which could lead to vessel collisions, groundings, or other navigational hazards (Bendovschi, 2015; Giannakopoulou, 2018; Akpan et al., 2022; Ben Farah, 2022). Moreover, ransomware attacks targeting shipping companies' IT systems can cripple operations by encrypting critical data and systems, leading to operational downtime and financial losses (Alcaide, and Llave, 2020).

Eventually, the 2017 NotPetya ransomware attack disrupted operations at the Port of Rotterdam, one of the world's busiest ports, highlighting the vulnerability of critical Shipping infrastructure to cyber incidents. This attack caused significant delays and financial losses for shipping companies and port operators, underscoring the potential impact of cyber threats on the smooth functioning of global supply chains. In the same incident, Maersk reported losses of hundreds of millions of dollars as a result of the attack, highlighting the significant financial and operational risks posed by cyber threats to the Shipping industry (Estay, 2020; Cybersecurity and Infrastructure Security Agency, 2021; Kaminska et al., 2021).

In addition to ransomware attacks, the Shipping Industry faces threats related to the theft of sensitive cargo information (Grammenos, 2010; Bendovschi, 2015; Petersson et al., 2019). Malicious actors may target shipping companies' databases to steal manifests, routes, and cargo contents, which can be exploited for economic gain or sabotage. For example, cybercriminals could use stolen cargo information to orchestrate thefts or hijackings of high-value goods, posing security risks to vessels and crew members. Moreover, the unauthorized disclosure of cargo information could disrupt supply chains, delay deliveries, and compromise the

confidentiality of sensitive shipments, undermining trust and confidence in the shipping industry (Loomis et al., 2021).

Furthermore, the increasing adoption of digital technologies in Shipping operations, such as electronic navigation systems, cargo tracking systems, and automated port terminals, introduces new attack vectors and vulnerabilities that threat actors can exploit (Sen, 2016; Giannakopoulou, 2018; Pöyhönen and Lehto, 2022; Ben Farah, 2022). For instance, cyber-attacks targeting electronic navigation systems could manipulate vessel routes or falsify GPS signals, leading to navigational errors or deliberate misdirection of vessels (Bendovschi, 2015; Akpan et al., 2022). Similarly, disruptions to cargo tracking systems could result in the loss or misplacement of shipments, causing financial losses and reputational damage for Shipping companies and logistics providers (Svilicic et al., 2019).

Besides, the Shipping Industry also faces cyber threats from state-sponsored actors seeking to gain strategic and economic advantages. Countries like China, Russia, and Iran have been implicated in cyber espionage campaigns targeting Shipping industries, aiming to steal sensitive information, intellectual property, and trade secrets. By way of illustration, Chinese hackers have been linked to cyber-attacks targeting Shipping companies and port operators to gain insights into global trade patterns, supply chain logistics, and strategic assets (Sen, 2016; Svilicic et al., 2019). Similarly, Russian and Iranian hackers have targeted Shipping companies to gather intelligence, disrupt operations, and undermine geopolitical adversaries, posing significant challenges to the security and integrity of Shipping operations worldwide (Oruc, 2020).

The Role of Cyber Counterintelligence in the Shipping Industry

The role of Cyber Counterintelligence (CCI) in safeguarding against cyber threats cannot be overstated, particularly in

industries as critical as Shipping operations. CCI involves proactive measures to detect, analyze, and neutralize malicious activities perpetrated by adversaries, whether they be state-sponsored actors, criminal organizations, or rogue hackers (Kanellopoulos, 2023). In this context, CCI plays a pivotal role in identifying and mitigating cyber threats that could compromise the integrity, safety, and efficiency of a corporate operation (Duvenage, and Solms, 2014). This includes monitoring for signs of unauthorized access, malware infections, or anomalous network behavior, as well as conducting thorough risk assessments to identify vulnerabilities and prioritize security measures (Duvenage et al., 2018; Prunckun, 2018). Moreover, CCI efforts often involve gathering and analyzing intelligence on emerging cyber threats, including tactics, techniques, and procedures employed by adversaries, to anticipate and preempt potential attacks (Sigholm and Bang, 2013; Jaquire and Solms, 2017).

Understanding Cyber Counterintelligence

Accurately, understanding CCI is paramount in navigating the complex and ever-evolving landscape of Cybersecurity threats that confront organizations across various industries (Bardin, 2011; Duvenage et al., 2017). CCI represents a proactive approach to defense, emphasizing the gathering, analysis, and dissemination of intelligence to identify, assess, and counteract threats originating from adversaries operating in cyberspace (Sigholm and Bang, 2013; Sangher et al., 2023). At its core, CCI involves a comprehensive understanding of the tactics, techniques, and procedures (TTPs) employed by threat actors, including state-sponsored groups, criminal organizations, and hacktivists (Duvenage, and Solms, 2014). One fundamental aspect of CCI is the continuous monitoring of digital networks and systems for indicators of compromise (IOCs) and suspicious activities (Duvenage et al., 2018). This proactive surveillance enables organizations to detect unauthorized access attempts,

malware infections, or anomalous behavior that may indicate a potential security breach (Jaquire and Solms, 2017). By leveraging advanced cybersecurity tools and technologies, such as intrusion detection systems (IDS), endpoint detection and response (EDR) platforms, and security information and event management (SIEM) solutions, organizations can gain real-time visibility into their IT environments and respond swiftly to emerging threats (Duvenage, and Solms, 2014).

In addition to monitoring for IOCs, CCI involves conducting comprehensive threat assessments to evaluate the likelihood and potential impact of cyber threats on organizational assets and operations. This involves analyzing threat intelligence data, including indicators of compromise (IOCs), threat actor profiles, and attack patterns, to identify potential vulnerabilities and prioritize security measures. By understanding the specific tactics and techniques employed by threat actors, organizations can tailor their defenses accordingly, implementing targeted security controls and mitigating strategies to reduce their exposure to cyber risks (Duvenage et al., 2018).

Furthermore, CCI profiling of threat actors offers insights into their motivations, objectives, and modus operandi (Bardin, 2011). This involves gathering intelligence on threat actor groups, including their affiliations, capabilities, and past activities, to understand their strategic goals and anticipate their next moves (Cho and Kyungho, 2016). By profiling threat actors, organizations can better assess the level of risk posed by different adversaries and tailor their defensive strategies accordingly. For example, state-sponsored threat actors may be motivated by geopolitical objectives, while cybercriminal groups may be driven by financial gain. Understanding these distinctions enables organizations to prioritize their defenses and allocate resources effectively to mitigate the most significant threats (Jaquire and Solms, 2017).

Moreover, CCI enables organizations to gather actionable intelligence on emerging threats, enabling them to stay ahead of evolving cyber risks and protect critical assets and infrastructure (Rudner, 2008; Alcaide, and Llave, 2020). By monitoring open-source intelligence (OSINT), dark web forums, and other sources of threat intelligence, organizations can identify emerging trends, vulnerabilities, and attack vectors before they are widely exploited by adversaries. This proactive approach to threat intelligence gathering allows organizations to anticipate emerging threats and take preemptive action to strengthen their defenses and mitigate potential risks.

Additionally, CCI plays a crucial role in facilitating collaboration and information sharing among industry stakeholders, government agencies, and cybersecurity experts. By sharing threat intelligence data, best practices, and lessons learned, organizations can collectively enhance their understanding of cyber threats and improve their ability to respond effectively to emerging risks (Dempsey et al., 2021). The importance of collaboration and information sharing in CCI cannot be overstated. By working together with industry partners, government agencies, and cybersecurity experts, organizations can leverage the collective resources and insights of the cybersecurity community to enhance their cybersecurity posture. Collaboration fosters a culture of collective defense, encouraging organizations to share information and expertise to address common challenges and vulnerabilities in cyberspace. Moreover, collaboration facilitates the exchange of best practices and lessons learned, enabling organizations to learn from each other's experiences and improve their cybersecurity strategies and tactics. By sharing information on emerging threats, vulnerabilities, and attack vectors, organizations can stay ahead of evolving cyber risks and adapt their defenses accordingly. Collaboration also enables

organizations to pool their resources and capabilities to develop joint initiatives and response plans, enabling a coordinated and effective response to cyber incidents (Duvenage et al., 2018).

Cyber Counterintelligence Strategy in the Shipping Industry

In a Shipping company, the implementation of CCI strategies serves as a pivotal mechanism to fortify cybersecurity defenses against the multifaceted spectrum of cyber threats that could imperil operational integrity and compromise sensitive data (Ben Farah, 2022). Here are delineated operational choices exemplifying CCI in practice within a Shipping company:

1. Continuous Surveillance and Monitoring: The adoption of continuous surveillance and monitoring protocols empowers the Shipping company to sustain real-time vigilance over its digital infrastructure, promptly identifying any anomalous network activity or indicators of compromise (The Department of Defense Strategy, 2009; Pöyhönen and Lehto, 2022). Through the deployment of sophisticated intrusion detection systems (IDS) and security information and event management (SIEM) platforms, the organization can effectively scrutinize network traffic, log data, and system events, thereby facilitating the expedited detection of unauthorized access attempts, malware incursions, or other aberrant behaviors indicative of potential security breaches (Sigholm and Bang, 2013; Duvenage et al., 2017; Ball, 2021).
2. Proactive Engagement in Threat Intelligence Collection: Proactively engaging in the collection of threat intelligence enables the Shipping company to remain abreast of emerging cyber threats and preemptively anticipate potential adversarial

incursions (The Department of Defense Strategy, 2009; Duvenage et al., 2018). This strategic endeavor encompasses subscribing to dynamic threat intelligence feeds, active participation in industry-specific information-sharing consortia, and diligent monitoring of open-source intelligence (OSINT) repositories. Such proactive intelligence-gathering endeavors furnish invaluable insights into the intricate tactics, techniques, and procedures (TTPs) espoused by malevolent threat actors, thus substantiating the formulation of informed defensive strategies and judicious resource allocation (Svilicic et al., 2019).

3. Systematic Vulnerability Assessments: The systematic conduct of comprehensive vulnerability assessments affords the Shipping company the means to meticulously scrutinize and rectify susceptibilities inherent within its IT systems and infrastructure (Sangher et al., 2023). Through the judicious implementation of vulnerability scanning protocols, penetration testing methodologies, and holistic security assessments, the organization adeptly identifies latent vulnerabilities, such as outdated software iterations, misconfigured network nodes, or insecure system protocols. This concerted effort furnishes the organizational leadership with actionable insights imperative for risk mitigation initiatives, enabling the prioritization of remedial measures to curtail the organization's cyber risk exposure (Ben Farah, 2022).
4. Threat Actor Profiling and Adversary Attribution: The strategic profiling of potential threat actors facilitates a nuanced comprehension of their motivations, modus operandi, and operational capabilities (Bardin, 2011). By conducting meticulous analyses of threat actor group dynamics, affiliations, and historical exploits, the Shipping company can

proficiently discern the strategic imperatives and potential threat vectors employed by adversarial entities. This insight-rich intelligence serves as a cornerstone for the organization's targeted incident response planning and adaptive defensive posturing, thereby optimizing the efficacy of its cybersecurity resilience endeavors (Cho and Kyungho, 2016; Duvenage et al., 2017).

5. Employee Training and Cyber Awareness Cultivation: The cultivation of a cyber-resilient organizational culture hinges upon the meticulous investment in employee training and cyber awareness cultivation initiatives (The Department of Defense Strategy, 2009; Bardin, 2011; Canepa et al., 2021). By provisioning regular cybersecurity training regimens, immersive phishing awareness workshops, and simulated incident response drills, the organization nurtures a workforce adept at recognizing and responding to emergent security threats (Canepa et al., 2021). This concerted emphasis on human-centric cybersecurity bolstering engenders an organizational ethos characterized by heightened vigilance and proactive participation in the collective defense against cyber adversaries (Black, 2014; Svilicic et al., 2019; Sithole et. al., 2023).
6. Incident Response Preparedness and Plan Elaboration: The judicious elaboration of robust incident response plans augments the organization's preparedness to deftly navigate and mitigate the ramifications of cyber incidents as they manifest. Through the meticulous delineation of role assignments, hierarchical escalation protocols, and methodical tabletop exercise simulations, the organization fosters an operational environment characterized by expedited incident detection, classification, and remediation (Duvenage et al.,

2017). This preemptive stance fortifies the organization's resilience vis-à-vis potential cyber assaults, facilitating expeditious recovery and the restoration of normal operational cadence (Duvenage, and Solms, 2014).

7. Synergistic Collaboration and Information Sharing: The cultivation of synergistic collaboration and information-sharing channels with industry peers, governmental entities, and cybersecurity domain experts fosters an ecosystem conducive to collective defense and mutual reinforcement. By actively participating in industry-specific information exchange forums, sharing proprietary threat intelligence feeds, and engaging in reciprocal knowledge dissemination initiatives, the Shipping company fortifies its cybersecurity posture through the cumulative wisdom and pooled resources of the cybersecurity community. This collaborative ethos engenders a collective resilience paradigm, fostering a cohesive front against the evolving cyber threat landscape (Dempsey et al., 2021).

In summation, the judicious adoption of CCI practices within a Shipping company encompasses a strategic amalgamation of operational choices, underpinned by the imperative to proactively detect, analyze, and mitigate cyber threats. Through the deployment of continuous surveillance protocols, proactive engagement in threat intelligence gathering, meticulous vulnerability assessments, strategic threat actor profiling, investment in employee training and cyber awareness cultivation, elaboration of robust incident response preparedness plans, and synergistic collaboration and information sharing initiatives, the Shipping company fortifies its cyber defense apparatus against potential adversarial incursions (Canepa et al., 2021). This holistic approach engenders an organizational posture characterized

by resilience, agility, and adaptability in the face of an ever-evolving cyber threat landscape.

Conclusion

In conclusion, the contemporary cyber threat landscape presents a complex tapestry of challenges, featuring a diverse array of actors ranging from non-state entities like organized crime syndicates and terrorist organizations to state-sponsored operatives such as those affiliated with China, Russia, and Iran. These actors engage in a spectrum of cyber operations driven by varied motivations encompassing financial gain, ideological pursuits, and geopolitical objectives.

Within the maritime domain, cyber threats manifest in diverse forms, including tampering with navigation systems, ransomware attacks targeting shipping operations, and theft of sensitive cargo information. High-profile incidents such as the 2017 NotPetya ransomware attack on the Port of Rotterdam and Maersk's operations underscore the susceptibility of maritime infrastructure to cyber-attacks, with profound implications for global trade and supply chain integrity. Furthermore, the exploitation of digital technologies in shipping operations introduces novel attack vectors and vulnerabilities, necessitating comprehensive cyber counterintelligence strategies.

In response, the adoption of CCI emerges as a cornerstone strategy for safeguarding maritime operations against cyber threats. Leveraging continuous surveillance, proactive threat intelligence collection, systematic vulnerability assessments, and meticulous threat actor profiling, maritime organizations can bolster their resilience and readiness to mitigate cyber threats effectively. Employee training initiatives, incident response preparedness, and collaborative information-sharing frameworks further fortify cyber defense postures. By

integrating these operational choices into a cohesive cyber counterintelligence strategy, maritime entities can navigate the intricate cyber threat landscape with enhanced resilience and adaptability, safeguarding critical maritime assets and operations in an increasingly digitized environment.

Literature:

1. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., and Michaloliakos, M. (2022). Cybersecurity challenges in the Maritime Sector. Network, 2(1), 123–138. https://doi.org/10.3390/network2010009.
2. Alcaide, J. I., and Llave, R. G. (2020). Critical infrastructures cybersecurity and the Maritime Sector. Transportation Research Procedia, 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.
3. Alshathry, S., (2017). Cyber Attack on Saudi Aramco. International Journal of Management and Information Technology. 11(5), 3037-3039.
4. Andriukaitis, L., Kalensky, J., Kargar, S., Panchulidze, E., Smetek, J., and Vangeli A., (2021) The misuse of social media platforms and other communication channels by authoritarian regimes: Lessons learned. Policy Department for External Relations – European Parliament.
5. Ball, K., (2021). Electronic Monitoring and Surveillance in the Workplace. Joint Research Center – European Commission.
6. Bardin, J., (2011). Ten commandments of cyber counterintelligence', CSO Magazine. Available at: https://www.csoonline.com/article/543519/identity-management-ten-commandments-of-cyber-counterintelligence-adapted-from-james-m-olson.html (Accessed 28/02/2023).
7. Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., and Bellekens, X. (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.
8. Bendovschi, A. (2015). Cyber-attacks – trends, patterns, and security countermeasures. Procedia Economics and Finance, 28, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1.
9. Black, J., (2014). The complexity of cyber counterintelligence training, Master of Science dissertation, Utica College, New York, US.
10. Canepa, M., Ballini, F., Dalaklis, D., and Vakili, S. (2021). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. INTED2021 Proceedings. https://doi.org/10.21125/inted.2021.0726.

11. Cho, I. and Kyungho, L. (2016). Advanced Risk Measurement Approach to Insider Threats in Cyberspace. Intelligent Automation & Soft Computing, 22(3), 405-413.
12. Colonial Pipeline: The DarkSide strikes. Congressional Research Service, 2021.
13. Counterintelligence in Cyberspace. The Department of Defense Strategy, 2009.
14. Defending Against Software Supply Chain Attacks. Cybersecurity and Infrastructure Security Agency, 2021.
15. Dempsey, K., Yan Pillitteri, V., and Regenscheid, A., (2021). Managing the Security of Information Exchanges. Publication 800-47, National Institute of Standards and Technology - U.S. Department of Commerce.
16. Duvenage, P., Jaquire, V., and Solms, S., (2018). Towards a Literature Review on Cyber Counterintelligence. Journal of Information Warfare, 17(4), pp. 284-297.
17. Duvenage, P., and Solms, S., (2014). Putting Counterintelligence in Cyber Counterintelligence. 13th European Conference on Cyber Warfare and Security.
18. Duvenage, P., Sithole, T., and Solms, S., (2017). A Conceptual Framework for Cyber Counterintelligence – Theory that Really Matters. 16th European Conference in Cyber Warfare and Security.
19. 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 01/03/2024).
20. Finklea, K., Christensen, M., Fischer, E., Lawrence, S., and Theohary Catherine, (2015). Cyber Intrusion into U.S. Office of Personnel Management: In Brief. Congressional Research Service.
21. Giannakopoulou, N., Thalassinos, E. I., and Stamatopoulos, T. V. (2016). Corporate governance in shipping: an overview. Maritime Policy & Management, 43(1), 19-38.
22. Grammenos, T., (2010). The Handbook of Maritime Economics and Business. Lloyd's List.
23. Jaquire, V., and von Solms, S., (2017). Towards a cyber counterintelligence maturity model. Proceedings of the 12th International Conference on Cyber Warfare and Security.
24. Jensen, B., (2023). How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy. Center for Strategic & International Studies, Available at: https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy, (Accessed 28/02/2023).
25. 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. 13th International Conference on Cyber Conflict.

26. Kanellopoulos, A. N. (2023). The Dimensions of Counterintelligence and Their Role in National Security. Journal of European and American Intelligence Studies, 6(2), 85-104.
27. Loomis, W., Singh, V., Kessler, G., and Bellekens X., (2021). A system of systems: Cooperation on maritime cybersecurity. Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-a-system-of-systems/ (Accessed 01/03/2024).
28. Mueller, R., (2019). Report On the Investigation Into Russian Interference In The 2016 Presidential Election. U.S. Department of Justice.
29. Oruc, A., (2020). Claims of State-Sponsored Cyberattack in the Maritime Industry. Conference Proceedings of INEC. Available at: https://library.imarest.org/record/7663/files/INEC_2020_Paper_30.pdf (Accessed 01/03/2024).
30. Petersson, N. P., Tenold, S., and White, N. J. (2019). Shipping and Globalization in the Post-War Era. Palgrave Studies in Maritime Economics.
31. Pöyhönen, J., & Lehto, M. (2022). Assessment of cybersecurity risks: Maritime Automated Piloting process. International Conference on Cyber Warfare and Security, 17(1), 262–271. https://doi.org/10.34190/iccws.17.1.18
32. Prunckun, H., (2018). [Advanced Sciences and Technologies for Security Applications] Cyber Weaponry || Weaponization of Computers. , 10.1007/978-3-319-74107-9(Chapter 1), 1–12. doi:10.1007/978-3-319-74107-9_1.
33. Rudner, M., (2008). Protecting Critical Energy Infrastructure through Intelligence. International Journal of Intelligence and Counterintelligence, 21(4), 635-660.
34. Sangher, K. S., Singh, A., Pandey, H. M., & 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), 349. https://doi.org/10.3390/info14060349.
35. Sen, R. (2016). Cyber and information threats to seaports and ships. Maritime Security, 281–302. https://doi.org/10.1016/b978-0-12-803672-3.00009-1.
36. Sigholm, J., and Bang, M., (2013). Towards Offensive Cyber Counterintelligence. 2013 European Intelligence and Security Informatics Conference. https://doi.org/10.1109/EISIC.2013.37.
37. Sithole, T., Toit, J. and Solms, S., (2023). A Cyber Counterintelligence Competence Framework: Developing the Job Roles. 22nd European Conference on Cyber Warfare and Security.
38. Svilicic, B., Kamahara, J., Rooks, M., and Yano, Y. (2019). Maritime Cyber Risk Management: An experimental ship assessment. Journal of Navigation, 72(5), 1108–1120. https://doi.org/10.1017/s0373463318001157.