BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Counterterrorism Planning in the Shipping Industry Leveraging Competitive Intelligence

Anastasios-Nikolaos KANELLOPOULOS, Ph.D. Candidate*
Anthony IOANNIDIS, Assistant Professor**

*Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ankanell@aueb.gr
**Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ai@aueb.gr

Abstract

This paper addresses the critical need to bolster Counterterrorism (CT) strategies in the Shipping industry, which is responsible for the vast majority of global goods transportation. The objective is to advocate for the integration of Competitive Intelligence (CI) into CT planning to address current security deficiencies. Key threats such as piracy in Somalia and the Gulf of Guinea, ship-borne terrorism, and attacks on ports are examined, highlighting the limitations of existing measures like the International Ship and Port Facility Security (ISPS) Code.

The first chapter delves into primary threats, including hijacking, piracy, ship-borne terrorism, and port attacks, providing an in-depth analysis of their implications and necessary countermeasures. The second chapter explores current CT measures, focusing on the role of the International Maritime Organization (IMO) and the effectiveness of the ISPS Code, while identifying the reactive nature of existing strategies. The third chapter proposes a strategic CI framework, emphasizing comprehensive data collection, advanced analysis, threat identification, and proactive strategy development. Each component is detailed to illustrate how CI can transform CT planning, making it more anticipatory and effective.

The authors anticipate that using CI will help stakeholders, including policymakers, Shipping companies, and security agencies, adopt more proactive and effective measures against emerging threats. The proposed framework emphasizes the importance of stakeholder collaboration, public-private partnerships, and international cooperation. This study aims to enhance maritime security, ensure global trade's safe and efficient operation, and improve global maritime resilience, offering valuable insights for all industry stakeholders.

Keywords:

Counterterrorism, Shipping Industry; Competitive Intelligence;
Maritime Security; Threat Analysis.

Article info
Received: 15 November 2024; Revised: 29 November 2024; Accepted: 9 December 2024; Available online: 17 January 2025

Citation: Kanellopoulos, A.N. and A. Ioannidis. 2024. "Counterterrorism Planning in the Shipping Industry Leveraging Competitive Intelligence". *Bulletin of "Carol I" National Defence University*, 13(4): 77-87. https://doi.org/10.53477/2284-9378-24-50

The Shipping industry plays a pivotal role in global trade, handling the vast majority of the world's goods transportation (Grammenos 2010). However, its crucial function makes it a prime target for terrorist groups seeking to disrupt economic stability and create fear. Recent increases in maritime terrorism, piracy, and other illicit activities highlight the urgent need for stronger Counterterrorism (CT) strategies in the sector (Mohsendokht et al. 2024). Traditionally focused on safety and accident prevention, the industry has overlooked CT planning, leaving it vulnerable to complex terrorist threats. This paper proposes integrating Competitive Intelligence (CI) into CT strategies to enhance maritime security.

The objective is to offer a comprehensive framework for incorporating CI into security measures, empowering stakeholders – including governments, Shipping companies, and international organizations – to proactively identify and mitigate potential terrorist threats. The authors expect that adopting CI will improve risk anticipation, leading to more effective and preventive measures. This study is intended for policymakers, maritime security experts, and industry stakeholders, aiming to strengthen global maritime resilience and safeguard the international supply chain.

Key Threats to the Shipping Industry

The present chapter delves into the primary threats facing the Shipping industry, focusing on hijacking and piracy, ship-borne terrorism, and attacks on ports and infrastructure. Each section aims to provide an in-depth analysis of these threats, highlighting their implications and the measures needed to counteract them. The objective is to offer a comprehensive understanding of how these threats disrupt global trade and what can be done to mitigate their impact.

Initially, piracy, particularly off the coast of Somalia and in the Gulf of Guinea, remains a significant threat to global Shipping. Piracy off the coast of Somalia, driven by financial motives, has led to increased Shipping costs, disrupted trade routes, and heightened security concerns. The collapse of Somalia's central government in the early 2000s created a lawless environment, enabling pirates to hijack commercial vessels for ransom (Stanley and Uwizeyimana 2023). Pirates typically use small, fast boats to overtake larger vessels, demanding substantial ransoms for the release of ships and their crews. Despite international efforts to curb these activities, the financial incentives from ransoms have perpetuated the cycle of piracy (Molina et al. 2024). The persistence of Somali piracy underscores the need for robust international collaboration and sustainable solutions to address the underlying political and economic instability in the region. Continued efforts to enhance maritime security and develop local economies are crucial to mitigating this threat.

Moreover, piracy in the Gulf of Guinea is characterized by more violent and organized attacks, often involving cargo theft, kidnapping of crew members, and armed robbery. This region, rich in oil, is a lucrative target for pirates who frequently attack oil tankers and vessels involved in the petroleum industry (Schandorf 2024). Unlike Somali piracy, which primarily involves hijacking for ransom, piracy in the Gulf of Guinea focuses on stealing cargo, particularly oil, and kidnapping crew members for ransom. The pirates in this region are highly organized, sometimes with connections to onshore criminal networks (Ahorsu et al. 2024). Further, the piracy situation in the Gulf of Guinea highlights the need for enhanced regional cooperation and stronger security measures. Addressing the socio-economic factors that fuel piracy and improving the capacity of local enforcement agencies are essential steps towards reducing this threat.

Subsequently, there is increasing concern that terrorist organizations might leverage hijacking and piracy to fund their operations or carry out ideologically driven attacks. In Somalia, the extremist group Al-Shabaab has reportedly explored maritime piracy as a revenue stream to support its insurgency efforts (Levy and Yusuf 2019). Similarly, in the Gulf of Guinea, militant groups involved in the Niger Delta conflict might turn to piracy to advance their political agendas. The potential for terrorist groups to exploit piracy for funding and operational purposes necessitates a multifaceted approach that includes CT strategies and strengthened maritime security protocols. Vigilant monitoring and international cooperation are critical to preventing such exploitation.

Furthermore, Ship-borne terrorism represents an evolving threat as terrorists increasingly consider using commercial vessels to transport weapons, explosives, or personnel. Terrorists could use the anonymity of the Shipping industry to smuggle weapons, including conventional arms, explosives, and weapons of mass destruction (WMDs), posing severe risks to coastal cities and critical infrastructure (Bueger and Edmunds 2024). Additionally, commercial ships may be used to transport personnel, including operatives planning attacks in other countries. The global nature of the Shipping industry provides cover for the movement of individuals across borders without attracting attention (McNicholas 2016; Romero 2021). The threat of ship-borne terrorism underscores the need for comprehensive security protocols and international cooperation to monitor and secure Shipping routes. Enhanced inspection procedures and intelligence sharing are vital in mitigating this risk.

Thereafter, ports serve as vital nodes in the global supply chain, making them prime targets for terrorist attacks. Attacks on major ports could have devastating economic consequences, disrupting global trade and triggering cascading effects throughout supply chains (Raymond 2006). The complexity of port operations, involving various stakeholders and handling vast amounts of cargo, presents numerous vulnerabilities that terrorists could exploit. Additionally, ports often house large quantities of hazardous materials, which can amplify the impact of an attack (Gordon et al. 2005). Cyber-attacks pose a significant threat to port operations, capable of disrupting logistics, sabotaging equipment, and compromising critical data (Kanellopoulos 2024b).

Increasing reliance on digital systems for managing logistics and coordinating vessel movements has heightened the risk of cyber-attacks. Terrorists could exploit these weaknesses to cause operational paralysis and financial losses (Kanellopoulos and Ioannidis 2024). The vulnerability of ports to physical and cyber-attacks highlights the need for comprehensive security measures and robust cybersecurity protocols. Investing in advanced security technologies and fostering international cooperation are essential to safeguarding port infrastructure.

Eventually, the Shipping industry faces numerous threats, including hijacking and piracy, ship-borne terrorism, and attacks on ports and infrastructure. Addressing these threats requires a multifaceted approach involving international cooperation, enhanced security measures, and addressing the underlying socio-economic factors that contribute to these risks.

Current Counterterrorism Measures in the Shipping Industry

This chapter explores the critical role of the International Maritime Organization (IMO) in enhancing maritime security and the measures taken by Shipping companies to protect vessels, crews, and cargoes from evolving threats. The focus is on the implementation and impact of the International Ship and Port Facility Security (ISPS) Code, the response to maritime terrorism, and the need for more proactive and intelligence-driven security strategies. The objective is to provide a comprehensive understanding of the current security landscape and the necessary steps to bolster maritime security globally.

The International Maritime Organization (IMO) has played a crucial role in implementing regulations designed to enhance maritime security on a global scale. Among the most significant of these is the International Ship and Port Facility Security (ISPS) Code, established as part of the broader International Convention for the Safety of Life at Sea (SOLAS) following the events of September 11, 2001. The ISPS Code provides a standardized framework for assessing and managing security risks in ports and on ships, outlining mandatory measures for governments, Shipping companies, and port authorities (Lloyd's Register 2024). This framework aims to deter and prevent acts of terrorism and other unlawful acts against ships and port facilities by mandating security assessments, the development of security plans, and the appointment of designated security officers. Moreover, the ISPS Code emphasizes the importance of international cooperation, requiring member states to share information and collaborate on security-related issues to protect the global maritime transportation system.

In response to the growing threat of maritime terrorism, Shipping companies have implemented various security measures aimed at protecting their vessels, crews, and cargoes (Osaloni 2023). These initiatives include the deployment of armed guards on board vessels, particularly when transiting through high-risk areas such as the Gulf of Aden and the Gulf of Guinea. Additionally, companies have adopted advanced vessel tracking systems that allow for real-time monitoring of ship movements, enabling faster responses to potential security incidents. Crew training programs have also been enhanced, focusing on raising awareness of security threats, improving emergency preparedness, and ensuring that crew members are equipped to respond effectively in the event of an attack (Kanellopoulos 2024a, 2024c).

Despite these efforts, many of these measures are reactive in nature, primarily designed to respond to incidents after they occur rather than to prevent them. The reactive nature of many security measures limits their effectiveness, as they are often implemented after a threat has been identified or an attack has occurred. This underscores the need for more proactive and intelligence-driven approaches to maritime security (Peisl *et al.* 2021). By integrating CI and other advanced analytical tools, the industry can enhance its ability to anticipate and mitigate potential threats before they materialize. Such strategies would involve continuous monitoring of threat landscapes, sharing of intelligence across borders, and the development of predictive models that can identify potential risks in advance (Rasool et al. 2022).

While the existing international regulations and industry initiatives provide a foundational level of security within the maritime sector, they are often insufficient to address the increasingly sophisticated and evolving nature of terrorist threats. Current strategies tend to focus on compliance with regulations and the implementation of defensive measures, such as armed security and tracking systems (Okafor-Yarwood and Onuoha 2023). However, these approaches may not be adequate in a landscape where terrorist tactics are becoming more complex and unpredictable. This underscores the need for more proactive and intelligence-driven approaches to maritime security (Peisl et al. 2021). By integrating CI and other advanced analytical tools, the industry can enhance its ability to anticipate and mitigate potential threats before they materialize. Such strategies would involve continuous monitoring of threat landscapes, sharing of intelligence across borders, and the development of predictive models that can identify potential risks in advance (Rasool et al. 2022).

Ultimately, closing the gaps in current CT strategies requires a shift from reactive to proactive security measures, ensuring that the maritime industry is better equipped to prevent terrorist attacks and protect global trade. By implementing comprehensive strategies that include advanced analytics, intelligence sharing, and continuous threat monitoring, the maritime industry can enhance its resilience against evolving threats and ensure the safety and security of global maritime operations.

Integrating Competitive Intelligence into Counterterrorism Planning

This chapter delineates a strategic framework for integrating CI into CT planning within the Shipping industry. Structured around several critical steps, this framework aims to enhance the industry's capacity to detect, assess, and respond to potential terrorist threats, thereby improving the security of global maritime operations. This introduction sets the stage for a detailed exploration of each framework component, emphasizing the importance of CI in maintaining a secure maritime environment.

- **Data Collection**: The initial step involves comprehensive data collection, which is foundational to the framework. The quality and breadth of data gathered directly impact the effectiveness of subsequent analysis and decision-making processes. To ensure a well-rounded understanding of potential threats, data should be sourced from diverse channels, including public records, intelligence reports, satellite imagery, and social media platforms (Raptis, Katsini, and Alexakos 2021). Each data stream offers unique insights, contributing to a multi-dimensional view of the threat environment. The primary objective here is to amass pertinent information to lay the groundwork for a detailed and accurate threat assessment (Klemmer et al. 2023; Rodríguez-Ibáñez et al. 2023).
- **Data Analysis**: Following data collection, rigorous analysis is crucial (Morgenthaler 2009). This process transforms raw data into actionable intelligence through advanced analytical tools and techniques such as data mining, machine learning algorithms, and predictive analytics. Each method provides unique capabilities in identifying potential security risks, thereby enhancing the ability to detect and address threats effectively.
- **Big Data Analytics**: In the CT context, big data analytics plays a pivotal role. The Shipping industry generates extensive data daily due to its vast and interconnected nature. Big data analytics enables the efficient processing and examination of this voluminous information (Saxena and Lamest 2018; Barnea 2021). Specifically, it allows for the monitoring of Shipping routes, tracking vessel movements, and analyzing communication patterns, which are crucial for identifying potential threats that might not be immediately apparent through traditional analysis methods.
- **Threat Identification and Prioritization**: Upon completing data analysis, the next step is to identify and prioritize potential threats systematically. This phase involves evaluating each identified threat's likelihood and potential impact on the Shipping industry (Yang *et al.* 2023). Prioritization is essential for efficient resource allocation, ensuring that the most significant threats receive immediate attention. By categorizing threats based on severity and probability, stakeholders can focus on mitigating the most pressing risks, thus enhancing overall security.
- **Strategy Development**: Based on the identified and prioritized threats, developing a targeted CT strategy is the subsequent step. This comprehensive strategy should incorporate measures designed to mitigate or neutralize identified threats, including implementing new security protocols, deploying additional resources to high-risk areas, and developing contingency plans for potential emergencies. The strategy must be adaptable, allowing for adjustments as new threats emerge or as the security environment evolves (Cavallo *et al.* 2020; García-Madurga and Esteban-Navarro 2020).
- **Collaboration Among Stakeholders**: Effective CT planning within the Shipping industry necessitates collaboration among a wide array of

stakeholders (Parker et al. 2017). This includes not only Shipping companies but also government agencies, intelligence organizations, and international bodies. CI serves as a critical enabler of this collaboration by providing a shared framework for threat identification, assessment, and response. Through CI, stakeholders can align their efforts, share valuable information, and coordinate their actions to enhance collective security.

- ➢ **Public-Private Partnerships**: Public-private partnerships (PPPs) are particularly vital in CT planning. The Shipping industry, primarily composed of private entities, must work closely with governmental bodies to effectively counter CT threats. PPPs facilitate the sharing of information, resources, and expertise between the public and private sectors. CI plays a central role in these partnerships by providing a common platform for data sharing and analysis, ensuring both sectors are well-informed and capable of joint action in the face of threats.
- ➢ **International Cooperation**: Given the global nature of the Shipping industry, international cooperation is indispensable for effective CT planning. This cooperation extends beyond national borders, encompassing collaboration with international organizations and regional security alliances (Seiglie and Matelly 2011). CI enhances international cooperation by offering a standardized approach to threat identification and assessment, facilitating the seamless exchange of intelligence across countries, and helping build a cohesive global response to maritime terrorism.
- ➢ **Implementation and Monitoring**: The final stage of the CI-driven CT framework involves implementing and continuously monitoring the developed strategy (Muramudalige et al. 2023). This requires deploying necessary resources, training personnel on new security protocols, and establishing monitoring systems to track the strategy's effectiveness (Gancher et al. 2023). Continuous monitoring is critical to ensure that the strategy remains responsive to evolving threats. This phase involves regular assessments and adjustments to the strategy as needed, ensuring its effectiveness in mitigating risks and protecting the Shipping industry from potential terrorist activities (Yang et al. 2023). By embedding CI into ongoing operational processes, stakeholders can maintain a dynamic and resilient CT posture capable of addressing current and emerging challenges.

In due course, integrating CI into CT planning within the Shipping industry represents a significant advancement in maritime security. By following a structured framework that includes comprehensive data collection, advanced data analysis, and proactive threat identification and prioritization, the industry can enhance its ability to anticipate and mitigate potential threats. Collaboration among stakeholders, public-private partnerships, and international cooperation further strengthen the industry's CT capabilities. Continuous implementation and monitoring ensure that strategies remain effective and adaptable to evolving threats. This proactive and intelligence-driven approach is essential for safeguarding global maritime operations and ensuring the security of international trade.

Conclusions

The present research leads to several key conclusions about the integration of CI into CT strategies in the Shipping industry.
Firstly, the study identifies critical threats to the industry, including piracy and hijacking, ship-borne terrorism, and attacks on ports and infrastructure. Piracy, particularly off the coast of Somalia and in the Gulf of Guinea, remains a significant threat, disrupting global trade and posing serious risks. The persistence of piracy in these regions underscores the need for enhanced international collaboration and sustainable solutions to address the underlying socio-economic issues that fuel such activities. Ship-borne terrorism, where terrorists use commercial vessels to transport weapons and personnel, presents an evolving threat that requires stringent security protocols and international cooperation to monitor and secure Shipping routes. Additionally, ports, as critical nodes in the global supply chain, are vulnerable to both physical and cyber-attacks. Comprehensive security measures and robust cybersecurity protocols are essential to safeguard these vital infrastructures.

Evaluating current CT measures reveals that while the ISPS Code provides a foundational security framework, its reactive nature limits its effectiveness. Similarly, industry initiatives such as deploying armed guards, implementing advanced tracking systems, and enhancing crew training programs are crucial but need to be complemented by predictive intelligence and continuous monitoring to preempt threats more effectively.

Moreover, the proposed integration of CI into CT planning involves several critical steps. Comprehensive data collection from diverse sources, followed by rigorous analysis using advanced tools, is essential for transforming raw data into actionable intelligence. Utilizing big data analytics to monitor Shipping routes, track vessel movements, and analyze communication patterns significantly enhances threat detection capabilities. Systematic identification and prioritization of threats ensure that resources are allocated efficiently to address the most significant risks.

Subsequently, developing proactive strategies involves collaboration among stakeholders, including Shipping companies, government agencies, and international bodies. CI facilitates this collaboration by providing a shared framework for threat assessment and response. Strengthening public-private partnerships and enhancing international cooperation are crucial for sharing information, resources, and expertise to counter CT threats effectively.

Furthermore, implementation and continuous monitoring of the developed CT strategies are vital. This requires deploying necessary resources, training personnel on new security protocols, and establishing monitoring systems to track the strategy's effectiveness. Regular assessments and adjustments are necessary to maintain the effectiveness of security measures. Continuous integration of CI into operational processes ensures a dynamic and resilient CT posture, capable of addressing both current and emerging challenges in maritime security.

Summing up, integrating CI into CT strategies provides a robust framework for enhancing maritime security. By adopting a proactive, intelligence-driven approach, stakeholders can significantly improve their ability to anticipate and mitigate threats, thereby ensuring the safe and efficient operation of global trade.

References

Ahorsu, Ken, David Suaka Yaro, and Derrick Attachie. 2024. "Maritime Piracy and Its Implications on Security in the Gulf of Guinea." *Eastern African Journal of Humanities and Social Sciences* 3 (2): 1–10. https://doi.org/10.58721/eajhss.v3i2.470.

Alam Muhammad Mahtab, Yannick Le Moullec, Rizwan Ahmad, Maurizio Magarini, and Luca Reggiani. 2020. "A Primer on Public Safety Communication in the Context of Terror Attacks: The NATO SPS 'COUNTER-TERROR' Project." NATO Science for Peace and Security Series, January 19–34. https://doi.org/10.1007/978-94-024-2021-0_3.

Barnea, A. 2021. "Big Data Can Boost the Value of Competitive Intelligence." *Competitive Intelligence Magazine, 26* (1). https://www.scip.org/page/Big-Data-Boost-Competitive-Intelligence.

Bueger, Christian, and Timothy Edmunds. 2024. *Understanding Maritime Security*. *Oxford University Press EBooks*. Oxford University Press. https://doi.org/10.1093/oso/9780197767146.001.0001.

Carvalho, P. S. de. 2021. "Fundamentals of Competitive Intelligence (CI) - Paulo Soeiro de Carvalho – Medium." *Medium.* https://paulosoeirodecarvalho.medium.com/fundamentals-of-competitive-intelligence-ci-1-ebf07520746e.

Cavallo, Angelo, Silvia Sanasi, Antonio Ghezzi, and Andrea Rangone. 2020. "Competitive Intelligence and Strategy Formulation: Connecting the Dots." *Competitiveness Review: An International Business Journal* ahead-of-print (ahead-of-print). https://doi.org/10.1108/cr-01-2020-0009.

Galgano, Francis A. 2024. "Hostis Humani Generis: Pirates and Global Maritime Commerce." *Research in Globalization* 8 (June): 100188. https://doi.org/10.1016/j.resglo.2023.100188.

Gancher, Joshua, Sydney Gibson, Pratap Singh, Samvid Dharanikota, and Bryan Parno. 2023. "Owl: Compositional Verification of Security Protocols via an Information-Flow Type System," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 1130-1147. https://doi.org/10.1109/sp46215.2023.10179477.

García-Madurga, Miguel-Ángel, and Miguel-Ángel Esteban-Navarro. 2020. "A Project Management Approach to Competitive Intelligence." *Journal of Intelligence Studies in Business* 10 (3). https://doi.org/10.37380/jisib.v10i3.636.

Gordon, Peter, James E Moore, Harry W Richardson, and Qisheng Pan. 2005. "The Economic Impact of a Terrorist Attack on the Twin Ports of Los Angeles–Long Beach". https://doi.org/10.4337/9781845428150.00019.

Grammenos Costas. 2010. The Handbook of Maritime Economics and Business. Taylor & Francis.

International Maritime Organization (IMO). 2020. International Ship and Port Facility Security (ISPS) Code.

Lloyd's Register (LR). 2024. *International Ship and Port Facility Security (ISPS) code.* https://www.lr.org/en/services/statutory-compliance/isps-code/.

Kalogeraki, Eleni Maria, Spyridon Papastergiou, Nineta Polemi, Christos Douligeris, and Themis Panayiotopoulos. 2018. "Exploring Cyber-Security Issues in Vessel Traffic Services." *Knowledge Science, Engineering and Management*, 442–51. https://doi.org/10.1007/978-3-319-99365-2_39.

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

Kanellopoulos, Anastasios-Nikolaos. 2024b. "Enhancing Cyber Security and Counterintelligence in the Shipping Industry." *National Security and the Future* 25 (1): 137–54. https://doi.org/10.37458/nstf.25.1.6.

Kanellopoulos, Anastasios-Nikolaos. 2024c. "Insider Threat Mitigation through Human Intelligence and Counterintelligence: A Case Study in the Shipping Industry." *Defense and Security Studies* 5 (March): 10–19. https://doi.org/10.37868/dss.v5.id261.

Kanellopoulos, Anastasios-Nikolaos and Ioannidis, Anthony. 2024. "Leveraging competitive intelligence in offensive cyber counterintelligence: An operational approach for the Shipping industry." *Security and Defence Quarterly*, 48 (4). https://doi.org/10.35467/sdq/192342.

Klemmer, Konstantin, Esther Rolf, Caleb Robinson, Lester Mackey, and Marc Rußwurm. 2023. "SatCLIP: Global, General-Purpose Location Embeddings with Satellite Imagery." *ArXiv (Cornell University)*, January. https://doi.org/10.48550/arxiv.2311.17179.

McNicholas, Michael A. 2016. "Targeting and Usage of Commercial Ships and Port by Terrorists and Transnational Criminal Organizations," 261–79. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-803672-3.00008-X.

Mohsendokht Massoud, Huanhuan Li, Christos Kontovas, Chia-Hsun Chang, Zhuohua Qu, and Zaili Yang. 2024. "Enhancing Maritime Transportation Security: A Data-Driven Bayesian Network Analysis of Terrorist Attack Risks." *Risk Analysis*, July. https://doi.org/10.1111/risa.15750.

Molina, Renato, Juan Carlos Villaseñor-Derbez, Gavin McDonald, and Grant R McDermott. 2024. "Dangerous Waters: The Economic Toll of Piracy on Maritime Shipping." *SSRN Electronic Journal*, January. https://doi.org/10.2139/ssrn.4811789.

Morgenthaler, Stephan. 2009. "Exploratory Data Analysis." *Wiley Interdisciplinary Reviews: Computational Statistics* 1 (1): 33–44. https://doi.org/10.1002/wics.2.

Muramudalige, Shashika R, Hung, Benjamin, Rosanne Libretti, Jytte Klausen, and Jayasumana, Anura P. 2023. "Investigative Pattern Detection Framework for Counterterrorism." https://arxiv.org/abs/2310.19211.

Okafor-Yarwood, Ifesinachi Marybenedette, and Freedom C. Onuoha. 2023. "Whose Security Is It? Elitism and the Global Approach to Maritime Security in Africa." *Third World Quarterly* 44 (5): 1–21. https://doi.org/10.1080/01436597.2023.2167706.

Osaloni, Oluwatosin S. 2023. "The Legal Frameworks Arising from Using Armed Guards Onboard Ships: Challenges and the Way Forward." Beijing Law Review 14 (02): 621–33. https://doi.org/10.4236/blr.2023.142032.

Parker, David, Julia M. Pearce, Lasse Lindekilde, and M. Brooke Rogers. 2017. "Challenges for Effective Counterterrorism Communication: Practitioner Insights and Policy Implications for Preventing Radicalization, Disrupting Attack Planning, and Mitigating Terrorist Attacks." Studies in Conflict & Terrorism 42 (3): 264–91. https://doi.org/10.1080/1057610x.2017.1373427.

Peisl, Thomas, Joanne Hyland, Richard Messnarz, Bruno Wöran, Samer Sameh, Georg Macher, Jürgen Dobaj, Laura Aschbacher, and Detlev Aust. 2021. "Innovation Agents – Moving from Process Driven to Human Centred Intelligence Driven Approaches." Communications in Computer and Information Science, January 319–35. https://doi.org/10.1007/978-3-030-85521-5_21.

Raptis, George E, Christina Katsini, and Christos Alexakos. 2021. "Towards Automated Matching of Cyber Threat Intelligence Reports Based on Cluster Analysis in an Internet-of-Vehicles Environment," July. https://doi.org/10.1109/csr51186.2021.9527983.

Rasool, Abdur, Chayut Bunterngchit, Luo Tiejian, Md. Ruhul Islam, Qiang Qu, and Qingshan Jiang. 2022. "Improved Machine Learning-Based Predictive Models for Breast Cancer Diagnosis." International Journal of Environmental Research and Public Health 19 (6): 3211. https://doi.org/10.3390/ijerph19063211.

Romero, J. 2021. "Prevention of Maritime Terrorism: The Container Security Initiative." Chicago Journal of International Law. 2021. https://www.semanticscholar.org/paper/Prevention-of-Maritime-Terrorism%3A-The-Container-Romero/ba5b4fa70728bd8ea8b90dd014d2867acb186c2c?utm_source=consensus.

Saxena, Deepak, and Markus Lamest. 2018. "Information Overload and Coping Strategies in the Big Data Context: Evidence from the Hospitality Sector." Journal of Information Science 44 (3): 287–97. https://doi.org/10.1177/0165551517693712.

Schandorf, Stephanie Oserwa. 2024. "Reimagining Counter-Piracy Efforts in the Gulf of Guinea: Lessons from the Theory of Infrastructure for Coordination and Information Sharing*." African Security Review, August 1–17. https://doi.org/10.1080/10246029.2024.2373110.

Seiglie, Carlos, and Sylvie Matelly. 2011. "Economics of Peace and Security -Global and Regional Security Alliances -Carlos Seiglie and Sylvie Matelly ©Encyclopedia of Life Support Systems (EOLSS) GLOBAL and REGIONAL SECURITY ALLIANCES." https://www.eolss.net/sample-chapters/c13/E6-28A-04-03.pdf.

Stanley Osezua Ehiane, and Dominique Uwizeyimana. 2023. "Exploring Maritime Piracy and Somalia National Security." International Journal of Membrane Science and Technology 10 (2): 3128–37. https://doi.org/10.15379/ijmst.v10i2.3068.

Yang, Yiling, Tiantian Gai, Mingshuo Cao, Zhen Zhang, Hengjie Zhang, and Jian Wu. 2023. "Application of Group Decision Making in Shipping Industry 4.0: Bibliometric Analysis, Trends, and Future Directions." Systems 11 (2): 69. https://doi.org/10.3390/systems11020069.