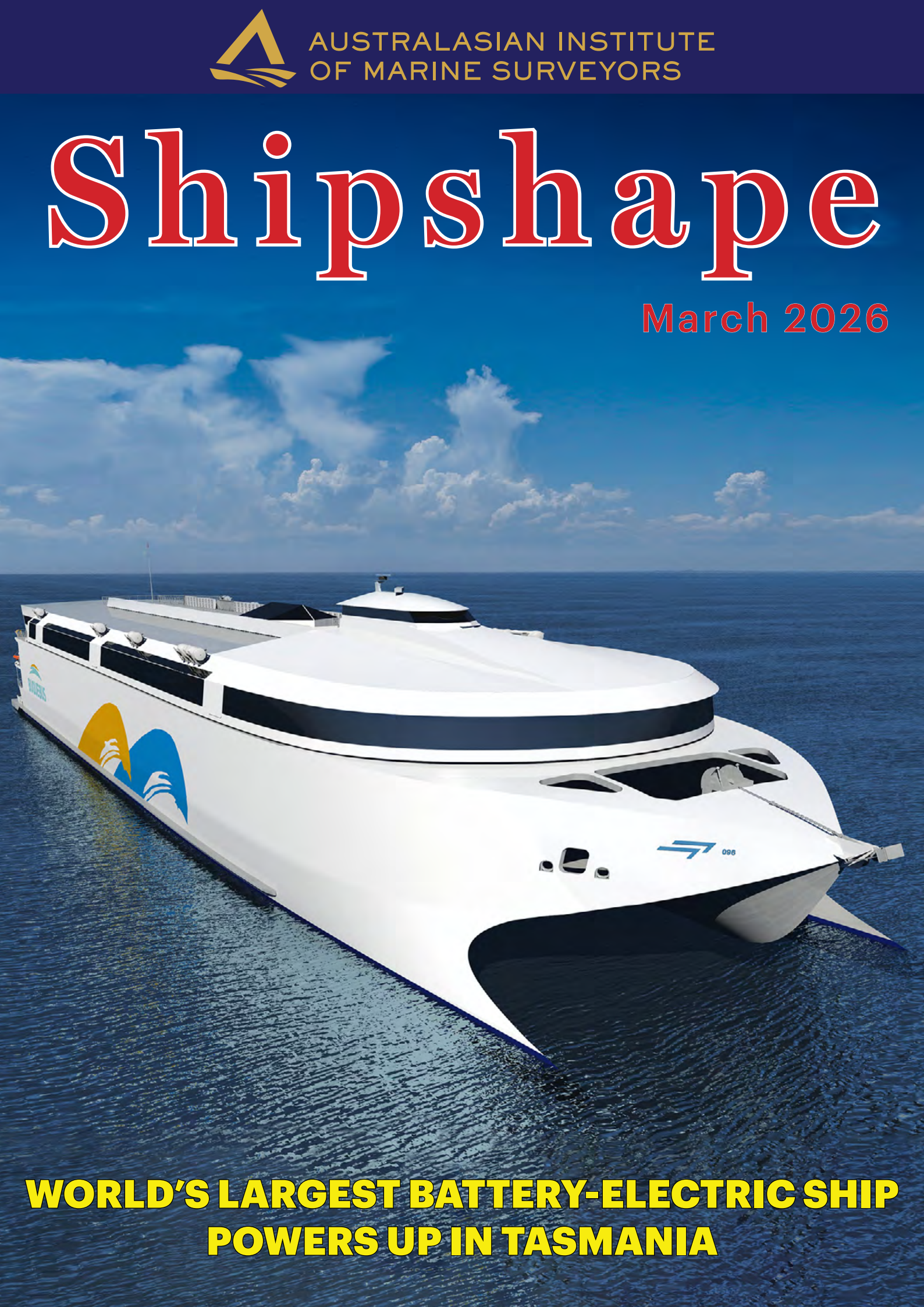
AUSTRALASIAN INSTITUTE
OF MARINE SURVEYORS

Shipshape

March 2026



WORLD'S LARGEST BATTERY-ELECTRIC SHIP POWERS UP IN TASMANIA

The impact of cybersecurity management in the maritime industry: threats and solutions

Ship at Bonny River – cybersecurity and cyberattack is home!

THE maritime industry has been impacted negatively by cyberattacks, even recently leading to losses in billions of dollars. The way forward is for a country and companies with large maritime coverage to pursue coordinated cybersecurity management by investing massively in the cyber-security industry in the maritime sector and embark on continuous training of maritime personnel.

To begin with, we must understand what cyber is and the source of derivation of cyber-security. A ship that is cyber-attacked in Bonny River may run aground into the Bonny oil and liquefied natural gas terminals and berthing facilities due to erratic behaviour of the engine and other computers, network, AI-aided navigation systems causing fires, especially during manoeuvring into port. Cyber-attack is that serious, systems can be jammed, and your location in Nigeria can be seen as if you are in an Australian port.

Origin of the word "cyber"

Who will ever believe in today's AI generation that from understanding the logics of mathematics and the use of its theory in controlling ship's steering gear and the rudder to give direction, including multi-faceted use of other machines and system communications for ship's motion will lead us to the word "cyber".

Well, that is what happened during the 1940s, when a mathematician named Norbert Wiener. of American origin, who understood the teachings of communication and control systems of machines in Greek terms, and thus derived from that wisdom the word "cybernetics" to mean a ship's "steer man" from the original Greek word of "kubernetes".

When you steer a ship, you are controlling the direction and communication; in the olden days, such communication was received initially through men who lined up from the ship's bridge to the aft steering gear flat, and later modernised by machine controls and currently aided by artificial intelligence (AI) innovation.

So, the communication of control from the bridge originally will be a shout like "Rudder Port Side"; that communication will pass through lined-up hands on deck until it reached the steering gear flat and the steer man who will finally activate the rudder control to port side for the ship's navigation.

The word "cybernetics" gained importance in the 20th Century when internet technology, cloud and submarine cables with computer aided networking becomes the order of the century in machine control.

The danger that accompanied these technological and engineering innovations led to genuine concern about security; that is, how safe, how secure and how being in charge of the happenings are we, resulting into what we now called "Cybersecurity".

The arising fear and danger from thinking about Cybersecurity is the belief, albeit a genuine belief, that the "bad child" may do something or attack, as we call it, to breach the

security or harm the control and communication technological internet systems. That something which the "bad child" may do is what is called Digital Cyberattack, which is regarded as a crime internationally.

The term "cybersecurity"

Arising from the explanation of the word cyber and security, the term "cybersecurity" is the assurance which a person or an entity or organisation envisaged to attain, to ward-off cybercrimes from bad child digital cyberattack of protecting systems, including attack on control internet networking, programs and data with storages, with the intention of accessing these systems, controls and storage facilities, and destroying any sensitive information or communication, thereby changing the smooth operational format of systems, simply for the purpose of:

- ❏ interrupting normal operation of business processes such as ship operations for the attacker's aggrandisement;
- ❏ extortion of money or unfair bargain or peculiar demand; or
- ❏ causing havoc and panics in the maritime community and industry.

Arising from the above definition it is evident that cybersecurity is about curing prematurely the effect of digital cyberattack which can bring about the following:

- ❏ maritime operational disruption;
- ❏ financial and wealth losses;
- ❏ fraud;
- ❏ data losses and breaches;
- ❏ mistrust about the personnel, about the systems and about the system providers;
- ❏ personnel or company identity theft; and
- ❏ privacy invasion of the company and the personnel in the maritime industry.

Cybersecurity management

Cybersecurity management cannot be understood without understating the concept of risk management.

The maritime environment is open to sea exploitation through the use of marine platforms and facilities, and sea trade facilitation by ships, all of which are prone to cyberattacks because of usage of current technological knowhow with internet and AI-aided computer system facilitation, and as such must involve cybersecurity management to be viable in the industry facing various cyberattack while experiencing plethora of local and international regime of regulatory control.

It is in this light that Widdowson 2003 stated that "Experts agree that the means of achieving the desired balance between trade facilitation and regulatory control is through the use of risk management". (David Widdowson, *Intervention by Exception: A Study of the Use of Risk Management by Customs Authorities in the International Trading Environment*, 2003, a thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy, University of Canberra, September 2003.)

Risk management

- ❏ In the world of international trade, there are four key stakeholders: the trader;
- ❏ the government;
- ❏ customs authorities; and
- ❏ the WTO (World Trade Organization) and the WCO (World Customs Organization).

The trader is more interested in his or her trade, and its facilitation for quicker and bigger returns with less restriction.

The government is interested in the revenues that come with trade, but exercises and enforces regulatory control over any form of trade that crosses its borders subject to its duty and maritime delimitation under UNCLOS, to overcome risk and now cybersecurity associated with trade movements.

Customs authorities are the primary checkpoint and in the forefront of ensuring compliance and deriving revenue for the nation through the ship-port maritime industry.

The WTO (World Trade Organization) and the WCO (World Customs Organization) are interested in facilitating trade, and encouraging agreements, conventions and treaties.

Also, of no less importance, are the International Maritime Organization which oversees the international law that supervises the legal activities on the seas through the United Nations Convention on Law of the Sea (UNCLOS) and other regulatory regimes, and the International Labour Organization, which supervises the Maritime Labour Convention 2006 (MLC 2006).

"Risk" is the danger posed by an activity such as cyberattack, which may have an immediate harmful effect or delayed harmful effects or loss targeted towards protected facilities of mobile or immobile maritime platforms, including ports facilities and ships.

The management of this risk is important to smooth operation of the maritime industry.

Risk management in the maritime environment is therefore border protection management, which requires profiling of ships by types, cargoes, crew nationality, last port of call and Flag State of the ship, used to enable the regulatory authorities to ascertain the level of risk associated with that ship or mobile facility, including the potential of digital cybersecurity attack likely to come from the marine vessel or towards the vessel as a target or random victim.

Sometimes, a cyberattack may not be targeted as such, but may be unleashed on random to catch unprepared victim or weak link of a system using internet technology and computer cloud data storage facilities.

The effectiveness of risk management strategies may reduce cost and increase government customs revenues, preserve interest of stake holders in the maritime front of international trade and improve trade facilitation.

Maritime control, enforcement and compliance have been an issue of contention among states and, in some instances, the issues in question have led to conflicts and "trade wars" between states. The contentions have always followed the same pattern of where does the maritime control, enforcement and compliance of a state begin and end such that it does not offend legitimate international activities flowing across boundaries.

Some issues that arise includes who to blame over cyberattack and from which country does the cyberattack emanate. This is important because an attack does not need to come from close range.

In the light of the understanding governing customs operations, the question that attends any regime in the maritime front was when a state can rightly claim that its maritime regulatory regime cum customs regimes are effective and in compliance with the existing customary law and international law regimes, and whether such regimes of policing have been breached by another, affecting its revenues drive.

It is arguable that a key performance indicator to improved customs revenue of a nation lies in the effectiveness of sea border management and risk management for a developing maritime nation such as Nigeria, in the West African region.

Nigeria offers a strategic location of ports and operation within the West Africa coastal maritime region. Nigeria is rich in crude oil and gas, and exports the same, while Nigeria imports various commodities, mainly by sea. Those attributes make Nigeria – a developing nation which adopted risk management and border protection management prescriptions with various ports of operation – a better case study to elucidate the impact of cybersecurity management in the maritime industry.

Nigeria has witnessed changes and experiences over the years, going by the Organisation for Economic Co-operation and Development (OECD) reports.

Nigeria is considered to be a regional leader in Africa, and in particular within the Economic Community of West African States (ECOWAS), on matters involving international trade, commerce, policy and practice.

Nigeria continues to play an important role in regional (Economic Community of West African States – ECOWAS), continental (African Union – AU) and international trade agreements. On the regional front, the ECOWAS customs union is viewed as a step towards an economic and monetary union with a single currency under the West African Monetary Zone (WAMZ). (AfricanEconomicOutlook2006-2007 www.oecd.org/dev/publications/africanoutlook)

Nigeria is a principal and founding member of the New Partnership for Africa's Development (NEPAD), which came into force in October 2001. The country is also a key member of the Economic Community of West African States (ECOWAS) and contributes significantly to the economic integration of the sub-region. (WTO 2005 page 6).

The OECD 2006 publication noted that seaports and inland waterways play a crucial role in shipment of freight. More than 80 per cent of Nigeria's merchandise trade is handled by the seaports. The navigable waterways are centred on the Niger and Benue rivers, which join at Lokoja and flow into the Atlantic Ocean. The coastal waterways extend from Badagry through Warri to Calabar, including Bonny to Port Harcourt. (AfricanEconomicOutlook2005-2006 www.oecd.org/dev/publications/africanoutlook, page 10.)

The body of knowledge available identifies risk management and border protection management as means of achieving appropriate balance between trade facilitation and regulatory control by the authorities; however, the impact of cybersecurity needs to be factored in the management to address the current risks posed by cyberattack in the maritime industry.

Cybersecurity needs to be coordinated as part of coordinated risk management strategies designed to facilitate trade and help the maritime industry move ahead of the effect of cyberattack. The concerns that the adoption of risk management will adversely impact, for instance the customs revenue of developing nations, are not realistic, as the COVID 19 pandemic shows that risk management strategy was the effective strategy in the circumstance and posed no concern that cannot be managed with coordinated risk management.

For a state to effectively harness its maritime resources to boost its customs revenue management drive and, in turn, its economy, and carry out its maritime responsibilities, it must have in place effective customs management, port control, border watch, sanitary and immigration control systems to allay fears, especially in terms of giving away sovereign control in the course of adopting

international collaborations, like the ABUJA MOU.

The management of cybersecurity in the maritime industry may be faced with jurisdictional constraint, the effectiveness of local and international laws, negative impact of porous border control of one jurisdiction on the revenue generation of another, and comparison of regulatory regimes and if any losses in terms of revenues arising from ineffectiveness of a given regime.

A regime may be too effective and cause losses to revenues, while, on the other hand, an ineffective regime enriches smugglers and cyber attackers to the detriment of the customs revenue drive.

Prior to the current influence of cybersecurity, and the use of Artificial Intelligence (AI) aided cyberattacks, Creck Buyonge was of the view that "there are three forces that are having an impact on the role of African customs administrations in this century.

"The first is the push for revenue optimization, an agenda pursued through revenue consolidation using the revenue agency model. The second is a demand for Customs to play a greater role in facilitating trade in the context of various preferential trade arrangements. The third is the requirement for Customs to take on more enforcement responsibilities either as part of a global Customs response to the threat of terrorism, or part of the mission of Customs to protect society and the nation through enforcement of various restrictions and prohibitions." (See Creck Buyonge, "Emerging Issues on the Role of Customs in the 21st Century: An African Focus" in the *World Customs Journal*, Volume 1, Number 1, p 55.)

In any event, maximisation of the use of communication technology has been long advocated, and Kafeero, in support of risk management in the East African Countries, stated that: " Apart from the provisions of Article VIII:1(c) of GATT 1994, it should be noted that the Revised Kyoto Convention has a lot to offer to trade facilitation through its key standards, principles and best practices that contribute to the simplification and harmonization of customs procedures and formalities.

"Such procedures and principles include standardized and minimum requests, minimum intervention and the use of risk management, separation of release from clearance, audit-based control, maximum use of information and communication technology, specially simplified procedures for authorized traders, and cooperation with other agencies as well as cooperation with foreign counterparts." (See Edward Kafeero, "Customs and Trade Facilitation in the East African Community (EAC)", *World Customs Journal*, Volume 2, Number 1, April 2008, p 67.)

In relation to current cyberattacks in our AI age, the suggestion of reducing the use of IT and other technologies is retrogressive. As far back as 2010, Enrique Fanta concluded that internationally agreed principles for improved border management included "Minimum intervention (based on identified risk), integrity, transparency and accountability, consistency and predictability. harmaonisation with international standards, improved cooperation with the private sector, coordinated approach to border management, maximum use of IT".

In examining the trend and growth in customs revenues since 2006 in Nigeria, it is pertinent to compare the context attending the growth with those that prevailed prior to the commencement of the government deregulation projects leading to the final adoption of the risk-based border management strategies in Nigeria.

Widdowson noted that: "Appropriate levels of both trade facilitation and border protection may be achieved and maintained, however, by incorporating supply chain security requirements into broader partnership arrangements between customs authorities and the private sector." (See Widdowson, David [2006], *Border Protection and Trade Facilitation – Are the Two Compatible?* p 9.)

Cybersecurity and cyberattack are not a one-sided issue: all stakeholders in the maritime industry must be involved to address the menace caused by cyberattack.

Border management

Goods of various kinds and people go through the border, including inshore and offshore economic infrastructures installations. However, the movement of some goods and people offends local regulatory regimes and, in some cases, international regulations, and in effect pose economic, political and social risks.

Some of the risk and unacceptable movement across the border includes illegal imports and exports, and people smuggling. Other matters which a country is under obligation to prevent include piracy, drug trafficking and slavery, illegal exploitation, acts of terrorism and home-grown cyberattack, to make the maritime industry safe.

The border management procedures adopted by one country may defer from that adopted by another and may compromise trade facilitation. It is more so that trade facilitation may be affected when there are various government agencies duplicating work and carrying out their authorised functions at differing times over the same goods, persons and infrastructures.

Coordinated border management

Coordinated border management is the contemporary, in-vogue approach to border management. This form of border management brings in to play at the same time all agencies of government sharing the same goals. Many experts have written on the topic of coordinated border management, listing its benefits as including efficient and cohesive response to border management operations, trade facilitation and improved border security. However, achieving this is also dependent on legislative coherency.

The intervening circumstances around the world may define the border administrative benchmark and the whole-of-government approach adopted by countries to the in-vogue coordinated border management.

In defining borders, Dunne – citing Ladley and White – suggested that "borders are places where governments exercise their sovereignty and that this is done by raising or lowering the fences into and out of the country to achieve a range of different policy objectives." (See Martyn Dunne, "New Zealand Customs Service: Changes Over the Last Decade and Into the Future", *World Customs Journal*, Volume 1, Number 1 [March 2007], page 42.)

While there are commentators on coordinated border management and different nomenclature of border protections aiming at the same purpose of coordinated border management, it appears none considered the implications (and, in particular, how the concept applies in a developing country such as Nigeria in the West African region) in the current AI and cybersecurity and cyberattack era.

The term "coordinated border management" (CBM) has been introduced in view of its encompassing nature. A 2009 Background Paper – WCO Inter-Agency Forum on Coordinated Border Management, introduces the evolved thinking of the WCO about CBM and outlines its major principles: coordinated border management (CBM) represents an approach to manage borders involving public-service agencies working across portfolio boundaries in a coordinated manner to achieve a shared goal, thus providing a cohesive government response to the challenges of border management.

CBM can be referred to as meaning a logical way to manage border operations to ensure efficient and effective processes and procedures used by all regulatory agencies who are involved in border security and regulatory requirements that apply to travellers, goods and conveyances crossing international borders.

The objective of a coordinated border management system is to facilitate trade and the clearance of travellers at the same time ensuring secure borders (WCO 2009, p. 5). (See Mariya Polner, page 52, Volume 5, Number 2, International Network of Customs Universities, *World Customs Journal*.)

The concepts of CBM have their antecedents in key WCO instruments, especially the International Convention on the Simplification and Harmonization of Customs Procedures (as amended) (the revised Kyoto Convention), and the SAFE Framework of Standards to Secure and Facilitate Global Trade (the SAFE Framework).

The revised Kyoto Convention entered into force in 1974 and was revised in 1999. One of the major principles of this convention was to simplify, as well as standardise, customs procedures. In particular, Chapters 3, 6 and 7 touch upon CBM mechanisms, such as the concepts of "juxtaposed office" and "joint controls", and the enhancement of international cooperation with other customs administrations. The standards relating to Single Window (Standards 7.3 and 7.4), which supports CBM through the exchange of information between the related ministries and agencies, are also stipulated in the Convention.

Techniques such as risk management (Standard 6.3) would benefit from the implementation of CBM, as it would assist in areas such as sharing information, intelligence and examination results. These actions will considerably enhance intelligence-driven risk management and promote coordination among the agencies. Thus a CBM approach, when used in conjunction with the standards and guidelines contained in the revised Kyoto Convention, provides a strong foundation upon which streamlining the border processes associated with both facilitation and control take place. (Polner, p. 51.)

Coordinated cybersecurity management

Coordinated cybersecurity management is akin to the approach to coordinated border management. It is a form of management that, when carefully adopted, brings into play at the same time all agencies of government and private stakeholders sharing the same goals – including international collaborations such as the Abuja MOU, for efficient and cohesive response to maritime cybersecurity threats and its management operations, trade facilitation and improved border security by making safe internet technology, computer, data and cloud data storages systems applicable in the maritime industry in protection of ships, cargoes and trade movements and facilitation.

However, achieving this is also dependent on legislative coherency and a willingness to act honestly in the interest of the maritime industry.

By the international collaboration under the Abuja Memorandum of Understanding (Abuja MOU), which is the MOU on Port State Control in West Africa and Central Africa, Nigeria arrested and detained the container ship *Athens Bridge* (IMO9409053, built 2009, with Panama flag) at Tin Can Island Port on 18 September 2025, arising from an inspection which showed various observations and inspection deficiencies. About nine deficiencies were outlined to warrant the detention by Nigeria's port state control inspector, who determined that the ship was unfit to proceed to sea and posed an unreasonable risk to the ship, its crew and the maritime environment.

Under the same MOU, Nigeria detained a container vessel MSC *Georgia II* (IMO:9357107, built 2007, Liberian flag) in Onne port in Rivers State on 8 September 2025, where the vessel revealed about 15 deficiencies. (These two vessels have since been released, having addressed the identified deficiencies.)

While the Abuja MOU appears to carry out its inspection work in compliance with the MOU and international collaboration to keep the maritime industry and environment safe, the website of the Abuja MOU Information System (AMIS) is developed and hosted by the Information and Coordinating Center on Port and Flag State Control of the Russian Federation in Moscow.

It is intended that such designed database collect and store Port State Control (PSC) inspection data from the Abuja MOU member states authorities and to provide information exchange on PSC data within the region.

This collaboration exhibited a form of coordinated risk management information sharing, usage, and storage to protect the maritime industry.

It is important to face reality from the above records: digital maritime has come a long way, and maritime organisations or entities are now using predictive maintenance deploying AI, which has exponentially reduced equipment downtime and cut maintenance costs and losses in time and revenue.

There is no doubt, given ships and the maritime industry usage of internet, computer technology that cyberattacks on shipping have dramatically increased in this AI era, with high costs of recovery in the millions for one incident.

However, with integrated systems of cybersecurity protection systems and effective collaboration, many shipping companies moving with the technology growth and with personnel training have less or no incidence of cyber-attack because of training and information harvesting enforcing cybersecurity.

Personnel and seafarers on board ships will benefit from basic cybersecurity training and ships with integrated bridge systems currently show significantly low navigation incidents, and substantially improved fuel efficiency with the new AI-aided technology.

Nowadays, remote monitoring and relevant integrated sensors with AI automation systems can predict engine failures months before they occur, and this will lead to prevention of breakdown maintenance. It is true that various roles in the maritime industry will change to make way for effective maritime cybersecurity, yet humans are not replaced, because people and machines complement each order for a better deal in our digital age.

In the olden times on board a ship, we shouted to reach the desired communication stations, say from bridge to engine room or steering gear flat, but now many ships do not use papers any more, and we have moved from the use of paper handwriting to smallest unit of digital picture display or pixels and thus invited cyberattack as we enjoy the sweetness of the technology rise in the AI-aided era.

About two decades earlier, there was regulatory change, allowing the International Maritime Organization (IMO) to make it mandatory for Electronic Chart Display and Information Systems (ECDIS), signalling a turning point from paper-based navigation about 2012. As at 10 January 2025, with AMSA's last update, Australia now requires up-to-date Electronic Navigational Charts ENCs for ships visiting Australia.

Internet and satellite connectivity becomes easier to use and adopte, but most radical changes were accelerated during COVID-19, with improved training such that inspections are conducted remotely, with digital exchanges meant to avoid contagious infection; but this drastically changed the maritime industry for good, with sea and shore-based operations becoming easier.

Now, AI-enabled machinery monitoring systems ashore detect faults that are not visible to the human eyes at sea, recalling a vessel back to port for maintenance sighted from shore, with a high degree of efficiency and accuracy.

It can now be said that AI and Digital recordings make it easier to demonstrate adherence to international and port control requirements for regulatory compliance, and easy communication for personnel.

The maritime industry is no exception to the tradition of scepticism for change, as this opposition to change appears real when one sees the trend of rapid change to AI machines as losing old knowledge and work status.

The real threats which now bring attacks also to the maritime environment include the following four.

Phishing attacks, which aim to trick uninformed or untrained crew members into sharing sensitive login details to enable the cyber attacker access the system to cause harm.

Ransomware, which, as the name indicates, aims to obtain financial and other benefits to ransom by locking or securing for harm critical navigation or operational systems, unless the said ransom was paid at a set location and time.

Disruption arising from remote breaches to stop bridge control operation, intended navigation blackouts, stopping or halting engines and other essential communication systems.

Internet and computer cloud-data connectivity enables efficiency, including quick data sharing for a real-time decision-making, however it also makes that data and the systems that run ships open to vulnerability, requiring essential investment in cybersecurity.

However, these threats, with effective investment in cybersecurity, can be significantly reduced by:

- personnel training in cyber defence before it happens, encouraging strong and unique passwords with notation to make regular changes of the password with many characters;
- making it a priority to avoid known unsecured devices or networks, or at least learn how to clean your footprint from the accessed network;
- being careful and slow to click to avoid bait, and not to open any unknown attachments or links without verification by a reliable authority or system in place for that purpose; and
- mandatory reporting of any iota of suspicious activity, even in the face of threats.

With cybersecurity at sea, all it takes is to transfer the already embedded culture of work safe and vigilance for safety in the maritime shipping industry to a cybersecurity management awareness in all personnel to avoid cyberattack that may affect or harm a ship's operations at sea or in port.

In any event, AI lacks the practicability of empathy in an immediate situation, and such ethical manoeuvre and emotional intelligence provide for the human's superiority over AI. Thus, while the use of AI appears inevitable, there are limits to its use.

Real tension amongst personnel can only be sensed by another human, and addressed by a human with emotional intelligence and the ability to provide a morale booster with empathy. It is the humans that remain when systems fail, and who correct the failure and meet the unpredictable realities of perils at sea.

The European Union's cybersecurity agency, reporting on 22 September 2025 about the disruption in airline operations in Europe, said that ransomware was deployed in the attack.

The attack affected check-in software of the US software provider Collins Aerospace. As part of investigation, the UK National Crime Agency reported that a West Sussex man in his forties had been detained. This cyber attack, demanding a ransom, disrupted several European airports, including Heathrow, which depended on the Collins Aerospace software.

The implication of this airline-operations cyber ransomware attack is that the maritime environment is not immune from attack, and active investment in cybersecurity is imperative to protect the maritime industry.

"Be prepared" is a Scout moto which the maritime industry must adopt, with extensive investment in cybersecurity, if the industry is to survive in our AI cyber threat age.

The recent European airport and airline lesson is what maritime companies and ship-owners and every seafarer must internalise, with the understanding that the maritime ecosystem is open to similar attack if we don't act now.

The use of flag of convenience may do the maritime industry more harm than good if inspections and verifying vessel condition are not taken seriously. However, while a ship may be registered in the country of the owner – or another country that may provide more benefits, including greater flexibility – effective maintenance is crucial in our AI world of cyberattacks.

Thankfully, the arrangement of a maritime Memorandum of Understanding, like the Abuja MOU, puts the duty on visited ports to ensure some compliance – and even arrest a vessel showing non-conformity or deficiency warranting detention of the ship.

The MOU allows the Port State Control (PSC) to inspect foreign ships in its national ports to verify that the operating condition of the ship and its equipment are in compliance with the requirements of all relevant international regulations and that the ship's crew is manning and operating the vessel in compliance with international regulations for maritime safety, security and

prevention of pollution to the marine environment.

The website of the Australian Maritime Safety Authority record for the Port State Control (PSC) states that: "While in an Australian Port, your ship may be subject to inspection. If your ship is found to have deficiencies, it may be detained until the issue is resolved."

These requirements put ships and ship owners is a state of preparedness before arriving in Australian ports. The Tokyo MOU, of which Australia is a member state, is also hosted by the Russian Federation, as is the Abuja MOU.

The bulk carrier *Navios Amethyst* (registered in Panama, built in 2022) was detained in the Chinese port of Zhangjiagang on 1 September 2025 for three deficiencies. In Port Hedland, Westen Australia, the bulk carrier *Frontier Garland* (registered in Panama) was detained on 1 September 2025 for a fire safety deficiency. (Both ships have since been released.)

PSC Code-15 means you can rectify your ship's deficiency at the next port, while a Code-16 must be rectified in 14 days and a Code-17 deficiency must be rectified before departure. However, a Code-30 is a detainable deficiency.

The world regional maritime delimitation for the purposes of compliance and detention of vessels under the PSC MOU like the Abuja MOU are grouped as follows.

- ❏ Abuja MOU: West and Central Africa.
- ❏ Acuerdo de Viña del Mar: Latin America.
- ❏ Black Sea MOU: Black Sea region.
- ❏ Caribbean MOU: Caribbean region.
- ❏ Indian Ocean MOU: Indian Ocean region.
- ❏ Mediterranean MOU: Mediterranean region.
- ❏ Paris MOU: Europe and the North Atlantic.
- ❏ Riyadh MOU: Persian Gulf region.
- ❏ Tokyo MOU: Asia and the Pacific.
- ❏ United States Coast Guard: A separate PSC regime.

Some countries belong to two PSC MOUs; for example, Australia has a dual MOU region of Tokyo and the Indian Ocean, while Canada also has dual MOU regions of Tokyo and Paris.

Risk profiling may lead to inspection of a ship and may vary between different MOUs, and the nature of deficiency may determine detention and type of regulatory requirement that will be applied for compliance.

Besides the PSC inspections, there are other external audits carried out, including classification authorities' verification processes, usually carried out for class survey renewal every five years, with in-between audits also carried out. These audits are also carried out for ports and ports facilities at port.

Oil tankers, gas tankers and chemical tankers have a special regime under the SIRE (Ship Inspection Report Programme) inspection, now SIRE 2.0, carried out under the direct supervision of the Oil Companies International Marine Forum (OCIMF), and are all prone to cyberattack.

There is also P&I Club Condition Survey, among others, with the only purpose being to ensure safety and be cyberattack-ready under the company safety management system procedures and manuals.

Threats and solutions in the maritime industry

AI and cybersecurity threats cut across all walks of life. The Chief Justice of Nigeria, Kekere-Ekun CJN, described the danger posed, stating: "With the increasing digitization comes the responsibility to secure sensitive judicial information from cyberattacks, data breaches

or misuse. Confidentiality is the lifeblood of trust in the judicial process. The robust protocols must be developed to safeguard data integrity and preserve the rights of litigants." (See *Cybersecurity in AI-Drive Justice Systems: The Bar, the Bench and Other Ethical Concerns*, Olumide Babalola.)

The increased digitisation is more felt in the maritime industry where a cyber breach can stop an engine, and an engine stop will sink the ship in rough weather. (For example, the Nigerian cargo ship *River Gurara* sank on 26 February 1989, during a storm, following engine failure off Cape Espichel in Portugal.) When a ship sinks, cargoes are lost and people can die at sea. The same thing applies when navigation equipment and data are breached and compromised by cyberattacks.

In 2017, Maersk ships and its cargo shipment logistics had the worst maritime cyber attack. Known as "Petya", it was a ransomware attack that spread through Maersk's global network, disrupting and shutting down its systems, leading to losses in the billions of dollars.

As recently as 10 November 2023, Australian ports managed by DP World were hit by a cyber attack that disrupted various operations affecting exports and imports and revenue from the ports. However, it was managed by responses that included disconnection of the systems from the internet, according to a DP World media statement.

It is certain that these cyberattacks and threats will continue unabated till effective solution are in place. In Australia, the telecommunication industry faces cyberattacks and is investing heavily in cybersecurity. Some of the companies involved provide services to ships at sea. The primary solution is training of all personnel to identify threats and to report any iota of threat The second is to invest heavily in cybersecurity programs and firewalls that are anti-cyberattack or at least minimise the effect of any attack.

Ensure personnel keep personal information private to avoid identity theft. The impact could be devastating to the ship or maritime facilities, and for the individual through loss of finances, credit cards details and loss of mental wellbeing.

Be prepared for sophisticated attacks. These attacks include email phishing, text smishing and other social engineering techniques, such as ransomware (where a ransom will be demanded to return the disrupted and breached system to normalcy).

Be vigilant with your communication and, before responding, be aware of who the person at other end is or represents.

Report your doubts, crosscheck and verify email addresses. Before you click any link or attachment, be sure of the author and the expectation from the link and attachments.

It is important that the procedure of the company prevent personal information through email or phone to a person that you do not know and does not represent a genuine business.

Use authentic company websites when required to do something unusual that awakens your suspicion.

If in doubt, go slow, and think carefully before you do anything further with any unknown request or attachment. Ask question from your superior or others if suspicion arises.

Be extremely careful when the demand comes with a sense of urgency, fear or curiosity, or seems unreasonable and greedy.

Check the greeting patterns and whether the target is your personal password or company-secured data, and ensure you change or update your software and password regularly.

Don't create the opportunities for the hackers by providing more information than asked or required in order to be polite.

Maintain software updates and preferably enable update automation to avoid forgetfulness. These days, some apps remind you to update. Personnel also need to be careful with the link provided by an app for update: it may come from attackers.

Make sure your password is beyond an ordinary guess to avoid easy access and being a weak link.

Make it mandatory that you do not use one password for two or more platforms; depending on sensitivity, multiple stages of verification should be activated.

Even in Freetown, things are not free, so be careful when invited to use free Wi-Fi; because it is public, it is prone to be used also by cyber criminals and attackers waiting for opportunities to access and steal important information and company or personal data.

Ensure you erase your footprint on visited sites if you must use public Wi-Fi. Disable all options that say save passwords and ensure you logout.

Report and share your experience and knowledge. When upgrading, be sure you are not giving away your life by authorising the app to take all the information about you.

Ensure to put eyes on the demands of cookies, cache and routinely delete browsing history.

Foolproof cybersecurity management is impossible in this

current AI era, however multiple layers of protection which spread across the computers, networks, programs or data that is protected may provide a degree of success that is reasonable to allow smooth operation until the investment in the cybersecurity industry can yield an absolute protection dividend.

In a maritime organisation, unified threat management – as in the form of coordinated cybersecurity management – may be the gateway system that is currently needed. For the maritime industry, with various security outposts, it may be easier to coordinate to checkmate cyberattacks, as the system of coordination already exists.

The vulnerabilities faced in the maritime industry are multifaceted; even when protected against outsiders, there is also a threat of a malicious insider manipulating or giving out security breaches. Cheating personnel wages and unreasonable sacking from work must be stopped to avoid cyberattack retaliatory actions, as these attacks can be performed remotely.

The attack in the European airports showcases weakness involved in being dependent on a single provider of software; there may be competition of software and poor design errors which overlooked weaknesses and security implications. Yet, investment in cybersecurity management and personnel training is the way to move forward for a cyber-secured maritime industry.

There is need for a targeted regulatory regime which grows with the cybersecurity industry – and in facts grows faster than it – to ensure compliance and that effective protection with a regulatory framework is available.

Nigeria may work with Australia collaboratively to exchange knowledge, experience and one another's working regulatory regimes, given that both nations are big maritime nations and apply the maritime Port State Control Memorandum of Understanding: for Nigeria, the Abuja MOU, and, for Australia, the Tokyo MOU or India MOU.

Professor Chief Emmanuel Tam. Ezekiel-Hart
AIMS Member

Note: This article is based on a lecture paper delivered by Professor Chief Emmanuel Tam. Ezekiel-Hart (Australia), who is Professorial Chair, Faculty for International Trade Relations and Logistics Management, EBS / HIBC College of Divinity, and an AIMS Member.

Cyber security

MARINE surveyors are on the frontline of the maritime industry, assessing the condition and safety of vessels.

Unlike the days before technology, the toolkit of a surveyor today has evolved from clipboards, film cameras and filing cabinets to tablets running specialised software, cloud-based data storage and artificial intelligence for data analysis.

With technology, marine surveyors are equipped with the digital tools to enhance efficiency, accuracy and reporting quality but they also introduce new risk. By relying on a chain of third-party software providers, surveyors inherit the security vulnerabilities of those platforms. Additionally, the amount of sensitive data surveyors handle is also seen as a treasure chest for cyber criminals.

Vessel blueprints, structural deficiency reports, client financial information and personally identifiable information make surveyors high-value targets for data theft and extortion.

The 2023 ransomware attack on maritime software provider DNV is a reminder that a similar flaw in a surveyor's software can also create a direct gateway for cyber criminals to steal data from the cloud or launch an attack that disrupts the surveyor's own operations.

In Australia, 62 per cent of small-to-medium enterprise (SME) businesses have experienced a cyber security incident. The average cost to recover from a cyber incident can easily reach six figures, an expense that a comprehensive Cyber Liability Insurance policy is designed to cover.

This insurance not only provides financial indemnity but also provides immediate access to the expert incident response, legal, forensic and public relations services necessary for business survival in the aftermath of an attack.

Getting a quote via our insurance partner is easy.

Follow this link now (Cyber Insurance - abcountrywide) and you will find Austbrokers Countrywide dedicated Cyber Insurance info page.

Alternatively, contact Amber Draffin at Austbrokers Countrywide Insurance Brokers on 1800 245 123.