Scientia Militaria
2023, VOL. 51, NO. 3, i-viii
DOI: 10.5787/51-3-1424

SCIENTIA MILITARIA
South African Journal of Military Studies

South African Journal *of Military Science*

Guest Editorial

As humanity seeks to exploit new frontiers in pursuit of greater wealth, prosperity and well-being, more intensive use of ocean territories and the exploration of more remote areas of the oceans unfold.[1] Population growth, declining land-based resources, technological advances, geopolitics, and climate change alongside growing consumption trends dovetail and compete to harvest the oceans for space, food, and materials. Early in the twenty-first century, several ocean debates took place, rose rapidly to more maturity, and shaped a set of paradigms broadly depicting maritime security, the blue economy, ocean health, and blue justice.[2] While the four paradigms serve as ordering mechanisms for analysing the complexities and competing interests, views and actors at play, operational maritime sectors hold their own demands, difficulties and tribulations. In addition, threats, vulnerabilities and opportunities manifest in each of the ocean sectors to further complexity and cut across each other to a larger or lesser extent. The inherent dynamics of the aforementioned plays out above, on the surface and below the surface of the oceans in visible and invisible ways that affect the myriad of activities depending on the oceans as a stock and flow resource.

The growing use of the oceans embedded in the range of actions undertaken in sectors, such as shipping, renewable and non-renewable energy extraction, harvesting of living resources, operating ports, subsea infrastructure, and monitoring the oceans as an environment has not only expanded in scope, but in complexity as well. In addition, actors operating in the different realms of maritime security, the blue economy, the environment, and justice all depend upon a growing common denominator to operate effectively, efficiently and safely: access to modern technologies and assurances of a safe and secure cyber-operating environment to protect the extensive information flows at play.

In lay terms, maritime cybersecurity entails safeguarding digital systems, networks, and data within the maritime domain from cyber threats. It encompasses measures to prevent unauthorised access, data breaches, and disruptions to navigation, communication, vessel control, and port operations. Maritime cybersecurity is also key to promote the sustainable,

1 JB Jouffray, R Blasiak, AV Norström, H Österblom & M Nyström, 'The Blue Acceleration: The Trajectory of Human Expansion into the Ocean', *One Earth*, 2(1), (2020), 43–54.

2 C Bueger & F Mallin, 'Blue Paradigms: Understanding the Intellectual Revolution in Global Ocean Politics', *International Affairs*, 99(4), (2023), 1719–1739.

safe and productive utilisation of the oceans of the world. Modern technology underpinned by an efficient cyber sector forms the backbone of maritime operations. The cyber nexus is also a vulnerability for functional maritime systems as cyber threats continue to grow as a critical hazard to maritime activities. Threats emanate from activists, criminals and terrorists for personal, economic and ideological gains. The actors and the threats they bring about create complex problems for those dependent upon safe and secure functioning of their technology-based systems, information, and data contained in the virtual and physical assets at play.[3]

Some dependencies that rely heavily on maritime cybersecurity and vulnerable to cyber threats entail the following domains: technological dependency, use of the oceans, supply chain continuity, port operations, prevention of financial loss, trade facilitation and compliance, innovation and digital transformation, and investor confidence.

Technological dependency is relevant for modern maritime operations that rely on advanced technology, including navigation systems, communication networks, and vessel control systems. These technologies are susceptible to cyberattacks that can disrupt navigation, communication, and other vital functions, potentially leading to accidents, collisions, and loss of life.[4] Economic use of the oceans depends on cybersecurity playing a pivotal role in enhancing the productive use of the oceans, and so does safeguarding the maritime industry against cyber threats and ensuring the uninterrupted flow of trade, communication, and operations. Here one finds several ways in which cybersecurity contributes to the economic utilisation of the oceans:

Supply chain continuity underpins the broader maritime industry as the backbone of global trade, and facilitates the movement of goods across continents. Cyberattacks targeting shipping companies, port operations, or logistic networks can disrupt supply chains, leading to delays in shipments and increased costs. Robust cybersecurity measures protect against such disruptions by ensuring the smooth flow of goods and minimising economic losses in a world where time is truly money.[5]

Port operations efficiency resonates with being vital hubs for loading and unloading cargo, and they rely heavily on digital systems for operations, such as vessel tracking, cargo handling, and customs clearance. Cybersecurity measures safeguard these systems against unauthorised access, data breaches, and potential disruptions, allowing ports to maintain high levels of efficiency and productivity.[6]

---

3 MS Karim, 'Maritime Cybersecurity and the IMO Legal Instruments: Sluggish Response to an Escalating Threat?', *Marine Policy*, 143 (2022), 105-138.

4 International Maritime Organisation, *Guidelines on Maritime Cyber Risk Management*. MSC-FAL.1/Circ.3/Rev.2. 7 June 2022.

5 S Kumar & RR Mallipeddi, 'Impact of Cybersecurity on Operations and Supply Chain Management: Emerging Trends and Future Research Directions', *Production and Operations Management*, 31(12), (2022), 4488–4500.

6 I de la Peña Zarzuelo, 'Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on this Issue', *Transport Policy*, 100 (2021), 1–4.

Prevention of financial loss requires dependable protection against cyberattacks that may result in financial losses due to ransom demands, theft of sensitive financial information, or fraudulent activities. By implementing cybersecurity protocols, maritime companies can mitigate the risk of financial losses arising from cyber incidents, protect their assets, and secure investments.[7]

Trade facilitation and compliance follows in the wake of many countries and industry clients requiring compliance with cybersecurity standards, such as the Tallinn Manual 2.0 to ensure secure trade operations, and equally so for maritime trade that remains at the core of world trade.[8] Adhering to set standards enables companies to continue participating in international trade with minimal disruptions caused by cybersecurity-related regulatory issues to ultimately promote economic growth.[9]

Innovation and digital transformation reside at the heart of the maritime industry, and the way it embraces digital transformation to enhance operations, reduce costs, and improve customer experiences. This digital shift however also attracts cybersecurity challenges. By addressing these challenges effectively, the industry can confidently explore and adopt innovative technologies that enhance economic competitiveness under the banner of cybersecurity best practices.[10]

Investor confidence grows when robust cybersecurity practices demonstrate the commitment by a company to safeguard its operations and assets. This fosters investor confidence and encourages investments in the maritime sector, supporting growth and expansion opportunities.[11] As the growing economic landscape of the future, building confidence in technologies that promote cyber efficiency and these technologies being encased in cybersecurity are akin to confidence-building measures.

Being lax, unprepared or even ignorant about maritime cyber risks holds implications for maritime players, their interests and business enterprises. The maritime sector is a current and future cornerstone of the global economy, with shipping and port operations facilitating the movement of goods. Damaging cyberattacks on maritime infrastructure, such as ports, energy installations, and subsea cable networks can disrupt supply chains,

---

7 D Reva, 'Maritime Cyber Security: Getting Africa Ready', *ISS Africa Report*, 29 (2020), 1–16.

8 MN Schmitt (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017)

9 O Melnyk, S Onyshchenko, O Onishchenko, O Shumylo, A Voloshyn, Y Koskina & Y Volianska, 'Review of Ship Information Security Risks and Safety of Maritime Transportation Issues', *TransNav: International Journal on Marine Navigation & Safety of Sea Transportation*, 16(4), (2022), 717-722.

10 EP Kechagias, G Chatzistelios, GA Papadopoulos & P Apostolou, 'Digital Transformation of the Maritime Industry: A Cybersecurity Systemic Approach', *International Journal of Critical Infrastructure Protection*, 37 (2022).

11 R Hopcraft, K Tam, JDP Misas, K Moara-Nkwe & K Jones, 'Developing a Maritime Cyber Safety Culture: Improving Safety of Operations', *Maritime Technology and Research*, 5(1), (2023), 1–18.

delay shipments, and result in significant financial losses for businesses and nations. Successful cyberattacks on maritime systems in shipping can compromise vessel stability and navigation, leading to accidents, such as oil spills and environmental damage. Ensuring cyber security is thus crucial to prevent incidents that could have long-lasting ecological consequences.[12] Maritime cyberattacks can be used as a tool by state and non-state actors to undermine national security. Disruption of naval operations, coastal surveillance, or navigation can pose threats to the defence capabilities and territorial integrity of a country.[13] Collectively the threats outlined threaten maritime security, blue economy expectations, the blue environment, and the potential to upset national, regional and even international ocean agendas and expectations.

Heeding best practices is an important risk mitigation measure and necessary for actors to remain in step with the codes and conventions of the International Maritime Organization (IMO) and related international bodies. The latter entities have recognised the significance of maritime cybersecurity by establishing guidelines and regulations to help manage cyber risks. Failure to comply with these regulations not only undermines safety but could also lead to legal consequences and sanctions in an ever-growing maritime community.

Africa is not spared the threat and disruptive consequences of maritime cyberattacks and vulnerabilities. Real and potential, African countries have been subject to and must shield themselves against maritime cyber threats.[14] Awareness and regulatory measures and implementing best practices are important steps for every African coastal state and their maritime entities to combat cybersecurity risks. The continent is utterly reliant on seaborne trade, and houses large landlocked economies and vulnerable populations. The African oceans harbours food resources, data cable networks, energy hubs, critical sea lines of communication and ports as connecting hubs for the overall economy of the continent, its blue economy agenda, and environmental security, and thus requires maritime security and blue justice. The aforementioned matters are also interconnected and operate efficiently thanks to cyber-based connectivity and buttressed by cybersecurity to operate securely, free of threats and – if disrupted – can be corrected speedily.

In a world that has turned irrevocably to enter the oceans as a long lingering frontier, technology is key to maritime operations raising robust cybersecurity as paramount for the safe and productive use of the oceans. In all of this, Africa cannot stand sidelined or idle. The interconnectedness of maritime systems, economic implications, growing environmental concerns, and national security considerations all highlight the urgency of mitigating maritime cyber threats, and African voices must be heard in debates. For this

---

12 M Elgan, 'Maritime Cyber Security: A Rising Tide Lifts All Boats', *Security Intelligence*, 4 November 2021. Available at: <https://securityintelligence.com/articles/maritime-cybersecurity-rising-tide/> [Accessed on 17 August 2023].

13 W Loomis, VV Singh, GC Kessler & X Bellekens, *Raising the Colors: Signalling for Cooperation on Maritime Cybersecurity* (Atlantic Council, 2021).

14 J Cronje & G Martin, 'Experts Warn of Increasing Cybersecurity Threats for the African Maritime Industry', *defenceWeb*, 22 October 2002. Available at: <https://www.defenceweb.co.za/featured/experts-warn-of-increasing-cyber-security-threats-for-the-african-maritime-industry/> [Accessed on 17 August 2023].

Special Issue of *Scientia Militaria*, Volume 51, Issue 3, 2023, the African maritime domain is approached in broad terms, including but not limited to the influence of new technologies and related threats to the African maritime sector, offshore oil and gas sectors, maritime transportation and maritime security, maritime cybersecurity governance, maritime trade and logistics chains, blue economy, African navies, border security and digital leadership.

The articles selected offer an insightful analysis and practical solutions to promote better policy and practice across the continent.

Tefesehet Hailu Sime (African Union Commission) addresses maritime cybersecurity: the need for a regional approach by the African Union and its member states in her contribution. Africa is referred as 'the largest island' on earth with oceans on all sides of the continent and a coastal line of 26 000 nautical miles. On top of that, 38 out of 55 African states are coastal countries or islands, and 90% of African trade is seaborne. These trading activities are facilitated by over a hundred port facilities in the region. The continent is therefore dependent on well-run ports, regulated shipping, and effective protection of its maritime resources. At national and regional level, there are however very few legal instruments specifically addressing the issue of cyberattacks on port facilities. Given the lack of attention that is given to this important aspect of maritime security and the lack of collective action from African states, the article seeks to analyse how cyber technology has affected the maritime domain of Africa as a whole. The article also reports on the consequences that could manifest should the cybersecurity of ships, ports, and their critical infrastructure continue to be ignored. In particular, the article addresses the following questions: to what extent do cyber vulnerabilities of African states extend offshore, and what should be done to address those vulnerabilities? What is lacking from the Convention on Cyber Security and Personal Data Protection adopted by the African Union? If maritime cybersecurity should be given focused attention, what is the task expected by the African Union and its member states? Taking into consideration the importance of this issue and in an attempt to address the research questions, the author sought to engage with policies, laws, regulations and other documents (both national and regional) that are currently guiding the area of maritime cybersecurity. Furthermore, the lack of maritime cybersecurity, and the resultant threats and vulnerabilities are addressed, hypothetical incidents are considered and previous incidents assessed, and current mitigation techniques and initiatives explored. After identifying the gaps in the legal framework adopted at national and regional level, policy recommendations are provided that could be implemented by the African Union and that could assist African states to tackle the challenges resulting from cyberattacks in the maritime domain.

Elsie Tachie-Menson (KAIPTC) covered the topic of maritime crime and cybercrime across the Gulf of Guinea: a hand-in-glove affair. As technology expands and spreads worldwide, the maritime industry and maritime crime are evolving rapidly. Although the increased use of digital technologies has proved beneficial in the effective and timely delivery of activities, such as maritime surveillance, policing, monitoring, and early warning, it also introduced serious drawbacks that affect its network of actors. This amalgamation can be attributed to geographical location, surveillance, and navigation systems of ports, vessels, and other state intuitions. With the emergence of cyber threats,

West Africa is poised to face a dual-pronged threat at its ports and shores, affecting the broader security environment of coastal states as more actors in the maritime domain increasingly use digital technologies. Moreover, these threats demonstrate a path for maritime criminals to evolve into maritime cybercriminals. The central theme of this article is the connection between cybercrime and maritime crimes, and the specific cybercrimes that have found a lucrative avenue in the maritime industry. The author also discusses cybercrime in maritime criminal activities occurring in West Africa and the implications for the maritime and cyber landscape of the region. Finally, she concludes with approaches for dealing with the risks posed by cyber maritime risks.

Chris Myers (Maritime consultant and researcher) contributed with a piece on assessing and managing risk within the African shipping sector. The African shipping sector is a significant enabler of trade within Africa, and of trade between Africa and the world. It sources and integrates technical systems of foreign suppliers and service providers into its vessels, ports, and maritime critical infrastructure that are cyber-enabled. Unfortunately, while providing the required functionality, these technical solutions create security vulnerabilities that place the African shipping sector at risk if security within the maritime cyber domain is taken for granted. Through this article, the author seeks to raise awareness of maritime cybersecurity in the context of the African shipping sector, and propose pragmatic steps to achieve such awareness.

Barend Pretorius and Brett van Niekerk (DUT) wrote on Industrial Internet of Things (IIoT) security for the maritime and related domains, the case of South Africa. The advent of the Fourth Industrial Revolution (4IR) has seen a rapid increase in connected 'smart devices' known as the Internet of Things (IoT). While this 'revolution' is most noticeable in commercial devices, there has been an 'evolution' in industrial devices, known as the IIoT. As Africa, and in particular South Africa, is racing to compete in the 4IR, various sectors, including the transportation sector, are introducing innovative projects. However, IoT and IIoT present cybersecurity risks. Cybersecurity itself is also a key component of 4IR; yet, organisations often neglect to consider the security implications of IIoT. A mixed-methods study was conducted to assess the security implications of IIoT in the South African physical transportation sector. Questionnaires were used with those working in the relevant fields to obtain quantitative data, and qualitative document analysis was conducted on frameworks for IoT and IIoT. The research aimed to evaluate and prioritise cyber threats, vulnerabilities, and appropriate countermeasures to mitigate the security risks associated with implementing IIoT in the transportation sector.

Brett van Niekerk (DUT) made a second contribution on a more specialist theme covering vulnerability of South African commodity value chains to cyber incidents. A commodity value chain can be considered as the 'route' from the source (provider) to the destination (client), including the various modes of transportation. This will often include some form of road or rail transport to a port for export to a destination country. Due to the rise in cybercrime and state-backed cyber operations, these commodity value chains may be disrupted, having a cascading affect down the value chain. Previous research considered this as a form of economic information warfare, and has indicated that state-sponsored cyber operations to disrupt a commodity intentionally would most likely fall below

the threshold of 'use of force' or 'attack' under international law. Subsequently, two pertinent instances of cyber incidents at ports have occurred: the disruption of a major Iranian port, and a ransomware incident at a South African major freight and logistics state-owned enterprise. Following the disruption resulting from the ransomware incident affecting South African freight organisations, there is a need to analyse the vulnerabilities of the sector to malicious cyber interference further. Expanding previous research, the author provides a specific look at the major commodity value chains in South Africa, their possible vulnerability to cyber incidents, and the potential implications thereof. In addition, publicly available information on the responses to the ransomware incident are discussed to gauge national readiness to crisis manage a major disruption to the primary trade mechanisms in the country.

A selection of book reviews by Dries Putter, André Wessels, Leon Steyn, Allan du Toit and Tilman Dedering concludes this special issue of *Scientia Militaria*.

The Guest Editors
Francois Vreÿ and Denys Reva