JOURNAL OF OCEAN GOVERNANCE IN AFRICA

JOGA VOLUME 3 2025

juta

Journal of Ocean Governance in Africa

First Floor, Sunclare Building,
21 Dreyer Street,
Claremont 7925

www.juta.co.za

ISSN: 2710-4044

Typeset in Melior 10.5pt on 13pt
Typesetter: Wouter Reinders
Cover design: Drag and Drop

Printed and bound by

CONTENTS

EDITORIAL TEAM

STEAMING TOWARDS CYBER-RESILIENT NAVIGATION: A REVIEW OF INDUSTRY READINESS AND THE EVOLVING REGULATORY LANDSCAPE

SAMKELISIWE NTULI[†]
Lecturer, Cape Peninsula University of Technology

As the maritime industry becomes increasingly digitised, shipboard navigation systems, including the Automatic Identification System (AIS), Global Positioning System (GPS), Radio Detection and Ranging (RADAR), and Electronic Chart Display and Information System (ECDIS), have emerged as critical vulnerabilities within the global supply chain. This paper evaluates the cybersecurity readiness of the maritime sector, highlighting the implications for African ocean governance and the regional blue economy. Adopting a qualitative doctrinal and comparative research methodology, the study analyses existing international legal instruments and South African domestic frameworks, such as the Cybercrimes Act 19 of 2020, to benchmark maritime standards against the robust regulatory regimes of the banking sector. The findings reveal significant gaps in maritime preparedness, characterised by a lack of harmonised standards and insufficient data-sharing protocols. The research argues that for African maritime nations to safeguard their waters and trade interests, a proactive regulatory shift is required, one that aligns with the 2050 Africa's Integrated Maritime Strategy (2050 AIMS). By adapting the successes of the financial sector's security frameworks, the maritime industry can strengthen its legal and technical resilience against evolving cyber threats.

[Keywords] 2050 AIMS, African ocean governance, banking cybersecurity, cyber- seaworthiness, cyber threats, doctrinal methodology, industry best practices, maritime cybersecurity, regulatory frameworks, risk management, shipboard navigation systems, vulnerability assessment

---

[†] NDip: Maritime Studies, BTech: Quality, PGDip: Shipping Law, LLM: Shipping Law, Chief Mate Certificate of Competency.

https://doi.org/10.47348/JOGA/2025/a4

I INTRODUCTION

The maritime industry underpins global trade, transporting over 90% of the world's goods.[1] This intricate network ensures the smooth flow of resources and finished products, fostering economic development and global connectivity.[2] However, this vital system faces a growing menace: cyber threats targeting shipboard navigation systems.

While traditional maritime security concerns like piracy persist,[3] cyberattacks pose a unique challenge. Unlike physical threats, cyberattacks can disrupt operations remotely, potentially rerouting vessels, manipulating cargo manifests, or even causing environmental disasters.[4] The interconnected nature of modern ships, heavily reliant on digital navigation systems Global Positioning System (GPS), Radio Detection and Ranging (RADAR), Electronic Chart Display and Information System (ECDIS),[5] creates vulnerabilities that malicious actors can exploit.[6] The consequences of successful cyberattacks can be devastating. Disruptions to global supply chains could trigger economic crises, delayed deliveries of essential goods, and ripple effects across interconnected industries. Furthermore,

---

1 Z Kosowska-Stamirowska et al 'Evolving structure of the maritime trade network: Evidence from the Lloyd's Shipping Index (1890–2000)' (2016) 1 *Journal of Shipping and Trade* 1 available at *https://jshippingandtrade.springeropen.com/articles/10.1186/s41072-016-0013-3* (accessed 1 February 2022).

2 L Martti 'Cyber Security in Aviation, Maritime and Automotive' in P Diez et al (eds) *Computational Methods in Applied Sciences Computation and Big Data for Transport Digital Innovations in Surface and Air Transport Systems* (Springer Nature 23 2020) available at *http://www.springer.com/series/6899* (accessed 3 February 2022).

3 ICC International Maritime Bureau 'Maritime piracy rises again in 2020' (2020) available at *https://www.hdi.global/infocenter/insights/2021/piracy/* (accessed 6 August 2021).

4 J King 'The Story You Aren't Being Told About Iran Capturing Two American Vessels' MPM News (2016) available at https://www.mintpressnews.com/the-story-you-arent-being-told-about-iran-capturing-two- american-vessels/212937/ (accessed 7 February 2022).

5 P H Meland et al 'A retrospective analysis of maritime cyber security incidents' (2021) 15 *The International Journal on Marine Navigation and Safety of Sea Transportation* at 519 available at *http://www.transnav.eu* (accessed 7 February 2022).

6 V Bolbot et al 'A novel cyber-risk assessment method for ship systems' (2020) 131 *Safety Science* at 1–2 available at *www.elsevier.com/locate/safety* (accessed 1 February 2022).

https://doi.org/10.47348/JOGA/2025/a4

the potential for environmental damage from accidents caused by manipulated navigation systems is a significant concern.

While the vulnerabilities of electronic navigation systems are a global technical concern, they pose a specific and existential threat to the burgeoning African Blue Economy. As maritime nations across the continent seek to implement the 2050 Africa's Integrated Maritime

Strategy (2050 AIMS), the security of shipboard systems becomes a prerequisite for regional economic stability and the protection of sovereign maritime domains.[7]

This paper addresses the critical escalation of cybersecurity threats within the maritime supply chain by evaluating the vulnerabilities inherent in modern shipboard navigation systems. Beyond technical risk, the study analyses the potential socio-economic consequences of cyber-interference and evaluates the industry's current state of readiness. To resolve these challenges, the research adopts a qualitative doctrinal and comparative methodology, critically measuring international maritime safety instruments against South African domestic frameworks, specifically the Electronic Communications and Transactions Act and the Cybercrimes Act. By determining whether these legislative models can be transposed to enhance ocean governance, this study proposes a path toward digital resilience within the broader African maritime sector, aiming to safeguard both the regional blue economy and the global trade networks it supports.

Despite growing awareness from industry bodies like the Baltic and International Maritime Council (BIMCO)[8] and regulatory authorities like the International Maritime Organisation (IMO),[9] current measures may not be sufficient. Cybersecurity is a rapidly evolving field, and adversaries constantly develop

---

7 African Union: 2050 Africa's Integrated Maritime Strategy (2050 AIMS) (2012) available at *https://faolex.fao.org/docs/pdf/UA179647e.pdf* (accessed 27 January 2026). The Strategy was formally adopted by the 22nd Ordinary Session of the Assembly of the Union in 2014.

8 BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021) available at https://www.bimco.org/about-us- and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed 6 December 2021).

9 International Maritime Organisation: Guidelines on maritime cyber security risk management (2017), available at *https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents*, (accessed 6 December 2021).

https://doi.org/10.47348/JOGA/2025/a4

new methods to exploit vulnerabilities. The maritime industry requires a proactive approach that emphasises continuous research and development of preventative measures to stay ahead of the curve.[10] Current African maritime governance frameworks, including the Lomé Charter, emphasise physical security and anti- piracy but remain largely silent on the 'silent' threat of cyber-interference.[11] This research argues that the industry's lack of readiness is not merely a technical failure but a governance gap that leaves African ports and shipping lanes susceptible to disruptions that could destabilise local economies dependent on maritime trade.

The vulnerability of African maritime infrastructure was starkly demonstrated in July 2021, when a major ransomware attack targeted Transnet, South Africa's state-run port and rail operator.[12] This breach forced the Transnet National Ports Authority (TNPA) to declare *force majeure* across all South African container terminals, reverting to manual processing systems and causing a massive backlog in the regional supply chain.[13] This incident underscored a critical weakness in African ocean governance: while physical port security is heavily regulated, the digital infrastructure supporting these ports remains exposed. The TNPA breach serves as a clear wakeup call that without robust cyber-governance and harmonised legal standards, the African maritime sector remains susceptible to systemic paralysis that threatens both national security and regional trade stability.

II RESEARCH METHODOLOGY

To rigorously assess the industry's readiness, this article employs a qualitative, doctrinal, and comparative legal research methodology. The legal analysis interrogates the interplay

10 M B Kao 'Cybersecurity in the Shipping Industry and English Marine Insurance Law' 2021 (45) *Tulane Maritime Law Journal* 467 at 472.

11 2016 African Charter on Maritime Security and Safety and Development in Africa (Lomé Charter) available at *https://lawlibrary.org.za/akn/aa-au/act/charter/2016/maritime-security-and-safety-and-development-in- africa/eng@2016-10-15* (accessed 27 January 2026). South Africa signed the Charter in 2016.

12 L Danielson 'Transnet ransomware attack' (2025) available at *https://www.huntress.com/threat-library/ransomware/transnet-ransomware* (accessed 27 January 2026).

13 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

between international maritime safety conventions, such as the IMO Guidelines, and the emerging continental frameworks intended to secure Africa's waters, specifically the 2050 Africa's Integrated Maritime Strategy (2050 AIMS) and the Lomé Charter. Furthermore, the study situates these international instruments within a domestic context by examining South African legislation, including the Electronic Communications and Transactions Act, the Protection of Personal Information Act (POPIA), and the Cybercrimes Act, to identify areas where the law is silent in current ocean governance.

Functionally, the research adopts a comparative approach to benchmark the nascent maritime cybersecurity framework against the mature regulatory regime of the banking sector. This comparison is not arbitrary; it is justified by the distinct operational parallels between electronic banking networks and shipboard navigation systems, both of which rely on interconnected nodes to transfer high-value assets across remote distances. By analysing the BIMCO guidelines alongside financial regulations like FICA, the study evaluates whether the 'transplantability' of banking's regulatory successes, such as mandatory reporting and zero- trust models, can provide a viable blueprint for enhancing legal and technical readiness within the African maritime domain.

III SHIPBOARD ELECTRONIC NAVIGATION SYSTEMS: A CRITICAL ANALYSIS OF OPERATIONAL PRINCIPLES AND CYBERSECURITY VULNERABILITIES

a) Introduction

Modern vessels rely on a suite of sophisticated electronic navigation systems (ENS) to ensure safe and efficient operations. These systems provide crucial information regarding a vessel's position, course, speed, and surrounding environment, significantly enhancing navigational capabilities and mitigating human error. This article examines the operational principles of key ENS components, including the Automatic Identification System (AIS), Global Positioning System (GPS), Radio Detection and Ranging (RADAR), and Electronic Chart Display and Information Systems (ECDIS). Furthermore, it critically assesses the increasing cybersecurity vulnerabilities associated with these interconnected systems, highlighting potential risks

https://doi.org/10.47348/JOGA/2025/a4

and proposing mitigation strategies. The interconnected nature of modern shipboard systems, while offering operational advantages, also creates potential attack vectors, making cybersecurity a paramount concern in contemporary maritime operations.

b) Operation of shipboard electronic navigation systems

(i) Automatic Identification System (AIS)

AIS is an automated broadcast transponder system that enhances maritime safety and collision avoidance by transmitting vital ship information, including identification, position, course, and speed, to other vessels and shore stations.[14] Operating within the VHF maritime mobile band[15] (using channels 87B and 88B), AIS leverages Self-Organising Time Division Multiple Access (SOTDMA) technology to manage message transmissions, accommodating over 2000 messages per minute.[16] This dynamic allocation of time slots minimises transmission conflicts and ensures efficient information dissemination.[17] AIS comprises a VHF transmitter, TDMA receivers, a DSC receiver, and a standard marine electronic communication link to shipboard systems.[18] It integrates a built-in GPS receiver for timing and position data, supplementing it with information from other onboard equipment like heading, speed, and rate of turn.[19] AIS operates in three modes: autonomous (continuous reporting based on vessel dynamics), polled/controlled (responding to

---

14 S Bhattacharjee 'What is Automatic Identification System (AIS) 0150 Types and Working (FAQs)' *Marine insight* available at *https://www.marineinsight.com/marine-navigation/automatic-identification-system-ais-integrating-and-identifying-marine-communication-channels/* (accessed 2 Feb 2023).

15 H Karahalios 'Appraisal of a Ship's Cybersecurity efficiency: the case of piracy' 2020 (13) *Transportation Security* 179 at 182, available at *https://www.researchgate.net/publication/344396341_Appraisal_of_a_Ship's_Cybersecurity_efficiency_the_cas e_of_piracy* (accessed 19 July 2022).

16 International Maritime Organization (IMO): Revised Guidelines for the onboard operational use of shipborne Automatic Identification Systems (AIS) Resolution A.1106(29) 1 at 17 available at *https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/AIS/Resolution%20A.1106(29).pdf* (accessed 2 February 2023).

17 Ibid at par 2.

18 Ibid at 15.

19 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

authorised interrogations), and assigned/controlled (remote configuration by authorities).[20]

(ii) Global Positioning System (GPS)

GPS, a crucial Global Navigation Satellite System (GNSS) component, provides continuous and highly accurate positioning, speed, and time information.[21] Developed by the US Department of Defence, GPS comprises three segments: space (satellite constellation), control (ground stations), and user (receivers).[22] A constellation of 24 satellites orbits Earth, transmitting radio waves that GPS receivers utilise to calculate position through triangulation.[23] The accuracy of GPS is influenced by factors such as satellite geometry, atmospheric effects, and clock errors.[24]

(iii) Radio Detection and Ranging (RADAR)

RADAR is a fundamental navigation tool used for collision avoidance and situational awareness.[25] It detects surrounding objects by transmitting electromagnetic pulses and analysing the reflected echoes.[26] The bearing and range of targets are

---

20 Furuno Class A AIS Operator's manual (2015) Japan, Furono Electric Co., LTD. iii, available at *https://www.furunousa.com//media/sites/furuno/document_library/documents/manuals/public_manuals/fa170_o perators_manual.pdf* (accessed 2 February 2023).

21 R W Sturdevant 'The navstar global positioning system: From military tool to global utility' (2012) 331 *Down to Earth: Satellite Technologies, Industries, and Cultures* available at *https://www.researchgate.net/publication/283483513_The_navstar_global_positioning_system_From_military_ tool_to_global_utility* (accessed 6 February 2023).

22 Federal Aviation Administration, USA. Global Positioning System Wide Area Augmentation System (WAAS) performance standard (2008) Department of Transportation, USA.1 at 2, available at *http://www.nstb.tc.faa.gov/* (accessed 6 February 2023).

23 International Maritime Organisation: Revised performance standards for shipborne Global Positioning System (GPS) receiver equipment (2000) 1 at 2, available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.112(73).pdf* (accessed 6 February 2023).

24 Federal Aviation Administration op cit note 23 at 3–5.

25 A G Bole, W O Dineley & A Wall *Radar and ARPA Manual: Radar and Target Tracking for Professional Mariners, Yachtsmen and Users of Marine Radar* 2 ed (2005) 1.

26 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

determined from the received echoes, providing crucial information for navigators, especially in restricted visibility.[27]

(iv) Electronic Chart Display and Information System (ECDIS)

ECDIS, an IMO-compliant computer-based system, replaces traditional paper charts with electronic navigational charts (ENCs).[28] It integrates data from various sources, including GPS, RADAR, and AIS, to provide a comprehensive navigational picture.[29] ECDIS systems can display both raster navigational charts (RNCs), which are scanned images of paper charts, and ENCs, which are vector charts containing detailed, interactive object information.[30] ENCs offer significant advantages in terms of data richness and dynamic updating capabilities. However, the availability of ENCs is not universal due to production costs.[31]

c) Cybersecurity risk assessment of shipboard electronic navigation systems

(i) Introduction

The increasing reliance on interconnected electronic systems has introduced significant cybersecurity vulnerabilities within the maritime domain. The 'Internet of Things' paradigm, while enhancing automation and efficiency, also exposes ships to potential cyberattacks. This section analyses the cybersecurity risks associated with the aforementioned ENS components.

(ii) AIS vulnerabilities

AIS, despite its benefits, suffers from inherent security weaknesses. Spoofing attacks can create fictitious vessels with

---

27 Ibid at 2.

28 International Maritime Organization (IMO) Resolution MSC.530(106): Performance Standards for Electronic Chart Display and Information Systems (ECDIS) (2022) 3 available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.53 0(106).pdf* (accessed 27 January 2026).

29 Ibid at 7

30 Ibid at 4 and 23

31 S Bhattacharjie 'What is Electronic Chart Display and Information System (ECDIS)?' *Marine Insight* (2021) available at *https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and- information-system-ecdis/* (accessed 6 March 2023).

https://doi.org/10.47348/JOGA/2025/a4

fabricated AIS data, potentially disrupting maritime operations and facilitating illicit activities.[32] This kind of attack has been used in various cases, mainly to 'conceal illegal fishing and other illegal activities' at sea.[33] From case studies, it can be said that AIS spoofing provides the attacker with endless scenarios, some of which may still be unknown, for conducting malicious acts, from crafting a fake vessel that can appear charging into another state's sovereign water to possibly start a war, to misleading an officer on board a ship to avoid a collision with a fake vessel which may lead to a targeted collision with another vessel, or even creating a fake distressed vessel to lure vessels to an attack.[34]

Hijacking attacks involve manipulating the AIS information of a real vessel, leading to confusion and potential misidentification.[35] This is achieved by intercepting the AIS communication midway and overriding it with a high-powered fake signal.[36] Therefore, what the receiving station gets on its end, is a modified version of the vessel's original message. This kind of malicious attack can ignite conflict, depending on the attacker's intentions. If used to conceal illegal activities, the perpetrators can steal another vessel's identity to shift blame.

Availability disruption attacks can disable AIS communications in a specific area, jeopardising safety and situational awareness.[37] This action will prevent all AIS transmitters and receivers within that area from communicating with each other.[38] Coastal stations use AIS to track and monitor traffic along the coast; should all AIS in a particular region suddenly shut down, coastal stations will lose effective control of the movement of vessels along their coastlines. Additionally, vessels relying on AIS information for navigation will be in a blind spot which may lead to collisions, depending on the amount of traffic and environmental factors. Furthermore,

---

32 A Androjna et al 'AIS Data Vulnerability Indicated by a Spoofing Case-Study' (2021) 11 *Applied Science* 1 at 9 available at *https://doi.org/10.3390/app11115015* (accessed 11 July 2022).

33 Ibid.

34 Ibid.

35 M Balduzzi, A Pasta & K Wilhoit 'A security evaluation of AIS automated identification system' (2014) *ACSAC* 436 at 438, available at *http://dx.doi.org/10.1145/2664243.2664257* (accessed 28 July 2022).

36 Ibid.

37 Ibid at 438–439

38 Ibid.

the attacker can command AIS transponders to change their frequency, thereby rendering the AIS useless, or delay the transmission, which will, in turn, prevent the vessel from transmitting its position; as a result, the targeted vessels or region will disappear from AIS tracking systems.[39]

(iii) GPS vulnerabilities

GPS is susceptible to both spoofing and jamming. Spoofing involves manipulating GPS signals to provide false position information, potentially leading vessels astray.[40] In June 2017, it was reported that hackers were able to interfere with the entire traffic in the Black Sea. According to the report, the GPS of a ship was altered to the extent that the position seen by the navigator on screen was out by 17 nautical miles from the actual position. During such time, no alarms were raised by the system to alert the navigator of foul play.[41] This incident did not affect only one vessel but the entire traffic within the spoofed region.[42] Though this attack did not cause any loss to the industry, it is a cause for concern as it has a potential for significant loss if the attackers decide to weaponise it to serve their cause.

Jamming involves overpowering GPS signals with radio frequency interference, effectively denying GPS access.[43] Both types of attacks can have severe consequences for navigation and safety[44]. The problem of jamming is made even worse by the fact that GPS jammers have become relatively more accessible in recent years.[45]

---

39 Ibid.

40 O Daum 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 8–9.

41 D Goward 'Mass GPS Spoofing Attack in Black Sea?' *Maritime Executive* available at *https://www.maritime- executive.com/editorials/mass-gps-spoofing-attack-in-black-sea* (accessed 8 July 2022).

42 Ibid.

43 International Association of Independent Tanker Owners (INTERTANKO): Jamming and Spoofing of Global Navigation Satellite Systems (GNSS) (2019) 1 at 4–5, available at *https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf* (accessed 6 March 2023).

44 Goward op cit note 42.

45 INTERTANKO op cit note 44.

https://doi.org/10.47348/JOGA/2025/a4

(iv) RADAR vulnerabilities

While hacking RADAR systems is considered more challenging than GPS or AIS, it is not impossible.[46] Interference, both intentional and unintentional, can degrade RADAR performance.[47] However, the presence of multiple redundant navigation systems often mitigates the impact of a single compromised RADAR.[48]

(v) ECDIS vulnerabilities

ECDIS vulnerabilities primarily stem from the process of updating electronic charts, which can involve internet downloads, USB drives, or CD/DVDs.[49] These methods introduce potential attack vectors for malware and unauthorised access.[50] Though ECDIS does not have a satellite connection, it is connected to servers that an attacker can remotely access. Additionally, research has shown that ECDIS presents cyber vulnerabilities that can impact other systems internetworking onboard.[51] This is due to the lack of robust end-to-end encryption and outdated security software within ECDIS systems.[52]

(vi) Recent cybersecurity incidents

Numerous cybersecurity incidents targeting shipboard systems have been reported in recent years, highlighting the growing threat. These incidents underscore the vulnerability of maritime navigation systems and the potential for significant disruption and damage.[53]

---

46 K Tam & K D Jones 'MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment' (2019) *Maritime Affairs* 1 at 11 available at *https://doi.org/10.1007/s13437-019-00162-2* (accessed 4 August 2022).

47 Ibid at 11–12.

48 Ibid at 12.

49 Ibid at 10.

50 Ibid.

51 Ibid.

52 B Svilicic et al 'Assessing ship cyber risks: A framework and case study of ECDIS security' 2019 (18) *Maritime Affairs* 509 at 514–517 available at *https://doi.org/10.1007/s13437-019-00183-x* (accessed 5 July 2022).

53 See Appendix A.

d) Cybersecurity risk measures for shipboard electronic navigation systems Addressing the cybersecurity challenges facing shipboard ENS requires a multi-faceted approach. Key mitigation strategies include:

(i) Limiting attacker resources

The most significant incentive when it comes to cybersecurity breaching has been feasibility.[54] The cost to the attacker on a single attack is meagre but yields excellent results, making it very appealing to the attackers. The devices used in cybersecurity breaches, such as spoofing and jamming, are easily acquired and affordable.[55] Increasing the difficulty and the cost of cyberattacks can deter potential perpetrators.[56] Strengthening the cybersecurity defences of navigation systems through upgrades and improved security protocols can reduce the success rate of attacks.[57] Cybersecurity upgrades on navigation systems may provide a degree of difficulty for the attacker, thereby reducing the success rate and rendering some hacking tools useless, limiting the scope of availability and incentives. However, achieving such a measure will require collaboration from all parties, including manufacturing, standardisation, and installation of ships' navigation systems.

(ii) Continuous risk assessment

Cybersecurity threats are constantly evolving, necessitating ongoing risk assessments to identify and address emerging vulnerabilities.[58] One can begin to draw up countermeasures by knowing the risk. It is this rationale that makes risk assessment an integral part of cybersecurity.[59] Regular evaluations and updates to security frameworks are essential to maintain

54 Daum op cit note 41 at 1–2.

55 Androjna op cit note 33 at 20.

56 Daum op cit note 41 at 11–12.

57 Ibid.

58 C Hemminghaus et al 'BRAT: A Bridge Attack Tool for Cyber Security Assessments of Maritime Systems' (2021)15 *The International Journal on Marine Navigation and Safety of Sea Transportation* 35 at 35, 36 and 42 available at *http://www.transnav.eu* (accessed 1 February 2022).

59 G Kavallieratos et al 'Shipping 4.0: Security Requirements for the Cyber-Enabled Ship' (2020)16 *IEEE Transactions on Industrial Informatics* 6617 at 6618–21, available at *https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9016093&isnumber=9128058* (accessed 7 February 2022).

https://doi.org/10.47348/JOGA/2025/a4

effective protection.[60] Various risk assessment tools involving test models, risk management programmes, etc., have been made available by different experts in the field.[61] However, one must acknowledge that, though effective, the feasibility challenge may make such tools unattainable to interested parties.

(iii) Cybersecurity awareness culture

Raising cybersecurity awareness among seafarers is crucial. Training programmes should emphasise the importance of cybersecurity best practices, including secure handling of data and software updates, and recognising signs of system compromise.[62] By raising the cybersecurity awareness culture onboard, navigators will be able to notice the signs of a

compromised system, thereby allowing for the engagement of cybersecurity protocols in due time. To achieve this, the industry must continuously remind seafarers of the importance of cybersecurity awareness onboard. However, even with the promotion of cybersecurity awareness onboard, success depends on the seafarer's honesty in following protocol.

(iv) Cybersecurity training

Awareness is not possible without proper training. Comprehensive cybersecurity training for seafarers is essential to equip them with the knowledge and skills to effectively respond to cyber threats.[63] Training should include practical exercises and simulations to prepare seafarers for real-world scenarios.

(v) Designated cybersecurity personnel

Training onboard is not conducted by a specified department that deals with staff development, as is the case ashore.

---

60 Ibid.

61 P H Meland et al 'A retrospective analysis of maritime cyber security incidents' (2021)15 *The International Journal on Marine Navigation and Safety of Sea Transportation* 519 at 526, available at *http://www.transnav.eu* (accessed 7 February 2022).

62 B Svilicic et al 'Paperless ship navigation: cyber security weaknesses' (2020)13 *Journal of Transportation Security* 203 at 204–205 available at *https://doi.org/10.1007/s12198-020-00222-2* (accessed 5 July 2022).

63 A Androjna et al 'Assessing Cyber Challenges of Maritime Navigation' (2020) *Journal of Marine Science and Engineering* 1 at 11 available at *https://www.mdpi.com/journal/jmse* (accessed 9 July 2022).

https://doi.org/10.47348/JOGA/2025/a4

Instead, training onboard is conducted by the officers as per the hierarchy, with the assumption that the officers have the proper knowledge. However, after analysing the research that has been conducted in this field of cybersecurity, one must appreciate the level of technicality that is required.[64] Cybersecurity breaches are not an issue that can be responded to with conventional means. As far as they fall under security, they are not a conventional security matter that can be combated by physical means only. It will take more than just a short course or a poster of the procedures on the bulkheads to fully understand what is required. For ship personnel who are already overstretched with their designated operational duties, it might be farfetched to expect them to adequately take the role of training, monitoring, and improving cybersecurity awareness onboard. Furthermore, being a nautical science or marine engineering officer does not automatically make one an expert in all trades. Appointing dedicated cybersecurity personnel, both ashore and onboard, can enhance cybersecurity management. These individuals can provide specialised expertise in cybersecurity protocols, risk assessment, and incident response.[65]

(vi) Cybersecurity reporting and information sharing

The industry is dealing with a new enemy which has the potential to do significant damage with just one attack.[66] They do not need to target a specific ship, and the attack can be targeted

on a specific region, affecting the entire fleet in that region.[67] Furthermore, the attackers do not rely on physical means to do damage but rely on technology and all its innovations.[68] To neutralise such an enemy, the industry must stay ahead in every way, e.g., research and development of its systems. This means the industry will need not only to deal with the known means of attack but also to forecast the enemy's possible attacks and fortify its systems against them.[69] Establishing robust

64 Ibid.
65 Ibid.
66 Daum op cit note 41 at 2.
67 P Kapalidis 'Cybersecurity at sea' in L Otto (ed) *Global Challenges in Maritime Security* (2020) 142, available at *https://doi.org/10.1007/978-3-030-34630-0* (accessed 1 February 2022).
68 Androjna op cit note 64 at 3.
69 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

reporting systems and information-sharing platforms is crucial for gathering data on cybersecurity incidents and disseminating best practices. Collaboration among stakeholders is essential to effectively address the evolving cyber threat landscape.[70]

(vii) Implementation and solidarity

Effective implementation of cybersecurity measures requires a concerted effort from all stakeholders.[71] International collaboration and resource sharing are essential to develop and enforce robust cybersecurity standards and protocols.

(viii) Conclusion

The increasing reliance on electronic navigation systems has revolutionised maritime operations, enhancing safety and efficiency. However, this dependence has also introduced significant cybersecurity vulnerabilities. Addressing these challenges requires a comprehensive approach that includes strengthening system defences, raising awareness, providing training, and fostering collaboration among stakeholders. By proactively addressing cybersecurity risks, the maritime industry can ensure the continued safety and security of navigation systems in the digital age.

IV MARITIME INDUSTRY CYBER RISK MANAGEMENT REVIEW

The increasing reliance on interconnected systems in modern shipping exposes maritime navigation systems to significant cyber security risks.[72] The exposure of critical navigation systems to such risks has compelled the industry to formulate specific cybersecurity guidelines. This section evaluates these primary frameworks, particularly those issued by the IMO and BIMCO, to gauge the sector's actual readiness. Crucially, this assessment is not conducted in isolation; it examines whether these international standards provide a sufficient regulatory baseline for the developing African maritime domain. By comparing existing global measures against the specific

---

70 V A Greiman 'Defending the cyber sea' (2020)19 *Journal of Information Warfare* 68 at 76–77 available at *https://www.jstor.org/stable/10.2307/27033633* (accessed 7 July 2022).

71 Ibid.

72 Daum op cit note 41 at 4–6.

https://doi.org/10.47348/JOGA/2025/a4

governance needs of the continent, particularly in light of the 2050 Africa's Integrated Maritime Strategy, the analysis highlights where the current regulatory regime falls short in protecting African waters.

a) The Lomé Charter (African Charter on Maritime Security, Safety and Development)

The Lomé Charter stands as a legally binding instrument designed to strengthen maritime security and safety across the African continent.[73] Adopted by the African Union, the Charter seeks to harmonise the actions of member states in preventing and combating cross-border maritime crimes while fostering a sustainable and secure Blue Economy.[74] Its provisions emphasise the necessity of regional cooperation and the establishment of national coordination structures to manage maritime risks effectively.[75] By providing a formal legal framework, the Charter encourages the development of shared security protocols and the promotion of maritime trade through the protection of vital shipping routes and port infrastructure.[76]

Despite its importance as a binding treaty, the Lomé Charter remains largely cantered on kinetic and physical threats, such as piracy, armed robbery, and maritime terrorism.[77] It provides minimal attention to the digital vulnerabilities of the maritime supply chain, offering no specific legal or technical standards for managing cyber-interference in shipboard navigation. As a result, the Charter currently lacks the specialised regulatory depth required to address the sophisticated cyber-risks that threaten modern maritime governance and the security of electronic navigation systems.

b) BIMCO guidelines on cybersecurity onboard ships

BIMCO's 2017 cyber security guidelines for ships provide a comprehensive framework for addressing cyber risks. Recognised by the IMO and widely adopted within the industry, these guidelines are regularly updated to remain effective against

---

73 *Lomé Charter* op cit note 12.
74 Ibid at 1-2.
75 Ibid at 6-7.
76 Ibid.
77 Ibid at 6.

https://doi.org/10.47348/JOGA/2025/a4

evolving threats.[78] They detail crucial aspects, including risk awareness, IT infrastructure protection, user authentication and authorisation, data protection, IT user management, ship-shore communication protocols, and cyber incident response planning based on rigorous risk assessment.[79]

BIMCO emphasises a collaborative approach, acknowledging that cyber security requires a concerted effort from all stakeholders, including shipowners, shipbuilders, hardware

and software developers, service providers, and onboard personnel.[80] Recognising the dynamic nature of cyber threats, BIMCO advocates for continuous innovation, risk assessment, and the development of adaptive prevention measures.[81] Within the context of African ocean governance, the practical application of these guidelines faces two significant hurdles. First, the non-binding nature of the BIMCO recommendations raises concerns regarding consistent enforcement across diverse African jurisdictions, where maritime law may not yet explicitly mandate cyber-compliance. Second, the feasibility of implementation, particularly for smaller regional operators, remains a concern. For these guidelines to be effective in securing the African maritime domain, they must be integrated into broader regional policy instruments to ensure they are not merely seen as international suggestions but as essential components of continental maritime safety.

c) The 2050 Africa's Integrated Maritime Strategy (2050 AIMS)

The 2050 AIMS serves as the overarching blueprint for fostering a secure and sustainable maritime domain across the African continent.[82] Developed by the African Union, this strategy provides a comprehensive roadmap for the 'Blue Economy', prioritising the protection of maritime supply chains and the enhancement of regional safety standards.[83] A key pillar of the 2050 AIMS is the achievement of 'Maritime Functional Awareness', which involves the seamless integration of technology and information-sharing to mitigate

78 IMO op cit note 10 at 4.
79 BIMCO op cit note 9.
80 Ibid at 8–10.
81 Ibid.
82 2050 AIMS op cit note 8.
83 Ibid at 7.

https://doi.org/10.47348/JOGA/2025/a4

diverse threats.[84] By establishing a shared vision for maritime governance, the strategy encourages member states to develop harmonised legal and technical frameworks, ensuring that digital security becomes an integral component of continental maritime security and economic development.[85]

Despite its strategic breadth, the 2050 AIMS remains primarily focused on traditional maritime security threats, such as piracy and illegal fishing, leaving a notable gap in its treatment of cyber-resilience.[86] The document offers limited guidance on the specific technical and legal standards required to protect shipboard systems from digital interference or systemic cyber-failures. Consequently, while the strategy provides a strong conceptual foundation for ocean governance, it lacks the specific regulatory mechanisms needed to address the unique vulnerabilities of a digitised maritime supply chain.

d) The Djibouti Code of Conduct (Jeddah Amendment)

The Djibouti Code of Conduct (DCoC), particularly through the 2017 Jeddah Amendment, represents a vital regional cooperation framework for maritime security in the Western Indian Ocean and the Gulf of Aden.[87] Originally focused on anti-piracy, the Jeddah Amendment significantly broadened the scope of the DCoC to include a wider array of maritime threats and the promotion of the Blue Economy.[88] It emphasises the importance of information sharing through regional centres and calls for the strengthening of national legislation to address maritime crimes.[89] By fostering inter-agency collaboration and regional capacity building, the DCoC aims to create a stable

---

84 Ibid at 8–10.

85 Ibid at 12 pars 21–22.

86 Ibid at 10 par 16.

87 2017 Revised Code of Conduct Concerning the Repression of Piracy, Armed Robbery against Ships, and Illicit Maritime Activity in the Western Indian Ocean and the Gulf of Aden Area (Jeddah Amendment to the Djibouti Code of Conduct 2009) available at *https://imcsnet.org/libraries/pdf.js/web/viewer.html?file=%2Fsites%2Fdefault%2Ffiles%2Fmedia_files%2FRevised-Code-of-Conduct-Concerning-the-Repression-of-Piracy-Armed-Robbery-Against-Ships-and-Illicit-Maritime-Activity-and-Gulf-of-Adan-Area.pdf* (accessed 27 January 2026).

88 Ibid.

89 Ibid at 39–41.

https://doi.org/10.47348/JOGA/2025/a4

maritime environment that facilitates secure trade and protects critical undersea and coastal infrastructure.[90]

However, while the Jeddah Amendment acknowledges the 'new and emerging' nature of maritime threats, it does not explicitly define or provide technical protocols for cybersecurity. The framework's emphasis on information sharing remains primarily geared toward physical vessel movements and criminal activities like trafficking, rather than the exchange of cyber- threat intelligence. Consequently, the DCoC currently offers limited practical guidance for member states on how to regulate or respond to the digital disruption of shipboard navigation systems, representing a significant gap in the region's collective security architecture.

e) IMO's regulatory response: Bridging the gap between voluntary and mandatory

The IMO's 2017 Guidelines on Maritime Cyber Risk Management, while initially presented as voluntary, represent a significant step towards regulatory enforcement.[91] These guidelines emphasise the crucial role of senior management in establishing effective cyber risk management practices.[92] Crucially, the IMO incorporated cyber security into the International Safety Management (ISM) Code.[93] This amendment mandates that shipping companies address cyber security risks within their safety management systems, subject to audit and verification.[94] This inclusion in the ISM Code, while not explicitly stating penalties for non-compliance, introduces a degree of compulsion, potentially driving compliance through the threat of legal repercussions.[95] However, the initial perception of voluntary compliance may lead to varying interpretations

90 Ibid.

91 IMO op cit note 10.

92 Ibid at 3.

93 Ibid.

94 Ibid.

95 The International Maritime Organisation (IMO) has a long history of adopting resolutions that are legally binding. For example, the IMO's ISM code is a legally binding treaty that sets international standards for the safety management of ships and imposes penalties for non-compliance, see IMO Knowledge Centre at *https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx*

https://doi.org/10.47348/JOGA/2025/a4

and implementation standards across the industry.[96] The IMO guidelines further advocate for the development of comprehensive guidelines incorporating national and international standards, best practices, risk control measures, and contingency planning.[97] While this holistic approach is promising, the timeline between guideline adoption and implementation raises concerns about the industry's ability to keep pace with the rapidly evolving cyber threat landscape.

Numerous other industry stakeholders have contributed to the growing body of cyber security guidance. These initiatives underscore the industry's recognition of the pervasive threat and the need for a unified response.[98]

f) Standardisation organisations: Setting benchmarks for cyber resilience

Organisations like the IEC (International Electrotechnical Commission),[99] ISO (International Organisation for Standardisation),[100] and NIST (US National Institute of Standards and Technology)[101] have developed standards aimed at ensuring cyber resilience within the maritime sector.

---

96 Voluntary guidelines are not legally binding. This means that organisations are not required to comply with them, and they can choose to interpret them in any way they see fit. However, the ISM code is a legally binding treaty. This can lead to different organisations having different understandings of what the guidelines mean, which can make it difficult to ensure that everyone is on the same page.

97 International Maritime Organisation Maritime (2017) 1 *Cyber Risk Management in Safety Management Systems* available at *https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).*pdf (accessed 6 December 2021).

98 There is a growing sense of urgency among the shipping industry to address the issue of cyber security. This has led to the publication of several guidelines by different entities in the industry, all of which spreads awareness on cybersecurity. See BIMCO Guidelines on cyber security onboard ships and IMO Guidelines on maritime cyber security risk management reviewed above.

99 International Organization for Standardization/International Electrotechnical Commission standard ISO/IEC 27001: Information technology—Security techniques—Information security management systems—Requirements (2013) Switzerland International Organization for Standardization, available at *http://www.itref.ir/uploads/editor/42890b.pdf* (accessed 6 December 2021).

100 Ibid.

101 National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 ed (2018)

https://doi.org/10.47348/JOGA/2025/a4

These standards provide frameworks for protecting critical infrastructure and address both technical and operational cyber security requirements for maritime assets.[102]

They cover vulnerabilities in systems operating within the maritime domain, offering a crucial foundation for robust cyber security practices.[103]

g) Classification societies: Tailored guidance for specific needs

Classification societies, including ABS (American Bureau of Shipping),[104] Lloyd's Register,[105] IACS (International Association of Classification Societies),[106] and DNV GL (Det Norske Veritas-Germanischer Lloyd),[107] have also released cyber security guidelines. These guidelines, often tailored to specific vessel types or operational contexts, provide detailed recommendations for vessel operators, owners, construction companies, and integration companies.[108] They address operational and technical cyber security measures, data integrity, and risk reduction strategies for both IT and OT systems.[109] The proliferation of these guidelines, while

---

available at *https://doi.org/10.6028/NIST.CSWP.04162018* (accessed 6 December 2021).

102 Ibid.

103 Ibid.

104 American Bureau of Shipping (ABS): Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS CyberSafety (2016) available at *https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf* (accessed 6 December 2021).

105 Lloyd's Register: Cyber-Enabled Ships—Deploying Information and Communications Technology in Shipping—Lloyd's Register's Approach to Assurance (2016) available at *https://www.lr.org/en/latest-news/early-adopters-and-innovators-in-connected-assets-on-ships/* (accessed 6 December 2021).

106 International Association for Classification Societies (IACS): Recommendation on Cyber Resilience Recommendation No. 166 (2020) available at *https://www.iacs.org.uk/publications/recommendations/161- 180/rec-166-new-corr1* (accessed 6 December 2021).

107 Det Norske Veritas-Germanischer Lloyd: Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation (2016) available at *https://www.dnv.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585* (accessed 6 December 2021).

108 Op cite notes 105 to 108.

109 Ibid.

demonstrating industry awareness, also highlights the need for harmonisation and standardisation to avoid confusion and ensure consistent implementation.[110]

The multitude of guidelines and initiatives demonstrates a clear industry-wide recognition of the cyber security threat. However, the question remains: does this activity translate into genuine industry readiness? While the progress is undeniable, several challenges persist. The voluntary nature of many guidelines, even with the IMO's inclusion of cyber security in the ISM Code, raises concerns about consistent implementation. The sheer volume of guidance from various organisations necessitates further harmonisation to avoid conflicting requirements. Finally, the rapid evolution of cyber threats demands continuous adaptation and innovation, requiring a proactive rather than reactive approach. Future research should focus on evaluating the effectiveness of these guidelines in real-world scenarios and identifying strategies to promote greater harmonisation and proactive cyber security management within the maritime industry.

V INDUSTRY READINESS FOR MARITIME CYBERSECURITY: A CRITICAL REVIEW

a) Introduction

While the global maritime sector has largely awakened to the reality of cyber threats, the transition from mere acknowledgment to active mitigation remains uneven. This growing awareness highlights the critical need for robust risk assessments, particularly within the developing regulatory architecture of African ocean governance. This section critically evaluates the industry's current state of readiness, contrasting existing operational practices against the comprehensive protective measures required to secure the African maritime domain and its supply chains.

b) Defining 'readiness'

'Readiness,' as defined by the Oxford Dictionary, is 'the state of being fully prepared for something'.[111] In the context of

110 Ibid.

111 *Oxford Online Dictionary* 'Readiness' available at *https://www.oxfordlearnersdictionaries.com* (accessed 12 July 2022).

https://doi.org/10.47348/JOGA/2025/a4

maritime cybersecurity, this translates to a state of preparedness that enables the industry to effectively identify and manage cybersecurity risks, facilitating early threat detection and responsive action to prevent or minimise losses and damage resulting from a breach. Effective readiness hinges on comprehensive planning involving all relevant stakeholders. This requires the integration of data from competent departments regarding identified risks, supported by strong leadership from top management. Crucially, assessment and planning must be followed by decisive action and continuous improvement.

c) Current state of industry readiness

(i) Existing measures

The industry has made some progress, evidenced by the development of guidelines and increased awareness through academic and expert publications (as cited in this study). The importance of continuous awareness campaigns and their implementation have been emphasised. Proposed measures include seafarer training, strengthening cybersecurity on navigation systems, and assigning designated cybersecurity personnel.

(ii) Gaps and challenges

- Lack of compulsion: A critical weakness is the absence of mandatory cybersecurity standards. While various guidelines and best practices exist, the lack of a unified, compulsory framework allows for considerable variability in implementation, potentially leaving vessels inadequately protected. This stems from the decentralised nature of the shipping industry and the potential cost of implementation. This lack of compulsion poses a significant risk, as a single vulnerable vessel can compromise the entire supply chain. Furthermore, it can erode public confidence in the industry.
- Absence of reporting procedures: The lack of established reporting procedures for cybersecurity incidents and near misses hinders effective learning and improvement. Unlike safety-related incidents, where reporting has significantly enhanced safety at sea,[112] cybersecurity breaches are often

[112] Section 9 of the International Safety Management Code (ISM) mandates accidents and near-miss reporting on hazardous situations.

https://doi.org/10.47348/JOGA/2025/a4

concealed due to fear of reputational damage.[113] This lack of transparency prevents the industry from fully understanding the scope and impact of cyber threats.

- Insufficient training: While training is recognised as crucial, its effectiveness is hampered by several factors. Training must extend beyond seafarers to the entire supply chain, acknowledging that breaches can originate from various points, such as during ECDIS installation (as highlighted by BIMCO guidelines).[114] Maritime-specific cybersecurity training programmes tailored to different roles and responsibilities are essential. Furthermore, challenges such as language barriers, time constraints, and a focus on compliance over genuine understanding, limit the effectiveness of current training practices. The absence of dedicated onboard cybersecurity experts further compounds this issue.
- Vulnerable network architecture: The common practice of using shared networks for both crew communications and ship operations creates a significant vulnerability. A single compromised crew device can provide a gateway for attackers to access critical ship systems.

(iii) Factors affecting industry readiness

- The unknown element: Cybersecurity threats are characterised by a significant 'unknown' element. The evolving nature of cyberattacks, the motivations of perpetrators, and the potential for these attacks to be linked to other criminal activities (e.g., piracy, terrorism) create a complex and unpredictable threat landscape. This uncertainty makes it difficult to anticipate and prepare for all potential scenarios. Furthermore, the lack of clear legal definitions for cybersecurity threats in shipping and the challenges faced by marine insurers in providing coverage for cybersecurity-related risks create further obstacles to effective mitigation.[115]
- Onboard challenges: Even with mandated cybersecurity measures, shipowners have limited control over

---

113 S Naoki, *Cyber Security Onboard* (2022) Tokyo, Japan, Nippon Kaiji Kyokai (ClassNK) 1 at 5, available at *https://www.classnk.com* (accessed 14 September 2022).

114 BIMCO op cite note 9 at 11.

115 Greiman op cit note 71 at 72.

https://doi.org/10.47348/JOGA/2025/a4

implementation once a vessel is at sea. Compliance relies heavily on the seafarers' good faith, which can be influenced by factors such as fatigue, stress, and language barriers. The lack of dedicated cybersecurity expertise onboard further weakens the ability to effectively manage and respond to threats.

d) Legal readiness: Navigating liability and the concept of cyber-seaworthiness

Industry readiness is frequently measured by technical defences, yet a critical and often overlooked component is the legal readiness to adjudicate the consequences of a breach. As this paper has established, the vulnerabilities of systems like ECDIS and GPS are significant. However, the conceptual difficulty lies in distinguishing between negligence, recklessness, and bad faith when these systems fail.

(i) From seaworthiness to cyber-seaworthiness

In traditional maritime law, a shipowner's duty to provide a 'seaworthy' vessel is absolute.[116] In the modern context, this must be expanded to include 'cyber-seaworthiness'. If a vessel is hijacked or grounded because of outdated software or an unpatched vulnerability, the legal question for International and Regional courts will be whether the shipowner exercised 'due diligence'. Currently, African ocean governance, including the frameworks under the Lomé Charter, lack a standardised benchmark for what constitutes a 'cyber-seaworthy' vessel. Without this, determining negligence becomes a subjective exercise, undermining the legal certainty required for a stable maritime economy.

(ii) The complexity of third-party liability

The intersection of cybersecurity and pilotage presents a distinct challenge for African port governance and the greater maritime domain. If a pilot introduces malware into a shipboard network via a Portable Pilot Unit (PPU), the lines between a pilot's professional negligence and a shipowner's vicarious liability

---

116 1968 Protocol to Amend the International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading (Hague-Visby Rules) art III available at *https://dgtr.de/wp- content/uploads/HagueVisbyRules19681979engl.pdf* (accessed 27 January 2026).

https://doi.org/10.47348/JOGA/2025/a4

become blurred. Under current South African law, such as the Cybercrimes Act 19 of 2020, unauthorised interference is criminalised, yet the civil liability for resulting maritime disasters remains abstract.[117] To move toward true readiness, African maritime states must develop a sustained doctrinal analysis that translates the concepts of good faith and bad faith into the practical realities of digital navigation.

e) Conclusion

Despite growing awareness and some initial steps, the maritime industry is not yet adequately prepared for the evolving landscape of cybersecurity threats. The lack of mandatory standards, insufficient reporting procedures, training deficiencies, and the inherent challenges of managing cybersecurity in a remote and complex environment create significant vulnerabilities. However, the study further reveals that technical and operational measures alone are insufficient for true preparedness. Achieving comprehensive readiness necessitates a concerted effort to bridge the existing legal and regulatory gaps within African ocean governance and the global maritime domain. This requires not only technical solutions and a focus on human factors but also a robust doctrinal framework to resolve the persistent ambiguities surrounding liability, negligence, and cyber-seaworthiness. Until regulatory bodies and industry stakeholders move beyond abstract guidelines to implement a framework that clearly defines accountability for cyber-incidents, the security of the African maritime domain and the global supply chains it supports will remain precarious.

VI BENCHMARKING CYBERSECURITY IN THE MARITIME INDUSTRY: LESSONS FROM ELECTRONIC BANKING SYSTEMS

a) Introduction

The maritime industry's increasing reliance on electronic systems, from navigation to cargo management, has exposed it to a growing threat of cyber-attacks. Recent incidents underscore the vulnerability of maritime targets, necessitating a proactive approach to cybersecurity. The recurring silence and gaps of key governing instruments on digital threats necessitates a

117 The Cybercrimes Act 2020 (Act 19 of 2020).

https://doi.org/10.47348/JOGA/2025/a4

comparative look at more mature regulatory environments, such as the banking sector. This section examines the cybersecurity vulnerabilities and countermeasures employed by the banking industry, a sector with extensive experience in combating cyber threats, to identify potential lessons and best practices applicable to the maritime domain. While benchmarking is a common practice, the relatively nascent nature of cyber threats in the maritime sector, coupled with the rapid evolution of these threats, necessitates continuous research and adaptation of cybersecurity strategies.

b) Background

Banks have been a prime target for cyber-attacks since the advent of electronic financial systems.[118] This sustained exposure has provided the banking sector with a deep understanding of cybersecurity risks and driven the development of sophisticated defence mechanisms.[119] Operating within a highly regulated environment, banks are compelled to remain at the forefront of technological and regulatory advancements in cybersecurity.[120] Both the maritime and banking industries manage high-value assets, some of which are remotely located and potentially vulnerable.[121] Furthermore, both sectors rely heavily on network connectivity and the integration of disparate systems, creating potential attack vectors. This research explores the cybersecurity vulnerabilities inherent in electronic banking systems and the countermeasures implemented to mitigate these risks, offering valuable insights for the maritime industry.

c) Comparative analysis of electronic systems operation

This section compares the operational principles of electronic banking systems with those used in maritime navigation,

---

118 International Monetary Fund 'The Global cyber threat' available at *https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm* (accessed 7 February 2023).

119 Ibid.

120 Ibid.

121 The banking sector moves large sums of money on a daily basis, and the maritime industry moves highly valuable cargo, making both these sectors very appealing to the perpetrators. Ships operate remotely from its operators, and ATM's and self-service electronic banking systems operate remotely from the banks, offering very little control for the operators.

https://doi.org/10.47348/JOGA/2025/a4

highlighting key similarities that justify benchmarking cybersecurity strategies.

(i) Electronic banking

Electronic banking utilises complex computer networks and telecommunication lines to facilitate digital fund transfers and real-time account management.[122] Access to these services is strictly controlled through authentication mechanisms, such as Personal Identification Numbers (PINs), to ensure transaction security.[123] The practical application and security frameworks of these systems are further illustrated through the examination of Automated Teller Machines (ATMs) and Internet Banking.

(ii) ATM

An Automated Teller Machine (ATM) is a computerised telecommunications device that facilitates remote financial transactions without human intervention.[124]

Comprising specific input peripherals and output mechanisms, the ATM functions as a node within an integrated network consisting of the terminal, a host processor, and the bank's central server.[125] On-premises ATMs are technically more advanced and support multiple services to complement a bank branch's capabilities. In contrast, remote ATMs are primarily designed for a single function based on the need for that location.[126] The host processor acts as a gateway, similar to an internet service provider (ISP), connecting the terminal

---

122 A Schaechter 'Issues in electronic banking: An overview' (2002) *Monetary and exchange affairs department* 1 at 3–4 available at *https://www.imf.org/external/pubs/ft/pdp/2002/pdp06.pdf* (accessed 6 April 2023).

123 B Chaimaa et al 'E-banking Overview: Concepts, Challenges and Solutions' (2021)117 *Wireless Personal Communications* 1059 at 1060–1061 available at *https://doi.org/10.1007/s11277-020-07911-0* (accessed 6 April 2023).

124 T Mahmood & S G Mujtaba 'Adaptive Automated Teller Machines' *Expert Systems with Applications* (2013)40 1152 at 1152–3, available at *http://www.elsevier.com/locate/eswa* (accessed 30 March 2023).

125 V K Lokesh 'The Formal Design Model of an Automatic Teller Machine (ATM)' (2013) 1 *Lecture Notes on Information Theory* at 56–58 available at *https://www.academia.edu/26612106/The_Formal_Design_Model_of_an_Automatic_Teller_Machine_ATM* (accessed 1 April 2023).

126 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

via leased-line or dial-up networks to the appropriate banking institution.[127]

The transaction lifecycle involves the host routing user inputs to the bank server for validation and fund transfer before authorising the final cash dispensation.[128] Crucially, this automated architecture mirrors the operational logic of Electronic Navigation Systems onboard ships, in both sectors, the system operates independently of constant human oversight, meaning the output reliability is entirely dependent on the integrity of the input data and verification points. Consequently, a compromise in any link of this communication chain results in erroneous transactions or, in the maritime context, navigation failure.[129]

(iii) Internet banking

Internet banking, a rapidly expanding sector of the digital economy, utilises personal computing devices to facilitate remote financial management.[130] By enabling direct transaction processing, ranging from international transfers to statement generation, users bypass the need for physical branch interaction or telephonic support.[131]

Accessible from any location via standard internet protocols, the system architecture bridges the user's interface directly with the bank's host processor through network service providers.[132] This direct linkage allows for the automated processing of service requests, effectively removing the human

---

127 Ibid at 58.

128 J Bowen 'How ATMs Work' available at *https://money.howstuffworks.com/personal-finance/banking/atm.htm* (accessed 30 March 2023).

129 Y Wang et al 'The Formal Design Model of an Automatic Teller Machine (ATM)' (2010)2 *IJSSCI*102 at 103 available at *https://www.researchgate.net/publication/220636950_The_Formal_Design_Model_of_an_Automatic_Teller_M achine_ATM* (accessed 30 March 2023).

130 K M Bansal 'Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis' (2020)19 *Elementary Education Online* 7724 at 7728 available at *https://www.ilkogretim-online.org/fulltext/218- 1659017731.pdf* (accessed 6 April 2023).

131 American Express 'Advantages and Disadvantages of Online Banking' available at *https://www.americanexpress.com/en-ca/business/trends-and-insights/articles/advantages-and-disadvantages- of-online-banking/* (accessed 6 March 2023).

132 B Chaimaa et al op cit note 124 at 1061–1063.

https://doi.org/10.47348/JOGA/2025/a4

intermediary from routine operations.[133] Advanced software logic distinguishes between fully automated tasks and complex requests requiring manual intervention ensuring seamless integration with the bank's broader electronic ecosystem.[134]

(iv) Similarities in system operation

Despite distinct functional outputs, electronic banking and navigation systems share a common operational architecture. Both rely on integrated, network-dependent pathways to process input data into actionable intelligence. However, these defined communication links create shared vulnerabilities to interception and exploitation. Furthermore, this comparison is functionally justified because both sectors operate on a 'trust-based' network architecture where valid inputs (whether GPS coordinates or SWIFT codes) are assumed to be true. Just as a bank verifies the identity of a depositor, a ship's navigation system must verify the identity of a signal transmitter, a protocol currently missing in maritime standards. It is this structural convergence that justifies benchmarking maritime cybersecurity strategies against the established protocols of the financial sector.

VII CYBER SECURITY VULNERABILITY AND MANAGEMENT OF ELECTRONIC BANKING SYSTEM

a) Background

As the global digital revolution accelerates, the banking sector's total transition from traditional to digital processes has created significant cybersecurity exposure. This chapter outlines the resulting vulnerabilities, specifically focusing on the breach points inherent in ATM architectures and internet banking systems.

---

133 Nedbank 'Online banking' available at *https://personal.nedbank.co.za/bank/digital-banking/channels/online- banking.htm* (accessed 6 April 2023).

134 S Islam & A S M Mahfuz 'Adoption of e-banking in Bangladesh: Evolution, status and prospects' 2014 *Int'l Conf. Computer and Information Technology, ICCIT 2013* 255 at 257 available at *https://www.researchgate.net/figure/The-Internet-banking-architecture_fig5_289334661* (accessed 6 April 2023).

https://doi.org/10.47348/JOGA/2025/a4

(i) ATM cyber security vulnerabilities

ATMs are a part of our daily lives; they offer the user a convenient banking experience outside the bank at any preferred time. However, this convenience is also accessible to malicious users, making it vulnerable to physical and remote hacking.

(ii) PIN card transactions vulnerability

ATM authentication relies on a two-step verification process involving the physical card and a Personal Identification Number (PIN). During this process, the background communication between the PIN Entry Device (PED) and the card often occurs via unencrypted channels.[135] This lack of encryption creates a primary vulnerability, providing a gateway for unauthorised interception and data duplication to facilitate fraudulent withdrawals.[136]

(iii) Hardware tampering vulnerability

Architectural weaknesses in ATM design often allow hackers to manipulate internal hardware without leaving physical evidence of tampering.[137] In terminals lacking anti-tamper protection, the Chip and PIN interfaces can be bypassed or replaced with fraudulent components. These unauthorised modifications grant attackers control over transaction data, enabling the theft of credentials and the creation of counterfeit cards.[138]

(iv) Skimming

ATM card skimming is amongst the popular card scams, where the hacker replaces the ATM card insertion terminal with a

---

135 S Navneet & R J Singh 'Analysis of different vulnerabilities in Auto Teller Machine transactions' (2012) 3 *Journal of Global Research in Computer Science* at 38 available at *www.jgrcs.info* (accessed 6 October 2022).

136 Ibid.

137 IBM Corporation 'ATM security: Identify and fix critical flaws in machines and the connected infrastructure— Remediate exploitable vulnerabilities by understanding how attackers can compromise machines' available at *https://www.ibm.com/case-studies/large-commercial-bank?cm_sp=CTO-_-en_US-_-OYDG2REZ* (accessed 6 October 2022).

138 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

fraudulent one.[139] When an unsuspecting user inserts the card, the card information is digitally stolen to make fake cards and gain access to the user's funds.

(v) Stand in time

This vulnerability arises during 'stand-in time', a database maintenance period where the dispensing network loses access to real-time account data.[140] To maintain customer service during this downtime, ATMs allow withdrawals up to a pre-set limit; however, the lack of database connectivity prevents balance verification, potentially enabling withdrawals that exceed available funds.[141]

(vi) Network vulnerability attack

ATMs are continually connected to banking systems through the network connection.[142] Hackers can intercept this connection by using computer programmes (malware) to breach flawed computer software and gain control of the ATM without leaving any noticeable evidence of foul play on the ATM.[143] Once the hackers gain control of the ATM, they can install their malicious software, which will allow them to have access to user's information and any other confidential information on the banking system, to use as they please.[144]

(vii) Cash-out vulnerability

An ATM cash-out attack targets the bank or payment processor's central systems rather than the physical terminal.[145] By gaining remote access to card management systems, often through phishing or malware, hackers disable fraud detection mechanisms and remove withdrawal caps on compromised or newly created accounts.[146] This allows coordinated groups to perform simultaneous, high-volume withdrawals until the ATMs are depleted.[147] Crucially, this exploit bypasses the

139 Navneet & Singh op cit note 136.
140 Ibid.
141 Ibid.
142 IBM op cit note 138.
143 Ibid.
144 Ibid.
145 Navneet & Singh op cit note 136.
146 Ibid.
147 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

terminal's local security by compromising the authorisation system at the source, demonstrating that the integrity of the network is as vital as the security of the hardware.

(viii) Internet banking cyber security vulnerabilities

While internet banking offers ubiquitous 24-hour access and unparalleled convenience, this hyper-connectivity creates an attractive attack surface for malicious actors. As with any digitised infrastructure, the removal of physical barriers invites sophisticated cyber-threats that target the system's accessibility.

(ix) Denial-of-service (DoS)

This attack prevents the targeted users from using a computer resource.[148] This is achieved by 'flooding' a network to block authorised network traffic, breaking up connections between two computers to block access to a service or a specific person, and interrupting service to a particular system or person.[149] This attack allows the hacker to access confidential information on the bank and its clients, thereby posing considerable risk to system security because financial information might be of strategic value to the legitimate users.[150]

(x) Repudiation

This kind of breach is possible on programmes/applications or systems which do not have controls to accurately track and log users' activities, making them vulnerable to repudiation attacks that allow for malicious manipulation or the creation of false action records.[151] Through this breach, incorrect data can be logged to log files by altering the authorising information of operations carried out by a malicious user.[152] The use of this information can be expanded to include general data

148 D Ghelani et al 'Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking' (2022) *American Journal of Computer Science and Technology* 1 at 6 available at *http://www.sciencepublishinggroup.com/j/ajcs* (accessed 9 April 2023).

149 Ibid.

150 Ibid.

151 M Vrîncianu & L Anica-Popa 'Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests' (2010)12 *The Amfiteatru Economic Journal* 288 at 391 available at *https://core.ac.uk/download/pdf/6492899.pdf* (accessed 9 April 2023).

152 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

modification done on behalf of others, thereby rendering the information in log files invalid.[153]

(xi) Man-In-The-Middle

Man-In-The-Middle is an attack in which hackers breach an existing connection to intercept transmitted data and introduce fake information.[154] It entails monitoring connections, breaking into connections, intercepting messages, and selectively altering data.[155]

(xii) Pharming

This breach is achieved by redirecting a user's internet connection to a fake website so that even though the user input address is correct it still gets directed to the fake website.[156] This is achieved by changing the host's file on the user's device or taking advantage of the Domain Name System (DNS) server software vulnerability.[157]

(xiii) Spoofing

Spoofing is identity theft that occurs when a person or computer effectively assumes someone else's identity by fabricating data and profiting from the situation.[158] This form of breach allows the hacker to access the user's banking credentials through various mediums, e.g., emails, fake websites, SMS, etc.[159]

(xiv) Conclusion

This non-exhaustive list of vulnerabilities demonstrates the operational parallels between electronic banking and maritime navigation. In both domains, infiltration techniques, targeting uninformed personnel, insecure network protocols, and legacy hardware, exhibit striking similarities. The primary objectives of these exploits remain consistent: system manipulation, data fabrication, and unauthorised access to sensitive information to mislead the operator. This convergence in threat vectors

153 Ibid.
154 Ghelani op cit note 149.
155 Ibid.
156 Chaimaa et al op cit note 124 at 1067
157 Ibid.
158 Vrîncianu & Anica-Popa op cit note 152 at 393.
159 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

justifies the use of the banking sector as a strategic benchmark for enhancing maritime cybersecurity resilience.

VIII CYBERSECURITY MANAGEMENT STRATEGIES OF ELECTRONIC BANKING SYSTEMS

a) Introduction

While national regulations vary, the global banking sector shares a common imperative: minimising illicit activity through robust cybersecurity frameworks. This section compares the regulatory approaches of South Africa, the United Kingdom, and the United States, serving as benchmarks for diverse cybersecurity management. By examining these distinct contexts, the study highlights universal challenges and divergent strategies in maintaining system integrity. This comparative lens identifies best practices for mitigating evolving threats, offering a blueprint for the maritime domain to address similar vulnerabilities.

b) Cybersecurity measures in the banking sector

(i) Common cybersecurity strategies

1. Encryption technology

Data security and privacy are paramount for financial institutions and their clients. To safeguard user information from cybersecurity risks, encryption technology has become the weapon of choice within the finance sector.[160] In addition to protecting data kept on computers and mobile devices, it secures data transported via networks, including ATM networks.[161] Encryption renders personal data unreadable without the appropriate authorisation or access keys, ensuring a secure transacting line.[162]

Using encryption technology in the banking sector helps protect, among other things, internet banking transactions, stop credit card fraud, and validate digital signatures when

---

160 K Arpan & D Supriya 'Cryptography in the Banking Industry' *Business Frontiers* (2012)1 1 at 2 available at *https://www.researchgate.net/publication/269405090_Cryptography_in_the_Banking_Industry* (accessed 15 April 2023).

161 Ibid.

162 Ibid.

https://doi.org/10.47348/JOGA/2025/a4

transferring money between accounts[163]. This makes encryption a crucial tool for protecting sensitive financial data from hackers who might use it to gain unfair advantage or hurt customers. Additionally, encrypting data can assist businesses in adhering to data protection laws.[164]

2. Third-party cybersecurity risk management

Any risk imposed on any company or institution by external partners in its supply chain is called third-party risk.[165] These parties could be vendors, suppliers, partners, contractors, or service providers with access to confidential data, systems, or procedures belonging to the company or its customers.[166] Similar to other sectors, the banking sector often relies on third- party vendors for their processes due to its advantages, e.g., cost-effective, risk reduction, regulation compliance etc.[167] However, companies usually lack complete control over or full transparency into third parties' security measures.[168] Though some third-party vendors have strict security guidelines and effective risk management procedures, others fall short.[169] This leaves a gap to be exploited in the supply chain and exposes the company to cybersecurity risks by giving hackers a more straightforward route to target even the most advanced security systems.[170]

The usage of third parties affects the company's cybersecurity in both direct and indirect ways, making third-party risk management crucial.[171] Third-Party Risk Management (TPRM) is the procedure for evaluating and reducing risks related to

---

163 U Dixit 'Cryptography – Security in E-Banking' (2017) *IOR Journals* 33 at 34–36 available at *https://www.iosrjournals.org/iosr-jbm/papers/Conf.17037-2017/Volume-2/6.%2033-37.pdf* (accessed 15 April 2023).

164 Ibid.

165 *G7 Fundamental Elements for third-party cyber risk management in the financial sector* (2023) 1 available at *https://www.gov.uk/government/publications/g7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector* (accessed 15 April 2023).

166 Ibid.

167 Ekran 'The importance of third-party vendor risk management for the banking industry' (2023) available at *https://www.ekransystem.com/sites/default/files/file_resources/third-party-vendor-risk-management-for-the- banking-industry.pdf* (accessed 15 April 2023).

168 Ibid.

169 Ibid.

170 Ibid.

171 *G7* op cit note 166 at 1–6.

https://doi.org/10.47348/JOGA/2025/a4

outsourcing to third-party suppliers or service providers.[172] Having TPRM policies in place helps reduce cybersecurity risk in the banking sector and complies with the data protection laws.[173]

(ii) South African approach

In South Africa, there is not a specific law governing cybersecurity yet. Instead, various pieces of law contain a jumbled collection of cybersecurity-related provisions. However, cybercrime is expressly addressed by several Electronic Communications and Transactions Act 25 of 2002 (ECTA) laws. ECTA covers every electronic transaction and data message. It makes unlawful acts involving computers like extortion, fraud, and forgery, as well as unauthorised access to, interception of, or interference with data, among other things, punishable by law.[174] The Regulation of Interception of Communications and Provision of Communication-related Information, Act 70 of 2002 (RICA), is a piece of legislation that, among other things, aims to control the interception of particular communications. Interception of direct and indirect communications is generally forbidden under RICA.[175] The Criminal Procedure Act (CPA) of 1977, which is South Africa's primary law governing criminal investigations and prosecutions, includes provisions for investigating and prosecuting cybercrimes.[176] The Protection of Personal Information Act of 2013 (POPIA) promotes the protection of personal data processed by public and private entities. It introduces several restrictions to set minimum standards for such processing.[177]

---

172 Ibid.

173 Ibid.

174 The Electronic Communications and Transactions Act 25 of 2002 available at *https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf* (accessed 8 October 2022).

175 The Regulation of Interception of Communications and Provision of communication-related Information Act 70 of 2002 available at *https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf* (accessed 8 October 2022).

176 The Criminal Procedure Act 51 of 1977 available at *https://www.gov.za/sites/default/files/gcis_document/201503/act-51-1977s.pdf* (accessed 8 October 2022).

177 The Protection of Personal Information Act 4 of 2013 available at *https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf* (accessed 8 October 2022).

https://doi.org/10.47348/JOGA/2025/a4

The South African banking sector also follows the Financial Intelligence Centre Act (FICA) and the Know Your Client policy (KYC).[178] Although the primary goals of FICA at the time it was implemented to combat terrorism, money laundering, and tax evasion offences. FICA, on the other hand, is a legal framework established to assist in identifying the proceeds of illegal operations.[179] Then, any further criminal activity targeted at the financial industry is implicitly included. Banks must adhere to the absolute minimum-security standards set forth by FICA to operate legally. To consistently research new methods to ensure users may conduct safe banking, this includes all assets tied to the bank.[180] For instance, banks have developed innovative ATM transactions to enable cardless transactions, preventing offenders from accessing user information and addressing the vulnerability of PIN card transaction skimming and other similar crimes.[181]

The verification process has also become more stringent, requiring not just the PIN or ID numbers but also phone confirmations, fingerprints, and eye and voice recognition. This enables the user to be informed in the event of a breach of the account and to be able to mitigate or neutralise the loss that would follow the breach.[182]

Additionally, the banking industry ensures that all workers receive regular training, ensuring they are all knowledgeable on risk management and relevant laws. They also endeavour to train users to ensure risk management and reduce vulnerabilities.[183] Furthermore, they collaborate with others in the industry to stay informed about the most recent security flaws criminals are trying to exploit. By doing this, they may develop new

178 The Financial Intelligence Centre Act 28 of 2001 (as amended) available at *https://www.gov.za/sites/default/files/gcis_document/201409/a38-010.pdf* (accessed 8 October 2022).

179 Ibid.

180 Ibid.

181 Nedbank 'How to withdraw at an ATM' available at *https://personal.nedbank.co.za/bank/digital-banking/needs/payments/cardless-withdrawls/withdraw-money-at-an-atm.html* (accessed 8 October 2022).

182 Ibid.

183 Nedbank 'Fraud awareness and prevention: Your guide to beating fraud' (2023) *Nedgroup Investments* 1 at 3–25, available at *https://www.nedgroupinvestments.co.za/content/dam/NGISingleSiteContent/pdfs/FRAUD%20AWARENESS%20 BOOKLET%202022%20RISK%20VERSION.pdf* (accessed 16 April 2023).

https://doi.org/10.47348/JOGA/2025/a4

risk-management techniques and offer their customers secure banking services.[184]

Annual audits of FICA compliance are conducted to verify compliance and those who fail to comply risk losing their certification and being unable to continue operating until the problem is resolved.[185]

In addition, the Cybercrime Act 19 of 2020 has been enacted to target any threats that are related to the Internet. The Cybercrimes Act is a significant statute that governs cybercrime in South Africa. It makes, among other things, the following types of online offences punishable by law and include a number of comprehensive provisions addressing cybercrime: 'Unlawful access to data, a computer program, a computer data storage medium or a computer system; unlawful interception of data; the unlawful and intentional use or possession of software and hardware tools in committing cybercrimes; cyber fraud; cyber extortion; cyber forgery and uttering; and malicious communications'.[186]

The Cybercrimes Act also includes provisions dealing with, among other things, cybercrime investigation, state-to-state mutual assistance, and reporting obligations for electronic communications service providers and financial institutions.[187] Electronic communications service providers and financial institutions must report to the South African Police Service (SAPS) any cybercrime offences that they become aware of, as soon as possible and, if possible, within 72 hours. This includes offences that are committed using their computer systems.[188] This will undoubtedly be a game changer in the fight against cyber security breaches, not just in the banking sector but in all cyber-related activities.

(iii) United States (US) approach

The banking industry in the United States has made significant progress in addressing cybersecurity breaches, both nationally and among state financial regulators. One example of this progress is the New York Department of Financial Services (NY DFS) cybersecurity requirements, which went into effect

184 The Financial Intelligence Centre Act op cit note 179.
185 Ibid.
186 The Cybercrimes Act op cit note 118 at ch 1 part 1.
187 Ibid ch 5.
188 Ibid ch 8.

https://doi.org/10.47348/JOGA/2025/a4

on 1 March 2017.[189] These requirements mandate that banks, insurance companies, and other financial services institutions under the NY DFS's jurisdiction establish and maintain a cybersecurity programme designed to protect customer information and IT systems.[190] Among the requirements proposed for regulated financial institutions are the following:

> Establishment of a cyber-security program; adoption of a written cyber-security policy; designation of a Chief Information Security Officer responsible for implementing, overseeing and enforcing the new program and its policy; annual penetration testing and bi-annual vulnerability assessments of an entity's information system; maintenance of audit trails to detect and respond to cybersecurity events, limitation and regular review of user access privileges, encryption of non-public information; establishment of an incident response plan; establishment of security policy for the third-party service provider.[191]

Because of this regulation, every company is required to conduct an analysis of the risks that are unique to their business and devise a plan to effectively mitigate those risks.[192] This matter needs to be taken very seriously by senior management, which also needs to take responsibility for the cybersecurity programme of the organisation and submit an annual certification confirming that it complies with these regulations. The cybersecurity programme of a regulated entity is required to protect the institution's safety and soundness as well as the customers of the entity.[193]

Furthermore, US financial institutions must follow the Bank Secrecy Act (BSA).[194] The (BSA), similar to the South African FICA, was enacted in order to better identify instances in which

---

189 New York State Department of Financial Services: Cybersecurity Requirements for Financial Services Companies 23 NYCRR 500 (2017) available at *https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23 NYCRR500.pdf* (accessed 8 October 2022).

190 Ibid s 500.0.

191 Ibid s 500.2–500.11.

192 Ibid s 500.9.

193 Ibid s 500.12.

194 Office of the Comptroller of the Currency *Comptroller's Handbook: Bank Secrecy Act/Anti-Money Laundering* (2000) available at *https://www.hsdl.org/?view&did=439815* (accessed 8 October 2022).

https://doi.org/10.47348/JOGA/2025/a4

money laundering is used to further a criminal enterprise, support terrorism, cover up tax evasion, or conceal other illegal activities.[195]

An advisory was published by the Financial Crimes Enforcement Network (Fin-CEN) of the United States Treasury Department in order to assist financial institutions in better comprehending their responsibilities under the Bank Secrecy Act (BSA) in regard to cyber- crime and cyber-enabled events.[196] This advisory also discusses the ways in which reporting mandated by the BSA helps authorities in the United States combat cyber events and crime that is enabled by the Internet.[197] FinCEN guides financial institutions through this advisory on:

> Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs); including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs; collaborating between BSA/ Anti-Money Laundering (AML) units and in-house cyber-security units to identify suspicious activity; and sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber- enabled crime.[198]

The Federal Banking Agencies (FBAs) took a similar approach to FinCEN when they issued an Advanced Notice of Proposed Rulemaking (ANPR) to establish enhanced cybersecurity standards.[199] The list continues according to different states, agencies, and jurisdictions, each with compelling regulations,

---

195 Ibid s 8.1.

196 Financial Crimes Enforcement Network (FinCEN): Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime FIN-2016-A005 (2016) available at *https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf* (accessed 8 October 2022).

197 Ibid at 2.

198 Ibid at 3–7.

199 Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation: Enhanced Cyber Risk Management Standards: Joint Advance Notice of Proposed Rulemaking Docket No. R-1550 (2016) available at *https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf* (accessed 8 October 2022).

https://doi.org/10.47348/JOGA/2025/a4

strategies, and guidelines for the financial sector to combat cybersecurity-related crimes.

(iv) United Kingdom (UK) approach

On 25 May 2018, the UK General Data Protection Regulation (GDPR) was enacted. The GDPR, among other things, significantly increases the accountability of all organisations that process personal data, significantly broadens the scope of individuals' data rights, and mandates that data controllers and processors put in place adequate and proportionate organisational and technical safeguards to protect personal data.[200]201 In addition, data subjects have the right to an efficient legal remedy against data controllers and processors in the event that they believe their rights have been infringed upon as a result of processing that does not adhere to the regulation.[201] This right is granted to them in the event that they believe their rights have been violated as a result of processing that.[202] Organisations must comply with the regulation's requirements for data processing and be able to prove it. Companies can show their clients that they are dependable and responsible by implementing an effective compliance strategy that helps them avoid costly fines and reputational harm.[203]

The Financial Conduct Authority (FCA) and the Bank and the Prudential Regulation Authority (PRA) jointly issued the final regulations and policies in March 2021.[204] The regulations are applicable to institutions that have been authorised and registered in accordance with the Payment Services Regulations of 2017 and the Electronic Money Regulations of 2011, including but not limited to 'banks, building societies, insurance companies, PRA-designated investment firms, recognised investment exchanges, enhanced scope senior managers, and certification regime firms'.[205] The regulations and guidelines that were intended to improve the operational

200 The Data Protection Act 2018 available at *https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.pdf* (accessed 10 October 2022).

201 Ibid at ch 3.

202 Ibid.

203 Ibid at ch 6 pt 6.

204 Financial Conduct Authority (FCA): Building operational resilience: Feedback to CP19/32 and final rules PS21/3 (2021) available at *https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf* (accessed 10 October 2022).

205 Ibid s 1.

https://doi.org/10.47348/JOGA/2025/a4

resilience of the financial sector went into effect on 31 March 2022. Companies now have until no later than 31 March 2025, to begin operating within their impact tolerances.[206] The FCA defines Operational resilience as 'the ability of firms, financial market infrastructures and the financial sector to prevent, adapt and respond to, recover and learn from operational disruption'.[207]

c) Conclusion

The regulatory maturity of the financial services sector offers a vital comparative blueprint for addressing the governance gaps currently present in the maritime domain. Unlike the nascent and largely voluntary frameworks seen in International and Regional Ocean governance, the banking industry has developed a resilient ecosystem defined by mandatory compliance regimes, standardised reporting, and clear liability structures. This resilience is not merely a product of technical innovation, but of a sophisticated legal architecture that enforces accountability while fostering proactive information-sharing networks. Having navigated cyber-vulnerabilities since the early stages of digitisation, the financial sector demonstrates that sustained operational growth is possible despite persistent threats, provided a multi-faceted approach is adopted. By benchmarking maritime preparedness against the established successes and ongoing challenges of the banking industry, the maritime sector can accelerate its own cybersecurity maturity, transforming abstract strategic goals, such as those in the 2050 AIMS, into enforceable and practical safety standards.

IX MARITIME INDUSTRY STATE OF READINESS IN RELATION TO BANKING SECTOR STATE OF READINESS

a) Introduction

The maritime and banking sectors are two of the most important and critical industries in the world. They are also two of the most vulnerable to cybersecurity breaches as both sectors rely on complex and interconnected networks.[208] The maritime sector

206 Ibid s 1 and ss 1.33.
207 Ibid s 1 and ss 1.23.
208 See sections III and VI above.

https://doi.org/10.47348/JOGA/2025/a4

relies on a network of ships, ports, and other infrastructure to transport goods and people around the world. The banking sector relies on a network of banks, financial institutions, and other infrastructure such as payment systems and data centres, to process financial transactions and provide financial services to businesses and individuals around the world. Both networks are complex and interconnected, using a network of computers, servers and other devices which makes them vulnerable to cyberattacks.

Furthermore, both sectors store sensitive data. The maritime sector stores data on ships, cargo, and passengers. The banking sector stores data on customers, accounts, and transactions.[209] This sensitive data is a valuable target for hackers. Additionally, both sectors are increasingly reliant on technology. The maritime sector is increasingly using technology to improve safety, efficiency, and productivity. The banking sector is also increasingly using technology to provide new services and products to customers.[210] This increased reliance on technology makes both sectors more vulnerable to cyberattacks.[211]

The research has shown the similarities between the shipboard electronic navigation systems and the electronic banking systems. In the maritime sector, electronic navigation systems are used to control and monitor ships. These systems are often interconnected with other systems, such as the ship's propulsion system, cargo handling system, and communications system.[212] In the banking sector, electronic banking systems are used to process payments, manage accounts, and provide other financial services. These systems are also often interconnected with other systems, such as the bank's customer relationship management system, fraud detection system, and risk management system.[213] This interconnection of systems creates a larger attack surface for cyber attackers. This is because there are more potential entry points for attackers to exploit. For example, if one system is not properly secured, attackers can use it to gain access to other systems.[214] However, although both sectors share similarities in their processes, their state of

209 Ibid.
210 Ibid.
211 Ibid
212 Ibid.
213 Ibid.
214 See sections III and VII above.

https://doi.org/10.47348/JOGA/2025/a4

readiness against cybersecurity breaches differs due to several factors highlighted below.

b) Banking and maritime sector relative state of readiness

(i) Background

What sets the banking sector apart from the maritime sector is that it has been a target for cyber- attacks for many years, and as shown in this study, they have developed some of the most robust cyber security measures in the world. Based on the comparison of cybersecurity risk management strategies for the two industries discussed in this study, it has been determined that the following are some of the reasons why the banking industry is further along in cyber security management strategies than the maritime sector.

(ii) Attack history

Because the banking industry has more experience dealing with cybersecurity breaches, more sophisticated security measures to protect their customers' data have been developed. The maritime industry, on the other hand, has only recently begun to recognise the significance of cybersecurity breaches, and as a result, it has not had to invest as heavily in cyber security.

(iii) Regulations

Due to many years in the fight against cybersecurity breaches, the banking sector has become heavily regulated, and these regulations often require banks to implement certain cybersecurity measures. The maritime sector, on the other hand, is still at the beginning phases in its fight against cybersecurity breaches, and as a result, still lacks cybersecurity regulations.

(iv) Resources

The banking sector has more resources at their disposal than the maritime sector, and these resources can be used to invest in cyber security. The maritime sector, on the other hand, has fewer resources, and as a result, they may not be able to invest as much in cyber security.

https://doi.org/10.47348/JOGA/2025/a4

(v) Culture

The banking sector has a strong culture of cyber security, and this culture is often driven by the need to protect customer data. The maritime sector has, for decades, enjoyed the protection of isolation and have not been exposed to cybersecurity breaches. It is through this rationale that it is believed that the maritime sector can learn a lot from the banking sector when it comes to cyber security management strategies and take advantage of what the banking sector have tried and perfected. In this way, the maritime sector will use what limited resources it has on strategies that are guaranteed to work.

c) A governance mandate for Africa

True readiness requires that the 2050 Africa's Integrated Maritime Strategy (2050 AIMS) be supported by domestic legislation that clearly defines liability for cyber-incidents. Just as the banking sector relies on the Electronic Communications and Transactions Act to assign liability for digital fraud, the maritime sector requires a regulatory blueprint that protects stakeholders from the 'unknown element' of cyber-interference. Until International and Regional ocean governance provides this conceptual clarity, the industry's readiness remains dangerously incomplete. Furthermore, under the current regional legal instruments, such as the Lomé Charter, there is no clear liability framework for a state-owned entity's failure, such as Transnet, to secure its digital ports, unlike the clear liability banks face under the ECTA for fraudulent transactions.

d) Banking sector strategies that might be used by the maritime sector

(i) Introduction

There are some strategies employed in the banking sector that the maritime sector might consider implementing. It is believed that for an industry that is resource-constrained, it might be beneficial to adopt and improve upon what has already been tried and tested. Therefore, using the little resources available to finding suitable ways to implement these strategies in their respective organisations rather than re-inventing the wheel.

https://doi.org/10.47348/JOGA/2025/a4

(ii) Implement a zero-trust security model

Through the data protection regulations and cybersecurity/fraud awareness campaigns, the banking sector has implemented a zero-trust security model which assumes that no one is trusted by default, not even the banks employees.[215] This means that all traffic, whether it is from an internal or external source, is subject to scrutiny. This helps to prevent attackers from gaining access to sensitive data or systems. Electronic navigation systems are often intercepted by hackers assuming identities of coastal stations, ships, or service providers.[216] With a zero-trust model, identity theft would be minimised.

(iii) Use multi-factor authentication.

This tool adds an extra layer of security by requiring users to provide two or more forms of identification before they can gain access to a system. This makes it much more difficult for attackers to gain access to accounts, even if they have stolen a user's password.[217]

(iv) Keep software up to date/encryption technology

Outdated software is one of the issues found on shipboard electronic navigation systems, making them susceptible to cybersecurity breaches.[218] Software updates often include security patches that can help to protect systems from known vulnerabilities that can be exploited by attackers. When software vendors release updates, they typically include fixes for security vulnerabilities that have been discovered. In addition to fixing known vulnerabilities, software updates can

---

215 In South Africa, the Financial Sector Conduct Authority (FSCA)'s requires banks to have a comprehensive cybersecurity programme in place which includes a number of principles that are consistent with a zero-trust approach, such as least privilege, micro segmentation, and continuous monitoring. Another example is the New York State Department of Financial Services (NY DFS) Cybersecurity Regulation which includes a number of requirements that are consistent with a zero-trust model, such as continuous monitoring, vulnerability remediation, and incident response. See section VIII above.

216 See electronic navigation systems cybersecurity vulnerabilities in section III above.

217 Nedbank 'Security is a top priority for Nedbank electronic banking channels' available at *https://businessbanking.nedsecure.co.za/download.aspx?tp=302&id=124* (accessed 6 April 2023).

218 Op cit note 217.

https://doi.org/10.47348/JOGA/2025/a4

also include new features and functionality that can help to improve security. For example, new security features may be added to software that can help to prevent attacks or detect malicious activity.

(v) Educate employees about cyber security

Employees are often the weakest link in a company's cyber security defences. They may click on phishing links, open infected attachments, or use weak passwords. This is even a bigger threat at sea due to the use of a common network point for private use and a ship's operation use. It is important to educate employees about cyber security risks and how to protect themselves and the company from attack.

(vi) Implementing a risk assessment

A risk assessment can help to identify the maritime sector's most critical assets and the threats that they face. This information can be used to develop and implement appropriate security measures. Risk assessments models have been developed within the sector, however, without implementation they are not useful.

(vii) Having a plan in place for responding to a cyber-attack

A cyber-attack can have a significant impact on any company's operations. It is important to have a plan in place for responding to a cyber-attack so that the company can minimise the damage and recover as quickly as possible. From the reported incidents in the maritime sector, it has been evident that the companies did not expect these attacks and as a result had no response plan in place.[219] In a very fast paced industry, there is no room for undue delays.

(viii) Working with partners

The maritime sector is a global industry, and cyber-attacks can come from anywhere. It is important to work with partners, such as shipping companies, ports, service providers and governments, to improve cyber security across the industry.

[219] See table of cases in Appendix A.

https://doi.org/10.47348/JOGA/2025/a4

(ix) Manage third-party risk

The maritime sector relies on a wide range of third-party vendors for a variety of services, including IT services, technician, manufacturers, logistics, and transportation. These third- party vendors may have access to sensitive data such as shipping data and routes etc. or critical navigation equipment. If a third-party vendor is compromised, this sensitive data could be exposed. The maritime industry can reduce the risks associated with third-party vendors and safeguard its vital infrastructure from cyber security breaches by implementing third party risk management strategies.

e) Possible challenges in the implementation of cybersecurity strategies in the maritime sector

It must be conceded that not all banking sector strategies can be adopted by the maritime sector. Though the sectors share similarities in the electronic systems, there are differences between the maritime and banking sectors when it comes to cybersecurity. For example, the maritime sector is more geographically dispersed than the banking sector and consist of a wide range of actors, including ship owners, operators, and ports. This can make it difficult to coordinate cybersecurity efforts and to ensure that all actors are taking the necessary precautions, therefore, creating a challenge in implementing and enforcing consistent cybersecurity measures. Additionally, the maritime sector is more reliant on third-party vendors than the banking sector. This makes it more difficult for the maritime sector to control its cybersecurity risks.

f) Conclusion

Despite these differences the similarities between the two sectors are such that there are reasons to believe that the maritime sector could profitably consider using at least some of the banking sector strategies together with what has been proposed and developed by industry experts to improve its cybersecurity position to the degree that it can be said, with minor exceptions, that it is ready for the fight against cybersecurity breaches.

X CONCLUSION

This article has argued that the current concept of 'industry readiness' in the maritime sector is dangerously narrow, often

https://doi.org/10.47348/JOGA/2025/a4

limited to technical defences while neglecting the necessary legal and regulatory architecture. As evidenced by the Transnet breach, the economic stability of the African maritime domain is inextricably linked to the integrity of its digital infrastructure. While international guidelines from the IMO and BIMCO provide a baseline, this study's review of regional instruments, including the 2050 AIMS, the Lomé Charter, and the Djibouti Code of Conduct, reveals a critical legislative void. These strategic frameworks, though vital for kinetic security, currently lack the specific mechanisms required to govern the complexities of cyber-risk, leaving the continent's 'Blue Economy' exposed to the 'unknown element' of digital interference.

The comparative analysis with the financial services sector demonstrates that true resilience is not achieved through voluntary guidelines alone but through a 'zero-trust' regulatory regime. The banking industry's success in establishing mandatory reporting and clear liability structures offers a viable blueprint for African ocean governance. Consequently, for the African maritime sector to transition from a state of vulnerability to true readiness, it

must move beyond aspirational strategies. It requires the codification of 'cyber-seaworthiness' into domestic law, ensuring that the legal definition of negligence keeps pace with technological reality. Only by harmonising these legal standards can African states and the greater maritime community secure their supply chains and assert effective sovereignty over their digital waters.

https://doi.org/10.47348/JOGA/2025/a4

APPENDIX A: REPORTED ELECTRONIC NAVIGATION SYSTEMS CYBER INCIDENTS (2008–2019)

Year	Incident	Details
2019	Navigation systems spoofing in the Strait of Hormuz	A British oil tanker, the Stena Impero, was seized by Iranian forces after the ship was spoofed into changing course into Iranian waters.[220]
2019	Malware on a US vessel	In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard Network.[221]
2018	ECDIS infected by virus	A vessel ECDIS was infected by a virus which resulted in undue delay on sailing Schedule.[222]
2017	Ships in Novorossiysk	At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32 km inland of their actual position. It is now believed to have been as a result of a GNSS spoofing attack.[223]

220 C Iphar et al 'An expert-based method for the risk assessment of anomalous maritime transportation data' (2020)104 *Applied Ocean Research* 1 at 4 available at *https://doi.org/10.1016/j.apor.2020.102337* (accessed 6 July 2022).

221 US Coast Guards 'Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels' available at *https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf* (accessed 6 July 2022).

222 BIMCO op cit note 9 at 11.

223 P Kapalidis op cit note 68 at 142.

https://doi.org/10.47348/JOGA/2025/a4

Year	Incident	Details
2013	Experiment on a yacht	GPS spoofing attack by a research team at the University of Texas on a Yacht.[224]
2008-2018	Illegal fishing activities	M/V Andrej Longov/Sea Breez1/ Ayda/STS-50 committed identity fraud by repeatedly falsifying her registry, producing multiple fake signals, and appearing in nearly 100 different locations simultaneously.[225]

[224] B Dodson 'University of Texas team takes control of a yacht by spoofing its GPS' available at https://newatlas.com/gps-spoofing-yacht-control/28644/ (accessed 7 February 2022).

[225] Iphar op cit note 221 at 4.

https://doi.org/10.47348/JOGA/2025/a4

NOTES TO CONTRIBUTORS

I INTRODUCTION

The editors of *Journal of Ocean Governance in Africa (JOGA) – Amalwandle Ethu* ('Our Seas' in isiXhosa) under the editorship of the South African International Maritime Institute (SAIMI), welcome the submission of manuscripts in English for publication, provided that the topic under discussion relates to ocean governance, including the law of the sea and maritime law, as it applies either in the whole African continent, in a specific African region or in one or more African States.

JOGA accepts manuscripts of four types. These are:

(a) **Articles**. Articles are the feature pieces of each issue of *JOGA*. They provide a detailed analysis of the topic under discussion. Articles should not exceed 12 000 words (including references). Longer manuscripts will only be considered in exceptional circumstances. All references must be footnoted. Each article must be accompanied by an abstract of not more than 200 words. The abstract should summarise rather than introduce the article. In addition, the article should include appropriate keywords.

(b) **Notes**. Notes are shorter, more focused pieces. They may discuss any specific issue, development, event, instrument or decision of interest to ocean governance in Africa. Notes should be between 3 000 and 8 000 words long. Longer notes are not considered. Notes do not include an abstract or keywords. All references must be footnoted.

(c) **Updates and reports**. Updates are brief descriptions of legal or policy developments which have taken place at the continental, regional or domestic level. Reports are brief summaries of events that have taken place or research that has been undertaken or is in progress. Updates and reports should not exceed 3 000 words. They do not include an abstract or keywords. All references must be footnoted.

(d) **Book reviews**. Book reviews are critical discussions of scholarly books on any topic relating directly or indirectly to ocean governance as it applies either in the whole African continent, in a specific African region or in one or more African States. Reviews should be between 2 000 and 5 000 words long. Longer reviews are not considered. All references must be footnoted.

A manuscript will be considered for publication:

(a) only on the assurance that it has not, in whole, in part or in substance, been published or submitted for publication elsewhere;
(b) on the understanding that it may be submitted in confidence to at least two expert referees for evaluation; and
(c) on the understanding that the editors reserve the right to make whatever changes they consider desirable:
    (i) to bring the manuscript into the house style of *JOGA*;
    (ii) to eliminate errors of typing, grammar, syntax, punctuation, spelling, idiom and the like;
    (iii) to eliminate ambiguity, illogicality, tautology, circumlocution and redundancy;
    (iv) to produce accuracy and coherence;
    (v) to improve the mode of expression and style of writing; and
    (vi) to avoid possible criminal or civil liability.

Authors are required to prepare their manuscripts very carefully to avoid the need for the editors to exercise extensively their right to make changes. In particular, authors are asked to acquaint themselves with the house style of *JOGA* and to check their manuscripts carefully against the guidelines that follow.

NOTE: Regrettably, a manuscript that does not accord with the house style of *JOGA* will be returned to the author(s) immediately, with a request that the manuscript be amended to conform to the house style. The quality of the piece will normally not be assessed before this has occurred.

II HOUSE STYLE

(a) General

What follows in this document are the stylistic requirements that most commonly require the attention of the authors and editors of *JOGA*. This document is merely a general guide because it is not possible to cover every possible referencing and stylistic issue. Where this document does not provide assistance, authors are requested to either:

(i) consult previous issues of *JOGA* and to see how a similar stylistic issue has been dealt with;

(ii) consult the main *House Style for Juta Publications*, which may be found at *https://www.jutajournals.co.za/jolga-style-guide/*; or
(iii) contact the editors for advice at Joga@saimi.co.za (the email address for the editing team).

(b) Matters of presentation and layout

(i) Page layout

The page should have 2.54 cm margins all round (top, bottom, left, right). Line spacing should be 1.15. The text must be right-justified.

All paragraphs (including those that come after long quotations) should be indented except the very first paragraph of a piece and any paragraph appearing immediately after a heading, subheading or sub-subheading.

There is no space after each paragraph except when the paragraph is followed by a heading (in which case there must be two line spaces after the paragraph) or a subheading or sub-subheading (in which case there must be one line space after the paragraph).

(ii) Font and type

A Times New Roman font is used by *JOGA*. The text must be in 12 point font. An 11 point font must be used for all indented quotations, ie long quotations of more than 40 words, which are preceded and followed by a 6 point space. Footnotes must be in 10 point font, with line spacing being 1.00 and the text being right-justified.

Italics are used for emphasis, for case names, names of journals and titles of books, plays, operas and films, names of ships and the titles of paintings and other works of art as well as for web sites and other electronic references. Italics are *not* used for foreign words. All italics in direct quotations are reproduced, however.

(iii) Titles of articles, notes, updates and book reviews

Titles of articles are in italics, right-aligned and always in caps in 14 point font. A line is left between the title and the author's initial(s) and surname, which are not in italics, are right-aligned and in 12 point font. The author's degrees are given in a footnote to the symbol † (and, in the case of a second author, ††) and

may be followed, in a separate sentence, by acknowledgements. The author's designation and affiliation appear immediately under his or her name, in italics, 12 point font and sentence case.

Titles of notes are in caps with, if applicable, case names in italics on a separate line. A line is left between the title and the author's initial(s) and surname, which are again in caps. The author's designation appears immediately under the name, in italics and sentence case. Degrees are not given but acknowledgements may be made in a footnote to the symbol † appearing after the author's surname.

Titles of updates are left-aligned and in bold. The first line indicates the relevant State, region or organisation in caps. The second line is in sentence case and contains the title of the update, which may be limited to the title of the relevant legal or policy instrument(s). The author's initial(s), surname, designation and affiliation are given in a footnote to the symbol †.

Titles of book reviews are left-aligned. The first line contains the title of the review in sentence case and in bold. The second line contains the reference to the book reviewed in sentence case and in the format in which the reference would appear if it were in a footnote with, in addition, the thirteen digits ISBN number. The initial(s), surname, designation and affiliation of the author of the review are given in a footnote to the symbol †.

(iv) Headings

All headings are left-aligned (other than headings of sections of *JOGA*). Main headings are in caps and bold. The headings in articles are numbered in roman numerals (e.g. 'I INTRODUCTION'). Subheadings and sub-subheadings are in sentence case. (a), (b), (c) are used for subheadings, which must be in bold. *(i), (ii), (iii)* are used for sub-subheadings, which must be in italics. Authors should avoid, wherever possible, going beyond sub-subheadings.

(v) Lists

(a), (b), (c) should be used for a list under a main heading and (i), (ii), (iii) should be used for a list under a subheading. Bullet points should only be used under sub-subheadings. Full sentences should start with a cap and end with a full stop. Phrases must start with lower case and end with a semi-colon (and a full stop right at the end of the list).

We use 'first' (not firstly); thereafter 'secondly', 'thirdly'.

(c) Spelling, grammar and other related matters of style or convention

(i) Spelling and capital letters

JOGA uses the 's' form of English spelling (e.g. recognise, emphasise, analyse, realise, organisation, but assets are 'realized'). We say 'in so far as' and not 'insofar as'; 'moneys' and never 'monies'.

Capital letters are used in all proper names (e.g. South Africa, Constitutional Court). They are also used in the English official title of legislation and international instruments as well as to distinguish between two different meanings of a word (e.g. 'Act' (the statute) and 'act' (the deed); 'Agreement' (the treaty) and 'agreement' (the act of agreeing); 'Constitution' (the supreme statute) and 'constitution' (the act of constituting); 'Convention' (the treaty) and 'convention' (the general agreement); 'Protocol' (the treaty) and 'protocol' (the formalities of a procedure); 'State' (the country) and 'state' (the condition or position)). Finally, capital letters are used by tradition in a few other cases, such as 'Parliament' (the highest legislative body) and 'President' (the head of a State).

Please note: Caps are not used for court, appeal court, judge, judge of appeal, committee, board, council, municipality, province, premier, etc. (When in doubt, use lower case.)

Examples:

The appeal was upheld by the Supreme Court of Appeal in 2011.

It is likely that the appeal court will turn down the appeal.

In terms of art 3 of the Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, …

The Nelson Mandela Bay Municipality is facing a number of challenges. Nevertheless, the Municipality has recorded several successes. Likewise, most other municipalities have …

… within the jurisdiction of the Minister of Home Affairs. No other minister may …

> … the already-ratified Conventions could be given effect …
> … there has been a 'follow-up' agreement to the 1990 Treaty in the form of the 1998 Protocol …

(ii) Numbers, dates, percentages, currencies

Use words for all numbers between one and twenty and for all approximations ('about two hundred years', 'a thousand ways'). Numbers higher than twenty must be in figures.

All numbers in tables and graphs are in figures. So are legislative provisions ('par 4'), ages ('5 years old'), percentages (*JOGA* uses the words 'per cent' in the text ('10.4 per cent'), and only uses the figure % in footnotes, tables and when it appears in a quote) as well as measurements, quantities and amounts ('12 nm', '6 cm', '40 km', 'ZAR 5 million'). It is advisable also to use figures where a lot of numbers appear in a piece, as a consistent style looks better. A space (not a comma) is used in large numbers, as for instance in '42 567'. Where a 'rand and cents' figure is used, the cents should be connoted by a short hyphen ('ZAR 456-45'). For other currencies, use USD, GBP, €, ¥.

A sentence should never begin with figures, ie recast the sentence or use words.

Dates and centuries: 'on the 4th of July 2008' (but 'on 4 July 2008' in Internet references and 'of 4 July 2008' in references to legal instruments); 'in the 1980s' (not 1980's – there is no apostrophe); 'in the 20th century'.

JOGA uses the long dash – (known in the publishing trade as the 'em rule') where the author wishes either: (i) to tack a word, phrase or clause onto the end of a sentence for emphasis; or (ii) to mark off a 'by the way' remark in much the same way as a parenthesis, but generally to give it greater emphasis.

> **Examples:**
> His expertise and loyalty are available – at a price.
> A policy shift is necessary to protect third parties – possibly unsophisticated entrepreneurs – who enter into pre-incorporation contracts.

In other circumstances, the short hyphen [-] must be used.

Examples:
Jean-Jacques.
Seven-year-old boy.

(iv) Quotations

Quotations are reproduced exactly, including all original italics and original punctuation, notwithstanding that the original forms might not comply with the *JOGA* style.

Quotations appear in single quotation marks. Quotations within quotations appear in double quotation marks. Back to single for the rare quotation within a quotation within a quotation.

Short quotations appear as part of the text. Long quotations, ie quotations of more than 40 words, are isolated from the text by being indented from both the left margin and the right margin.

Whenever a quotation is introduced by other words, the quotation should start with lower case (using square brackets to indicate an alteration where necessary). Ellipses need not be used at the start of a quotation but must be used in the middle and at the end of a quotation to indicate missing words. We use three dots for any missing word(s). We do not include in a quotation of up to 40 words the full stop at the end of that quotation. (Thus 'right […]'. and not 'right […].')

(d) Requirements for referencing standard legal sources

(i) International instruments

A reference to an international instrument must include the year of adoption and official name of the instrument (if not mentioned in the text) as well as the reference to where the instrument has been published, including the *UNTS*, *ILM* and *LOSB* references, if applicable. (See below for referencing style in the case where the instrument is only available on the Internet.) In addition, the reference must mention: the date of adoption (date, month and year); the date when the instrument came into effect or the fact that the instrument has not come into effect ('EIF: not yet'); and the status of the instrument with regard to the State(s) concerned (e.g. 'signed in 2002' or 'ratified in 2010'). In footnotes, 'UNGA' is used instead of 'UN General Assembly' and 'UNSC' instead of 'UN Security Council'.

Examples:
1982 UN Convention on the Law of the Sea [1833 *UNTS* 3, (1982) 21 *ILM* 1245; adopted: 10 December 1982; EIF: 16 November 1994]. South Africa ratified the Convention in 1997.
2000 Constitutive Act of the African Union [2158 *UNTS* 3; adopted: 11 July 2000; EIF: 26 May 2001]. South Africa ratified the Act in 2003.

Please note: The title of a Protocol must include the title of the instrument to which the Protocol constitutes an addition (e.g. 'the 2008 Protocol to the 2000 Constitutive Act of the African Union on the Statute of the African Court of Justice and Human Rights').

Please also note: Do not abbreviate the word 'section' when it is used to refer to: (a) a division within one of the seventeen parts of the UN Convention on the Law of the Sea; or (b) any similar division within another instrument.

(ii) Cases

All case names are to appear in italics. A shortened name should be used consistently in the main text, with the full name and citation being given in a footnote the first time the case is referred to. Additional parties are referred to using 'and Another' or 'and Others').

Examples:
M/V 'Saiga' (No 2) (Saint Vincent and the Grenadines v Guinea) 1999 ITLOS Reports 10 at 23.
Broad (Pty) Ltd v Thin 2008 (4) SA 456 (SCA) 15.

Page references (with marginal letters) may be given. Paragraph references must be provided when paragraphs are numbered. If the case is not reported in a published set of law reports (either at all, or has not as yet been published in this manner due to the decision being very recent), the author should please provide some form of citation for the purposes of reference. This could be a JOL or JDR citation, or a neutral citation used by the courts and SAFLII.

With the proliferation of electronic databases and neutral citations, there is less and less call for an author to refer to a case as being unreported. However, where it is necessary to do so, the *JOGA* uses two basic styles for unreported cases, the date being the date of judgment: '*Dlamini v Jacobs* (NPD) unreported case no 98/05 of 3 August 2006' or '*Dlamini v Jacobs* (NPD) unreported case no 98/05 (3 August 2006)'. In addition, the placement of the word 'unreported' may be varied in accordance with the structure of the sentence, e.g. 'in the unreported case of *Dlamini v Jacobs* (NPD) case no 98/05 of 3 August 2006 …'.

A full set of standard case abbreviations and citations may be found in the *House Style for Juta Publications*.

(iii) Books

All the author's initials and surname must be given as they appear on the title page of the book or on the title page of the chapter / relevant page of the article. For instance, 'John D Smith' must appear as 'J D Smith' and not as 'John D Smith' or 'J Smith'.

In a reference, the co-authors of any work (book, article, chapter, whatever) take an ampersand (e.g. 'J Smith & M Dlamini'). We cite up to three authors (e.g. 'J Smith, M Dlamini & R Pillay'). Thereafter use 'et al' (e.g. 'J Smith et al'). Avoid as much as possible to refer to authors in the text (rather give whatever credit is required in a footnote).

If the named persons are the authors of the book, then no more need be said. But if these are the editors, then the abbreviation (ed) or (eds) must appear after the last surname.

Book titles take the title case and appear in italics. If it is the first edition of the book, then no edition need be referred to; it will be assumed that it is the first edition. If the book is in an edition after the first, the number of the edition must appear after the title ('2 ed', '3 ed', '4 ed', not '2nd ed', '3rd ed', '4th ed').

The year of publication must appear in brackets after the title (in the case of first editions) or edition.

The precise page number(s) where the authority was found comes next, if necessary. If the book operates by numbered paragraphs (which may be connoted either by 'par' or by '§'), then this will be a sufficient reference. If it is necessary to refer to both paragraph and page, then do so as follows: 'par 27 at 160'. This latter method should be used only where absolutely necessary. Where the reference is generally to a chapter in

the book, this should be indicated by using the whole word (not 'ch').

Examples:
John D Smith & Sipho Dlamini *Hand's Law of Arbitration* 5 ed (2006) 115.
P Q R Boberg *The Law of Delict: Aquilian Liability* (1984) chapter 3.

(iv) Chapters in books

Where an author refers to a chapter in a book written by a specific author (most commonly in a book constituted of chapters by experts on a common theme and which have been collected and edited by a general editor or editors), then both the chapter and the book must be referenced in full the first time the work is cited.

The author must be referred to exactly as he or she was in the book and the titles of chapters in collections are always in sentence case and roman. The book is to be cited as above.

Example:
M Bear & D Bear 'Too hot, too cold, just right?' in M Goldilocks (ed) *The Politics of Cookery* 3 ed (2004) 23–27.

Some works (especially encyclopaedias and loose-leaf books) can give problems. Try to follow this style:

A J Kerr 'Lease' in W A Joubert (founding ed) *The Law of South Africa* (1999) XIV first reissue par 164.
Joe Bloggs 'Executive government' in S Woolman et al (eds) *Constitutional Law of South Africa* 2 ed (Service 12) 6-18.

(v) Journal articles

All the author's initials and surname must appear exactly as they appear in the journal being cited (the rules apply as for books).

The title of the article must appear in sentence case, in roman, and within single inverted commas.

The year (in brackets, except where there is no volume number), the volume (where relevant), the issue (in brackets and only where page numbers start again at page 1 in each

issue) and the title of the journal must be supplied. The title of the journal must be in italics.

The names of journals should only be abbreviated in the following cases:

AGR	African Geographical Review
AJICL	African Journal of International and Comparative Law
AJIL	American Journal of International Law
AJLS	African Journal of Legal Studies
AJMS	African Journal of Marine Science
ASR	African Security Review
AYIL	African Yearbook of International Law
CILSA	Comparative and International Law Journal of Southern Africa
EJIL	European Journal of International Law
ICLQ	International and Comparative Law Quarterly
IJMCL	International Journal of Marine and Coastal Law
ILM	International Legal Materials
JAL	Journal of African Law
JAUS	Journal of African Union Studies
JIML	Journal of International Maritime Law
JMA	World Maritime University Journal of Maritime Affairs
JMLC	Journal of Maritime Law and Commerce
JSAS	Journal of Southern African Studies
LA	Law in Africa
LMLJ	Loyola Maritime Law Journal
MLJ	Maritime Law Journal
MP	Marine Policy
OCLJ	Ocean and Coastal Law Journal
OCM	Ocean and Coastal Management
ODIL	Ocean Development and International Law
OY	Ocean Yearbook
RAAMT	Revue Africaine des Affaires Maritimes et des Transports
SAJIA	South African Journal of International Affairs
SAJMET	South African Journal of Maritime Education and Training
SAJMS	South African Journal of Marine Science
SAYIL	South African Yearbook of International Law

TMLJ Tulane Maritime Law Journal
UNTS United Nations Treaty Series

The numbers of the first and last pages always need to be indicated, followed, if applicable, by the number of the page(s) being referred to.

> **Examples:**
> G Abraham 'Lines upon maps: Africa and the sanctity of African boundaries' (2007) 15 *AJICL* 61–82.
> E de Coning & E Witbooi 'Towards a new "fisheries crime" paradigm: South Africa as an illustrative example' (2015) 60 *MP* 208–215 at 211.

(vi) Theses

D B Hamman *River and Maritime Boundaries between South Africa and Namibia* (unpublished PhD thesis, University of Cape Town, 1991) 134.

(vii) Newspapers

Angela Jones 'Nuclear reactor in trouble' *The Star* 24 May 2005 at 2.

(viii) White papers, etc

The White Paper on Energy Policy (GN 3007 in *GG* 19606 of 17 December 1998).

(ix) Law Commission papers

South African Law Commission Issue Paper 20 (Project 123) *Protected Disclosures* (2002) par 3.

South African Law Commission Discussion Paper 107 (Project 123) *Protected Disclosures* (2004) par 56.

South African Law Commission (Project 123) *Report on Protected Disclosures* (2007).

(x) The South African Constitution

The long citation (used when referring to the Constitution for the first time) is simply 'Constitution of the Republic of South Africa, 1996'. The interim Constitution is 'the Constitution of the Republic of South Africa Act, 1993 (Act 200 of 1993)'.

(xi) Legislation

Give the short title and year in the text (e.g. 'the Maritime Zones Act, 1994' or 'the Maritime Zones Act, 1994 (MZA)' (when you are referring to the Act and/or its specific provisions more than once)) and indicate the number and year of the statute in a footnote (e.g. 'Act 15 of 1994'). Thereafter, use the acronym (e.g. 'Section 4 of the MZA', 'See s 5–6 of the MZA').

Use abbreviations for 'section', 'subsection', 'paragraph', 'subparagraph' and 'article' (but never at the start of a sentence): section = 's', subsection = 'ss', paragraph = 'par', subparagraph = 'subpar', article = 'art'. The abbreviations are the same for the plurals. Please note that the above words are not abbreviated when they are not referring to a legislative provision.

Use 'annex', 'appendix' 'chapter', 'part', 'schedule' and 'title'.

(xii) Delegated legislation

A proclamation is cited as follows: Proc R46 in *GG* 24567 of 31 January 2003.

Regulations are cited by referring to the notice in which they appear, e.g. 'the Merchant Shipping (Navigation Bridge Visibility) Regulations, 2004 (GN R1199 in *GG* 26878 of 15 October 2004)'. A regulation is abbreviated to reg, as in reg 5(1) (but not at the start of a sentence).

(xiii) Internet references

Wherever possible, a published and authoritative source should form the basis of a reference. When it is not possible, authors may refer to websites, provided that the authors consider carefully how authoritative the source of the information is before using it.

Where an Internet reference is to be used, it must appear as follows:

> **Example:**
> African Union 'Decision on maritime security in Africa' (AU Doc. EX/CL/Dec. 60 (III) 2003, available at *http://www.au.int/en/sites/default/files/ex%20CL%20DEC%2020%20-%2074%20(III)%20_E_0.pdf*, accessed on 16 September 2013).

North Atlantic Treaty Organisation *Operation Ocean Shield Fact Sheet* (2012) (available at *http://www.nato.int/nato_static/assets/pdf/pdf_topics/1889-12_Factsheet_OOS_en.pdf*, accessed on 17 December 2013).

Please note: the URL must appear in italics, in black and must NOT be underlined.

When it is not possible to ascertain the date of the document or page to which one refers, '(no date)' must be used after the title of the document or page.

Where an author has accessed a published source on the Internet (e.g. a journal article accessed through WestLaw), the original citation should be given, and there is no need to refer to the URL. The exceptions to the above rule are newspaper articles accessed from the Internet, or resources such as law commission reports etc. from other countries, which may not be obviously or easily accessible to interested readers. For convenience, authors are strongly encouraged to give a URL reference over and above the reference to the published source.

(e) The use of footnotes

Authors are encouraged to use footnotes to elaborate on points that would otherwise clutter the main text of the contribution. The other important purpose of footnotes is to provide the relevant references without cluttering the text.

In footnotes, a reference to any authoritative source (which must comply with the house style described above) is given once in full. Apply the relevant requirements for referencing standard legal sources (see (d) above).

Thereafter a book, chapter, journal article, newspaper article, law commission report, thesis will be cited by author(s) and a cross-reference (using 'op cit') to the FIRST footnote, where the full reference appeared. An abbreviated reference to the work may be used to provide further guidance where appropriate (e.g. several of an author's works are cited sporadically in an article).

Examples:
Smith & Dlamini op cit note 5 at 67.
Dugard *International Law* op cit note 13 at 234.
See Ali op cit note 14 at 33, who expresses … .

Cases are also cited using the cross-referencing method, but 'supra' is used.

Examples:
Nottebohm supra note 12 par 34.
Supra note 16 at 365G–H.

For consecutive references to the same work, 'ibid' is used with or without a page number or paragraph reference as appropriate.

Examples:
Ibid.
Ibid at 45.
Ibid par 45.

(f) Miscellaneous

A name should appear in full before any acronym is used for it. The acronym must be introduced immediately after the full name it is referring to (e.g. 'the Benguela Current Commission (BCC) governs …'). (*JOGA* uses 'LOSC' for the 1982 UN Convention on the Law of the Sea and 'UNCLOS I', 'UNCLOS II' and 'UNCLOS III' for the UN conferences on the law of the sea.) However, this does not apply, in the footnotes, to acronyms that are very well known (e.g. AU, BRICS, EAC, ECOWAS, EEZ, EU, FAO, ICJ, ILO, IMO, ITLOS, NGO, OAU, PCA, SADC, UN, UNEP and US or USA).

If at all possible, avoid starting a sentence with an acronym or any other kind of abbreviation.

Where an entire sentence appears in parentheses, the full stop is placed inside the second bracket. (Here an entire sentence is bracketed.)

When giving starting and ending page numbers and paragraph numbers, do not remove figures (e.g. '34–35' and not '34–5').