Journal of World Energy Law and Business, 2023, **16**, 354–366
https://doi.org/10.1093/jwelb/jwad014
Article

OXFORD

Cyber and AI security challenges for LNG maritime transport and terminals—responses in law and standards

Juei-Cheng Jao* and Jason C.T. Chuah **

ABSTRACT

This article considers how key state players in the maritime transport and storage of liquefied natural gas (LNG) face up to the cyber security threats which have sadly become ubiquitous in recent times. The cyber threat for the gas sector, with increasing investment in LNG and current geopolitics, makes the study especially acute.

1. RATIONALE

It is a trite proposition that liquefied natural gas (LNG) carriers and terminals are involved in a particularly high risk and sensitive maritime-based trade. Carriers or tankers face a range of technical, structural and safety challenges, as vessels require sophisticated technology to transport and maintain their liquefied cargo. This in turn makes LNG shipping a capital-intensive business from both a CAPEX[1] and OPEX[2] perspective.[3] Leaving aside the economic and commercial risk perspective, from a macro-policy level too there are serious safety and security concerns for loading and especially off-loading ports. From a ship design and structure perspective, standard LNG carriers already measure up to 300 meters, making physical fitness and material fatigue key safety concerns. These design and structural aspects are very much guided and controlled by the input and processing of large volumes of data by highly computerized systems, including the increasing reliance on artificial intelligence.[4] Cargo containment, reliquification and propulsion systems too must meet high technological and digital standards of safety and reliability in order to transport LNG. Sophisticated software is needed for owners to manage sloshing risk by calculating the exact motion of liquid within tanks, thereby improving safety and avoiding spillage.[5] Moreover, as

* Juei-Cheng Jao, Professor of Maritime Law, College of Ocean Law and Policy, National Taiwan Ocean University, Taiwan
** Jason C.T. Chuah, Professor of Commercial and Maritime Law, Universiti Malaya, Malaysia and City, University of London, UK. Email: jason@um.edu.my

The authors acknowledge with thanks the support for this research provided by the National Science and Technology Council of Taiwan to the National Taiwan Ocean University under the subproject D 'The Legal Impact by AI in International Maritime Law' in the master project: 'Development and Application of Marine Exploration and Ecological Survey Technologies under Climate Change', 110-2634-F-019-002. The authors are also grateful to the reviewers for their helpful remarks.

[1] Capital Expense.
[2] Operating Expense.
[3] As reported by virtually all classification societies, see eg LNG carriers | Marine & Offshore (bureauveritas.com).
[4] See the many scholarly references cited in Y Ao and others, 'An Artificial Intelligence-Aided Design (AIAD) of Ship Hull Structures' (2021) JOES (accepted for publication; draft available at <https://www.sciencedirect.com/science/article/pii/S2468013321001303> accessed 18 July 2023).
[5] ibid.

new-build technology evolves,[6] different types of LNG containment and transfer systems are becoming available for LNG bunkering[7] vessels. Those technology-driven designs must, however, be thoroughly evaluated for safety, regulatory compliance and ship-to-ship bunkering compatibility. LNG terminals too have to be designed with safety and security in mind.

It is worth recalling that for any LNG port design the primary objective is to guarantee the safe approach into the port, the safe berthing and calm mooring. It is also crucial that infrastructure and operational procedures are in place to ensure the safe arrival and departure from the terminal and/or safe aborting of any entry or egress manoeuvres during an on-board or onshore emergency.[8] These matters are addressed largely by means of computerized programmes, and increasingly, through artificial intelligence decision-making processes.

A matter which is seldom considered is that AI is becoming routinely used to calculate the arrival, loading and discharge rate and storage tank capacity of the LNG carrier. These efficiencies help reduce delays by enabling the vessel to avoid lengthy periods at less safe areas of the port zone. The vessel is better able thus to avoid the impact of inclement weather conditions.[9]

Terminal and port authorities also will need to know the total safety level of the LNG shipping operation in the context of the existing infrastructural and surrounding shipping movements. Again, computer technology is used to measure and evaluate the risks related to collisions, groundings, contacts, fire and explosion on board, eventually leading to the release of gas and any other deleterious consequences. Both large and small ports are susceptible to those risks. Even countries preferring to use Ship to Ship transfers (STS) or Floating LNG (FLNG) facilities are not inured—the calm seas required for STS operations or an FLNG facility are usually fairly enclosed or protected waters, which means that vulnerable on-shore communities are never far away.

Using Taiwan as an observational target, this research interrogates the different regulatory approaches at the international and national law making levels aimed at ensuring better cyber security in the security-sensitive area of maritime transport and storage of LNG.

The last few years have witnessed an important geopolitical or perhaps geo-economic development in the South China region—Taiwan has been engaged in intensifying its LNG storage and transportation activities quite significantly. From contracts to build a much larger national fleet of LNG tankers,[10] additional at-port LNG import tanker storage facility[11] and diversifying its imports away from Russia by making long-term supply contracts with Qatar, Australia, Indonesia and other suppliers.[12] There is also diversification by means of mixing long- and short-term contracts, alongside trading on the spot markets. The prevailing policy backdrop is to drive forward the jurisdiction's agenda to shift from a dependency on coal to natural gas. Those plans were given a

[6] For example, orders for new LNG carriers with the competence to sail across the frozen conditions of the Arctic have seen an increase. These orders pre-dated the invasion of Ukraine by Russia. They primarily relate to the Arctic LNG2 project in Russia. Source: <https://www.upstreamonline.com/lng> accessed 18 July 2023.

[7] It is perhaps useful to refer to the legal definition of 'bunkering' adopted by the EU in art 2(1) of Regulation 2017/352 establishing a framework for the provision of port services and common rules on the financial transparency of ports. Adapting that definition to the LNG context, it might be said that LNG bunkering is the provision of LNG, to be used as fuel, used for the propulsion of the LNG-fuelled waterborne vessel as well as for general and specific energy provision on board of the waterborne vessel whilst at berth [see also EMSA Guidance for LNG Bunkering 2017, para 2.4.1 available at Sustainable Ports—LNG Bunkering & OPS—EMSA—European Maritime Safety Agency (europa.eu)].

[8] J Van Doorn, Safety of LNG Shipping Around Ports and Terminals [2012] Port Technology International Technical Paper (31 January 2012) at Technical Papers Archive—Port Technology International.

[9] In a Taiwan context, see 配合國家能源政策於國際商港 LNG 接收站之規劃及建設, <http://www.cie.org.tw/cms/JournalFiles/11003_chapter06.pdf> accessed 12 July 2023.

[10] On 13 January 2022, it is reported that Taiwan is investing in building another 16 LNG tankers for its national fleet. [Taiwan set sights on national fleet of 16 LNG carriers | TradeWinds (tradewindsnews.com)]. That said, Taiwan could be deemed to have developed a domestic-owned fleet of LNG carriers. Many of the construction contracts (such as the ones with Qatar) do not confer full ownership to Taiwan. Therefore, in many cases, natural gas transportation and related operations can only be conducted by cooperating with foreign teams, leading to an unstable gas supply. (Source: 國家隊就位 拚 LNG 國貨國運, <https://ctee.com.tw/news/industry/590748.html#:~:text=%E7%9B%AE%E5%89%8D%E5%8F%B0%E7%81%A3%E9%80%B2%E5%8F%A3%E5%A4%A9%E7%84%B6,%E8%B3%BC%E6%B0%A3%E5%90%88%E7%B4%84%E4%B9%8B%E8%B2%A8%E6%B0%A3%E3%80%82> accessed 18 July 2023). In contrast, many neighbouring countries such as China and Korea are pushing ahead with the construction of LNG carriers.

[11] On 18 July 2022, the Port of Taichung in Taiwan broke ground for the construction of two 180,000 m^3 full containment LNG tanks, Taiwan's largest storage tanks ever built. The site will also see the construction of large regasification facilities. [Bechtel starts construction on Taiwan's largest LNG storage tanks (prnewswire.com)]. There are also plans to expand LNG terminals at Taoyuan and Keelung.

[12] Taiwan set to wind down Russian LNG imports as contract expiry nears | S&P Global Commodity Insights (spglobal.com). See Table A1 in the Appendix.

significant push following the invasion of Ukraine by Russia leading to economies antipathetic to the invasion seeking to wean themselves off dependency on Russian gas and for Taiwan a matter of national security. Indeed, the Taiwan Ministry of Transportation and Communications is seriously considering amending the Regulations of Materials and Instruments Imported by Maritime Transportation for Governmental Agencies and State-owned Enterprises to give priority of carriage to Taiwan-flagged ships for LNG.

These developments are intended to be very technology dependent, both in the software and hardware contexts.

That technology dependency raises specific risks and challenges for an economy such as Taiwan. There are indeed important and useful guidance and regulatory standards from the International Maritime Organization (IMO), which Taiwan is gradually incorporating into its maritime safety and security regime. Despite the fact that Taiwan is not a UN member and does not have a seat at the IMO, its engagement with IMO standards is worthy of evaluation.[13]

Taiwan is chosen as study subject for several reasons. First, Taiwan is an important LNG trader in the region given its agenda to move from coal to natural gas by 2025. As a substantial importer of LNG[14] but also, like many European countries, its attempts to diversifying its sources will only continue to increase LNG tonnage in its shipping links and equally crucially its port infrastructure, which is extremely computer technology and AI dependent.[15] Secondly, its geopolitical circumstances raise the stakes for legal and regulatory cyber security controls, especially in an economic activity of national and security importance. Thirdly, Taiwan has always been (cyber) security conscious and significant investments have been placed on technological defensive measures. The technological defensive shield serves as an important backdrop to the legal and commercial cyber risk controls. Fourthly, Taiwan does not have explicit regulations dealing with cyber security concerns in the LNG sector. Instead, it has recently adopted general laws on cyber security. States might be categorized into (i) those with detailed legally binding standards on cyber security in the LNG sector (such as the EU), (ii) those without any cyber security specific laws and (iii) those with only general laws dealing with cyber security. Taiwan has somewhat arguably moved from (ii) to (iii). By assessing how this approach impacts on cyber security in the transport and terminal storage of LNG might thus produce useful lessons for other regulators. Fifthly, most states belonging to the UN/IMO family of nations will implement high-level principles and recommendations emanating from the IMO in varying degrees of consistency. As alluded to above, Taiwan is not a member of the IMO, as a result of its exclusion from the UN. The international cyber security standards for maritime transport and terminal operations established by the IMO are thus not legally binding on the jurisdiction. Yet Taiwan has consistently incorporated various IMO rules, standards and recommendations into its domestic system of maritime regulation, despite its prerogative not to do so. This places it in a comparable position to those states with a 'broad' preference to be part of the IMO normative system, but not always in a sufficiently strong economic or political position to do so. Thus, insights into how the Taiwanese regulatory and quasi-regulatory landscape is shifting to accommodate the cyber security concerns raised by the IMO should be helpful for a cross jurisdictional analysis.

Section 2 below will examine the recent legislative and regulatory interventions internationally, especially those under the auspices of the IMO. Those provisions are intended to buttress

[13] Taiwan has consistently voluntarily adopted various IMO standards and regulations; in between 2011 and 2016 Taiwan carried out voluntary external and independent auditing of its compliance with IMO standards in safety, security and environmental matters. [See S-T Ung, C-C Tsai and C-L Chen, 'A Rigorous Review and Thorough Planning for Ship Inspection System in Taiwan' (2013) 21 (5) J Marine Sci Technol 569]. This was undertaken before the audit became a mandatory treaty obligation for Member States in 2016. For more about the IMO audit scheme, please see Member State Audit Scheme (imo.org). It should, however, be noted that Taiwan had not adopted the cyber security recommendations promulgated by the IMO—not by design, it should be said, but largely because those recommendations are still very fresh.

[14] Please see Table A2 in Appendix.

[15] This has been the focus of cooperation among the Taiwan International Ports Corporation, port pilots and Chinese Petroleum Corporation to produce a joint risk assessment of LNG fuel bunkering operations. These efforts were recently buoyed by the berthing of Global Sealine, a 180,000 m^3 LNG carrier, at Taichung Port in 2022. Ensuring a safe approach and berthing remain key priorities. (See 台灣中油公司台中液化天然氣廠成功靠卸 18h 萬立方公尺級液化天然氣船, <https://www.cpc.com.tw/News_Content.aspx?n=28&s=69549> accessed 18 July 2023).

technological efforts aimed at the detection, prevention and sanctioning of cyberattacks. It will show, however, that there needs to be better coordination of law and standards making across the international, national and industry domains. This is followed by Section 3 which looks to the regulatory response in Taiwan, juxtaposed against an international governance regime the country is not privy to. In particular, the work tests the extent to which the IMO principles and standards are able to influence, or not as the case may be, domestic and local level standards making. Taiwan as an observational subject is useful not only in respect of territories or countries with limited recognition in the UN system but also states, including a good number of 'flag of convenience' states, which interact with the IMO rule-based system only in a limited way.

2. REGULATORY CONTEXT AT IMO LEVEL

International Safety Management Code—guidelines on maritime cyber risk management

The IMO's Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98)—Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages state administrations to ensure that cyber risks are appropriately addressed in existing safety management systems [as defined in the International Safety Management (ISM) Code[16]] no later than the first annual verification of the company's Document of Compliance after 1 January 2021. That Resolution is followed through with the adoption of the Guidelines on maritime cyber risk management by the Facilitation Committee,[17] at its 41st session (4–7 April 2017), and by the Maritime Safety Committee, at its 98th session (7–16 June 2017).[18] The Guidelines provide first high-level recommendations or principles on cyber security management and prevention, and secondly, technical granularity as applicable to the particular systems in the shipping context. These Guidelines are intended for shipping, generally and are not specific to the energy sector. However, their description of 'vulnerable systems' coincides tidily with the specific weaknesses in the LNG sector. For example, the Guidelines provide that those vulnerable chinks include

a) Bridge systems.
b) Cargo handling and management systems.
c) Propulsion and machinery management control systems.
d) Access control systems.
e) Administrative and crew welfare systems.
f) Communication systems.

On an LNG carrier with limited crew, much reliance is placed on technological systems—especially the ones identified above. Indeed, specialist service providers have stepped forward offering their commercial services to LNG fleet owners to audit and enhance their cyber security preparedness to meet the requirements of the IMO Cyber security Recommendations.

The Resolution places a quasi-legal[19] responsibility on flag states to put in place appropriate regulations to ensure the cyber security management principles are complied with and set up monitoring, supervisory and enforcement procedures as regards its flagged vessels. Most LNG tankers,

[16] Often referred to as the ISM Code; its full title is International Management Code for the Safe Operation of Ships and for Pollution Prevention.

[17] The Facilitation Committee (FAL) deals with matters related to the facilitation of international maritime traffic, including the arrival, stay and departure of ships, persons and cargo from ports. The Committee also addresses electronic business, including the single window concept, and aims to ensure that the right balance is struck between regulation and the facilitation of international maritime trade. [Source: Facilitation Committee (FAL) (imo.org)].

[18] MSC-FAL.1/Circ.3.

[19] IMO Resolutions are of course not legally binding but those from some committees, such as this one emanating from the Facilitation Committee provides not only vital guidance to Contracting States but also clarifies the legal duties of state members under the Convention for the Facilitation of International Maritime Traffic, 1965 (as amended) (the so-called FAL Convention). The FAL Committee also engages with the industry, widely construed, creating thus broad consensus on the legal norms relevant and applicable to state members. [Facilitation Committee (imo.org)].

properly classified by their classification societies and flying a legitimate flag, will have to comply with these ISM Code measures.

Three observations might be made about these recent developments in international maritime law. First, the IMO's approach was intentionally generalized as to the type of shipping cargo/trade in question. Secondly, the Guidelines are expressed to be risk based[20]—the onus is on the shipping companies to ensure that proper cyber risk measures are established but there is also emphasis on the state's role in ensuring in making and implementing regulation on cyber security management, the same risk-based approach is adopted. This contrasts with the rule-based systems sometimes mooted by IMO member states. Thirdly, the notion of cyber security is formally described as connoting 'a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised'.[21] In this definition, no distinction is made between failures which are negligently or carelessly caused, maliciously induced or innocently generated. Fault, therefore, is not intended to be a distinguishing attribute in the regulatory framework.

The new IMO principles for managing the cyber risk intersect equally with recent guidelines from various national and international organizations. For the LNG sector, reference should be made of the highly influential Guidelines on Cyber Security Onboard Ships (Version 4) 2020 (hereafter referred to as the 'Ships Cyber Security Guidelines')[22]—a notable contributor to the Guidelines is INTERTANKO which represents a significant proportion of the energy shipping sector. As for ports and terminals, the IMO also draws attention to the IAPH Port Community Cyber Security Report 2020, to be referred hereafter as the 'Ports Cyber Security Report'.[23] It is beyond the scope of this article to describe the different anti-cyberthreat measures recommended by these industry and government-backed guidelines. There are some commonalities of the cyber security strategy in these guidelines. These strategic principles are useful when appraising the Taiwanese and indeed any other domestic state-based cyberthreat combat plan.

First, the proposition that there needs to be a 'common global language to address cyber security issues'.[24] This is translated into the risk assessment model recommended by the Ships Cyber Security Guidelines. It is provided that 'prior to starting a cyber risk assessment on board, the following activities should be performed:

- Review the documentation of IT and OT systems.[25]
- Identify main manufacturers of critical shipboard IT and OT equipment.[26]
- Identify cyber security points-of-contact with the most important manufacturers and establish a working relationship with them.
- Review detailed documentation on the ship's maintenance and support of the IT and OT systems.
- Establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment'.[27]

[20] Paras 1.1 and 1.4, Guidelines.
[21] Para 1.1, ibid.
[22] Guidelines produced by BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC).
[23] The Report is produced under the auspices of the World Ports Sustainability Programme [established by the International Association of Ports and Harbors (IAPH) with participation from the International Cargo Handling Coordination Association (ICHCA) and the TT Club which represents the independent mutual insurance services]. IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf (sustainableworldports.org).
[24] Chapter 2, ibid.
[25] Whereas Information Technology (IT) systems manage data and support business functions, Operational Technology (OT) is the hardware and software that directly monitors/controls physical devices and processes and as such are an integral part of the ship and must function independently of the IT systems onboard. The systems can, however, be connected to the IT network for performance monitoring, remote support, etc. Such systems are sometimes referred to as belonging to the Industrial Internet of Things (IIOT). [Section 1.4, see above (n 22)].
[26] A risk-based approach should be used in this identification process. See above.
[27] Section 6.2, see above (n 22).

Central in these activities is a common understanding of the language and scope of the risks and risk ameliorating measures. It is especially needful for the contractual obligations to reflect the same cyber security or cyber management language used in the audit, design and maintenance documentation. Importantly, the contracts for transporting LNG are likely to be passed down the sale chain of contracts.[28] Third parties receiving the rights under the sale and/or carriage contracts are unlikely to be privy to the original contracting matrix of information and knowledge. The European Maritime Safety Agency, in its Guidance for LNG Bunkering, for example, stated quite unequivocally:

> The creation of interface environments in LNG bunkering raises the concern about how different regulatory frames ('land side' vs 'ship side', 'road' vs 'port', 'road' vs 'ship-side', etc.) … can also unveil potential training discrepancies, equipment mismatches and other factors that can, ultimately, influence Safety and affect the Environment with unnecessary methane emissions. The minimization of risk to life and property, and the mitigation of gas release are the fundamental drivers to make the LNG chain inside the port area as lean and simple as technically possible.[29]

Establishing a common understanding between all stakeholders, whether they are brought together by contract[30] or regulation,[31] can be properly achieved by the global industry cooperating in the taxonomical exercise, supported and facilitated by governments. The IMO Guidelines, Ships Cyber Security Guidelines and the Ports Cyber Security Report all stress the importance of the common language when identifying individuals in the shipping supply chain or networks who should assume responsibility for different aspects of cyber security. Ship design rules should also mirror the common language—especially in a security-sensitive sector like LNG. Indeed, the IMO produced the International Code for the Construction and Equipment of Ships Carrying Liquefied Gases in Bulk (IGC) and the International Code of Safety for Ship Using Gases or Other Low-flashpoint Fuels (IGF). Those Codes pay specific attention to cyber or technological concerns in LNG carrier design, operations, fuel handling procedures and installation of equipment onboard.[32] Not all LNG carrier flag states have signed up to the codes.

Secondly, there should be industry and intergovernmental understanding, knowledge or awareness[33] as to the procedure for addressing the cyber threat. The model of governance, as we have adumbrated above, is characterized as one which is risk rather than rule based. That connotes a degree of common understanding of the risk assessment processes. The IMO Guidelines, like the Ships and Ports Cyber Security Guidelines, stipulate that the process should not be seen as sequential. The functional elements to the risk management process should be concurrent and continuous. These 'elements' (rather than 'steps') are portrayed as:

1) Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
2) Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
3) Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

[28] This is achieved by the buyer transferring on to a sub-buyer the bill of lading representing the LNG cargo for price consideration. See generally J Chuah, *Law of International Trade: Cross Border Commercial Transactions* (6th edn, 2019) chapters 2, 6.
[29] See above (n 7) at para 2.4.2.
[30] For example, suppliers and buyers.
[31] Authorities responsible for goods clearance, maritime safety and security, border controls, etc.
[32] See International Code for the Construction and Equipment of Ships Carrying Liquefied Gases in Bulk (IGC Code) (imo.org) and International Code of Safety for Ship Using Gases or Other Low-flashpoint Fuels (IGF Code) (imo.org).
[33] Or even better still an awareness or knowledge which is anticipated or required by law or regulation. It is submitted that such an approach is not necessarily inconsistent with the risk-based approach, generally preferred by the international bodies concerned (infra).

4) Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.[34]
5) Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber event.[35]

These principles are intended to serve as the flesh to the wider duties of states and shipping companies provided for in the ISM Code,[36] which is given a legal effect by Chapter IX of the International Convention for the Safety of Life at Sea (SOLAS) 1974.[37]

IMO International Ship and Port Facility Security Code

The other IMO regulatory tool relevant to cyber security risks in sensitive shipping such as in the LNG context is the International Ship and Port Facility Security (ISPS) Code.

The ISPS Code as part of the SOLAS Convention, in contrast to the ISM Code, is more concerned with maritime security[38] rather than maritime safety although it is axiomatic that both are complementary mainstays of international maritime law. It is a mandatory governance system extending to both shipping and port/terminal operations. The ISPS Code comes in two parts. Part A which regulates port and terminal security matters is compulsory. Part B provides non-binding guidance on how those requirements in Part A might be met. The focus of the ISPS Code is the ship/port interface—where ship and port interact, that is presumptively where security risks are most acute. It is fairly obvious that whilst that approach might be appropriate for traditional shipping and port operations, with increased computerization and digitization in the sector, the ship/port interface is not simply physical but virtual and is much more integrated into IT and OT systems in the entire logistics chain. Perhaps an overhaul of the ISPS Code's approach is needed.

As it currently stands, the ISPS regulations take a piecemeal approach to the matter of cyber security. The regulations require the relevant authorities at the port state to carry out port facility security assessments (PFSAs) and plans. Port facilities must appoint properly qualified security officers and invest in appropriate security equipment. Port facilities are dutybound too to supervise and manage communications, access and activities involving the port area. All these obligations must be reported in a port facility security plan (PFSP). A purposive interpretation of the ISPS Code suggests that the general duties 'should' include cyber security concerns, despite the clear tendencies towards the physical attributes of the ship/port interface. For example, the PFSA identifies radio and telecommunication systems, including computer systems and networks, as relevant 'elements'.[39] This reference must surely imply that if cyber threats might compromise vessel and/or port security, that cyber risk should be considered in the security assessment. Moreover, the ISPS explicitly stipulates that the PFSA shall include 'the identification of *possible* threats to assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures'.[40] It is thus reasonable to conclude that the role of the PFSO must evolve to encompass cyber security at the ship/port interface, rather than being focused purely on physical threats. And as the Ports Cyber Security Report stresses, the PFSA must extend 'more generally to cyber issues relevant for the wider well-being of maritime assets, infrastructure and supply chain operations'.[41]

[34] This aspect is particularly important in LNG bunkering—emergency shutdown procedures are often required by national law to prevent harm of methane contamination and explosions. The cyber aspect of emergency shutdown procedures cannot therefore be underestimated. The shutdown is often executed by a series of computer commands and those commands must therefore be protected by appropriate firewalls and manual overrides be made possible and effective. Indeed, the Society of Gas Tanker and Terminal Operators (SIGTTO) published a Technical Note in 2009 solely due to clarify the functional requirements for ESD systems, primarily differences between the needs of the LNG industry and those of the LPG industry. Proposals were presented for a standardized links to connect ship and terminal emergency shutdown (ESD) systems that are designed to communicate and initiate ESD of cargo transfer as safely and as quickly as possible. (Publications | SIGTTO—The Society of International Gas Tanker and Terminal Operators).
[35] Para 3.4, MSC-FAL 1/Circ.3. See above (n 18).
[36] See above (n 18).
[37] See The ISM Code (imo.org).
[38] The Code came into force on 1 July 2004, intending to address security risks in international transportation, following the horrific events of 11 September 2001 in the USA.
[39] ISPS Code, Part B, 15.3 sub 5; note that the word 'element' is consistent with that used in the ISM Cyber Security Guidelines above.
[40] ISPS Code, Part A, 15.5 sub 2; emphasis added.
[41] Chapter 5, see above (n 23).

Similarly, at the EU level, Directive 2012/18[42] which requires Member States to prevent major hazard incidents, to mitigate their consequences and to take recovery measures, is framed without specific reference to the cyber aspect. It is a general directive and not specifically directed at LNG terminals, but it has direct relevance given the presumption that the risk of a major hazard incident occurring at LNG terminals is especially pronounced. It requires all operators[43] of the installation or facility in question to produce a safety report.[44] The directive does not spell out any explicit cyber risks for the safety report to address[45] but it is safe to deduce that the physical and process risks cannot, like in the ISPS Code context above, exclude the technological risks.

3. THE TAIWAN REGULATORY RESPONSE

Taiwan has consistently attempted to mirror the principles and rules issued by the IMO in its national scheme for protecting maritime safety and security. It also adopts a good number of International Standards Organizations recommendations relevant to maritime safety and security. That said, there are some key challenges with that regulatory environment.

First, the ship inspection system in Taiwan has been weaker than it should be when compared to other signatory states to the Paris Memorandum. Colleagues at the National Taiwan Ocean University draw attention to the fact that in 2013, the annual examination rate of the vessels calling at Taiwanese ports was less than 10 per cent[46] largely caused by a lack of human resources. The issue has anecdotally improved but progress is yet slow and not helped by the lockdowns and disruptions caused by the COVID-19 pandemic.

Secondly, research on perceptions of safety and security aspects in Taiwanese waters by stakeholders and experts reveal albeit implicitly the lack of active awareness of the issue of cyber risk.[47] The study in question, conducted in 2015, focused on the harbours and surrounding waters where maritime incidents are concentrated and interrogated the potential factors that vessels should assess when traveling through these areas. Pilots, captains, deck officers, experienced maritime employees and experts with deep professional knowledge of maritime traffic were interviewed. The respondents placed a great deal of emphasis on the physical and human factors as potential causes of marine casualty in those waters. Although some did mention communication systems as a potential cause, this author's interpretation of the dataset reveals a lack of direct or active awareness of the computer technology-related aspects of navigation. Of course, the fact that in 2015 the matter of the cyber risk was fairly nascent amongst Taiwanese shipping professionals. However, the research does show that a culture shift is needed as we move into a much more cyber-embedded maritime network.

Thirdly, whilst there are industry and government guidelines on port facility safety and handling of hazardous materials which would take onboard the cyber risk, more broadly, the cyber risk regulatory system is under-development. To that extent, there is a regulatory gap between general law and industry-specific standards. In the international context as we have observed, international bodies such as the IMO or EU lay down high-level principles and rules which are intended to work in tandem with the sector-specific recommendations and standards. That does not appear to be as well articulated in the Taiwan context.

The question for this article is whether and to what extent is that likely to change with the recent legislative initiatives on cyber security.

[42] A directive on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.

[43] Defined in art 2 as 'any natural or legal person who operates or controls an establishment or installation or, where provided for by national legislation, to whom the decisive economic or decision-making power over the technical functioning of the establishment or installation has been delegated'.

[44] Art 10.

[45] See Annex III for the list of information required of the safety report.

[46] Ung (n 13).

[47] C-C Chou and others 'Key Navigation Safety Factors in Taiwanese Harbors and Surrounding Waters' (2015) 23(5) J Marine Sci Technol Art 12. (ntou.edu.tw).

In 2018, the Executive Yuan enacted the Cyber Security Management Act,[48] which enables the Government to make relevant secondary legislation to support the new legislative agenda. The following rules and regulations[49] have thus come into effect as of 1 January 2019:

- Enforcement Rules of the Cyber Security Management Act (CSMA Enforcement Rules).
- Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency (Audit Regulations).
- Regulations on the Notification and Response of Cyber Security Incident (Incident Regulations).
- Cyber Security Information Sharing Regulations.
- Regulations on Classification of Cyber Security Responsibility Levels (Classification Regulations).

These are general legal acts covering certain defined areas of economic and public activity and are not energy or transport specific. That said, the Cyber Security Management Act was enacted to address cyber security threats on the country's critical infrastructure—which would include transport and energy. The Act pointedly defines critical infrastructure as 'asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities, which shall be re-examined and promulgated by the competent authority regularly'.[50]

Sectoral legislation is likely to be introduced to provide flesh on the bones; at the time of writing, there are no plans to introduce any transport or energy-specific cyber security legislation. The key sectors where there are sector-specific laws are banking, insurance and finance, highly sensitive technology goods and mobile technology.[51] There are also general legislations addressing public concerns such as terrorism,[52] data protection,[53] national security,[54] surveillance[55] and money laundering.[56]

A useful consideration is the Cyber Security Management Act's definition of 'cyber security'. Article 3(3) defines the term as meaning 'such effort to prevent information and communication system or information from being unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system'. The Act further adopts the term 'cyber security incident' to refer to any breaches of state of the system, service or network which violate the cyber security policy.[57] Albeit a little clunky, the translation does make it plain that those violations do not need to be intentional or malicious. Violation is deemed present if the consequence is such that the information and communication system function of the entity in question is 'adversely' affected. Adversely is necessarily a matter of degree. It does therefore leave some room for administrative discretion when it comes to supervision, monitoring and enforcement of the Act.

The Act governs the cybersecurity requirements for government agencies,[58] excluding military and intelligence agencies, and the so-called 'specific non-governmental agencies'. These non-governmental agencies are critical infrastructure providers, state-owned enterprises and government-endowed foundations.[59] The Act requires the government and non-governmental agencies in question, when outsourcing their technology services, to assess the moral hazard of the

[48] The Official English translation of the Act is available at Law—Laws & Regulations Database of The Republic of China (Taiwan) (moj.gov.tw).
[49] English translations of these laws are available at Law—Laws & Regulations Database of The Republic of China (Taiwan) (moj.gov.tw).
[50] Art 3(7).
[51] See laws made under the auspices of the Financial Supervisory Commission, the Ministry of Finance amongst others.
[52] Counter Terrorism Financing Act.
[53] Personal Data Protection Act.
[54] National Security Act.
[55] Computer Security and Surveillance Act.
[56] Money-Laundering Control Act.
[57] Art 3(4); the cyber security policy refers generally to the cyber security system of the entity in question. That entity can be a government agency or a non-governmental agency which is a provider of critical infrastructure. See below.
[58] The military and intelligence agencies are excluded from the Act though (art 3(5)).
[59] Art 3(6).

outsourced outfit accordingly and the nature of the cyber security risk in question.[60] The Act does not explicitly lay down liability on the outsourced undertaking for breaches or violations of the cyber security policy or system of the entity in question.

In this connection, the Act establishes the foundations for LNG terminal operators to be treated as providers of critical infrastructure. The Act requires such entities to produce and implement a Cyber Security Management Plan[61] to designated supervising authorities. These supervising authorities will be tasked to audit the Plans and will have the power to order improvements and remedying measures to be taken by the entity in question.[62] A procedure for handling and reporting cyber security incidents[63] is also provided in generalized terms.[64] It is hoped that measures would now be taken to see through the establishment and implementation of cyber security schemes for LNG terminals. That said, it is difficult to envisage extension of the Act to LNG carriers—it might be a stretch of the law to deem LNG carriers as providers of critical infrastructure. The LNG product itself could not constitute 'infrastructure'.

Contrasting the Taiwan legislative approach to those we witnessed internationally, the former is somewhat thin on high-level principles. The legislation is much more bureaucratic than principle oriented. It focuses on a reporting process whereby the regulated entity demonstrates that it has the appropriate cyber security measures in place to avoid breaches. Where there has been a breach, the entity has a duty to ensure that there is proper transparency for the authorities in case any remedial action needed to be taken by the authorities.

It leaves the principles of cyber security governance to be fleshed out through scientific learnings, research and the sharing of good practice from domestic and international entities.[65] This is of course where relevant international standards, such as ISO[66] and EN,[67] would help inform the adoption and/or development of Taiwan's cyber security standards. As regards the cyber security principles proposed by the IMO, the Taiwan government, under the new Act, would be able to continue to reflect international standards in its cyber security plan *vis-à-vis* the transport and storage of LNG.

An important strategy in a cyber security legal framework should be directing regulation at the cyber products in question. Article 4 of the Cyber Security Management Act makes mention of this aspect:

> In an effort to promote cyber security, the government shall provide resources, and integrate the momentum of both civilian groups and private sectors, and boost cyber security awareness of all people, and implement …
>
> (4.) Development of cyber security related software and hardware specifications, relevant services and *verification* mechanism.[68]

Specific and more detailed provisions have yet to be introduced. The reference to 'verification mechanism' is important. That is quite consistent with the strategic direction of the EU Cybersecurity Act.[69] The EU certification scheme, as one might recall, serves to provide an

[60] Art 9.
[61] Which includes annual reporting of the execution of the Plan. See Chapters II and III of the Act.
[62] Arts 13 and 16 for government agencies and non-governmental agencies (which provide critical infrastructure services), respectively.
[63] For a definition of cyber security incident, see above at p. 9.
[64] Arts 14 and 18, for government agencies and non-governmental agencies (which provide critical infrastructure services), respectively.
[65] Art 5 provides 'The competent authority shall plan and promote the cyber security policy, and the cyber security technology development, and interchange and cooperation with international community, and the comprehensive cyber security protection relevant undertakings, as well as announce the report of national cyber security status, the summary auditing report on the implementation of the cyber security maintenance plan for the government agency, and the national cyber security program'.
[66] Technical specifications agreed by the International Organization for Standardization.
[67] European Standards or *Europäische Norm* drafted by the European Committee for Standardization.
[68] Emphasis added.
[69] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cyber security) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cyber security Act).

EU-wide accreditation system of Information and Communications Technology (ICT) products or services so that users have confidence that these products meet the standards of cyber security agreed by the EU technical panels. Use of LNG bunkering, discharge and transit computer programmes is unregulated which leads to potential cross-contamination or infection. Therefore, requiring all relevant operators to use only verified or certified ICT products goes a long way in reducing the cyber risk.

4. CONCLUSION

It is safe to say that after a disconcerting lull, despite some very pressing cyber security concerns, Taiwan finally has a piece of enabling cyber security legislation. For the LNG trade, this is an improvement from the non-explicit approach to cyber security. However, for a country that wishes to engage positively and actively with the IMO rule based regime, its cyber security regulatory system is somewhat distant from the high level principles setting approach taken by the IMO as regards shipping and the LNG trade. The core principles appear to be present but are regrettably not fully articulated and often couched in a bureaucratic procedure-driven system of regulation.

It is in this context that recommendations for change must entail better consistency between the national, industry and international. A good way forward is to treat IMO standards both as regulatory ones (for those countries where IMO measures apply as a matter of law) and representing good practice in the LNG shipping sector (for the global scene regardless of IMO or UN membership). However, it is also vital to remind ourselves that these standards are not necessarily the 'best' standards, but 'good' standards for a minimum threshold of cyber security protection. It is, largely, also for the markets and industry to develop best practices for the sector. It is in this regard that Taiwan presents such a useful observational target. Its response to the cyber security threat, catalysed by its geopolitical environment and the importance of the LNG sector there, has shown that law and industry practice must work in tandem.

APPENDIX

Table A1. LNG Sources of Taiwan

Sources of Imported LNG																				
Period	Total	Qatar		Australia		Russia		Papua New Guinea		Indonesia		United States		Malaysia		Brunei Darussala		Nigeria		Others	
	(10^3 MT)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)	(10^3 MT)	(%)
2011	11,984	3,877	32.3	335	2.8	186	1.5	–	–	1,958	16.3	–	–	3,321	27.7	–	–	660	5.5	1,648	13.8
2012	12,488	5,784	46.3	247	2.0	–	–	–	–	1,898	15.2	–	–	2,795	22.4	–	–	1,159	9.3	607	4.9
2013	12,547	6,107	48.7	60	0.5	64	0.5	–	–	1,959	15.6	–	–	2,928	23.3	61	0.5	570	4.5	797	6.4
2014	13,277	5,824	43.9	75	0.6	64	0.5	977	7.4	2,146	16.2	–	–	2,834	21.3	625	4.7	117	0.9	616	4.6
2015	14,229	6,620	46.5	254	1.8	252	1.8	1,371	9.6	2,349	16.5	105	0.7	2,305	16.2	675	4.7	59	0.4	240	1.7
2016	14,845	6,210	41.8	263	1.8	1,267	8.5	1,344	9.1	2,022	13.6	–	–	2,555	17.2	302	2.0	486	3.3	397	2.7
2017	16,508	5,089	30.8	1,012	6.1	1,658	10.0	1,847	11.2	2,148	13.0	164	1.0	3,001	18.2	427	2.6	494	3.0	669	4.1
2018	16,808	4,833	28.8	2,563	15.2	2,301	13.7	1,153	6.9	1,142	6.8	254	1.5	2,799	16.7	679	4.0	184	1.1	902	5.4
2019	16,581	4,667	28.1	4,394	26.5	1,478	8.9	1,451	8.8	351	2.1	505	3.0	2,479	14.9	246	1.5	204	1.2	807	4.9
2020	17,749	4,959	27.9	4,728	26.6	2,401	13.5	1,624	9.2	1,134	6.4	1,007	5.7	709	4.0	254	1.4	391	2.2	541	3.0
2021	19,439	4,765	24.5	6,265	32.2	1,893	9.7	1,434	7.4	1,171	6.0	1,761	9.1	495	2.5	60	0.3	583	3.0	1,012	5.2
2022																					
2022/01	1,534	415	27.1	566	36.9	54	3.5	160	10.5	–	–	172	11.2	0	0.0	–	–	–	–	166	10.8
2022/02	1,451	419	28.8	443	30.5	135	9.3	155	10.7	–	–	117	8.1	–	–	–	–	–	–	182	12.5
2022/03	1,677	299	17.8	596	35.5	126	7.5	78	4.7	171	10.2	181	10.8	–	–	–	–	105	6.3	121	7.2
2022/04	1,715	479	27.9	607	35.4	64	3.7	78	4.6	55	3.2	163	9.5	137	8.0	–	–	–	–	131	7.6
2022/05	1,647	483	29.3	605	36.8	128	7.8	77	4.7	122	7.4	231	14.0	–	–	–	–	–	–	0	0.0
2022/06	1,564	420	26.9	519	33.2	121	7.7	155	9.9	117	7.5	233	14.9	–	–	–	–	–	–	–	–
2022/07	1,875	512	27.3	579	30.9	201	10.7	79	4.2	56	3.0	183	9.8	198	10.5	–	–	–	–	66	3.5
2022/08	1,762	449	25.5	684	38.8	64	3.6	151	8.6	112	6.3	245	13.9	–	–	–	–	–	–	57	3.2
2022/09	1,767	479	27.0	851	48.2	–	–	78	4.4	185	10.5	117	6.6	–	–	–	–	–	–	59	3.3
2022/10	1,690	420	24.9	728	43.1	70	4.1	70	4.1	112	6.6	169	10.0	122	7.2	–	–	–	–	–	–
2022/11	1,573	417	26.5	569	36.1	–	–	157	10.0	112	3.5	177	11.2	144	9.1	–	–	55	3.5	–	–
2021/01–11	17609.6	4403.786	25.01	5664.579	32.17	1691,453	9.605	1261.076	7.161	1170.945	6.649	1688.04	9.586	495.0971	2.812	60.11082	0.341	469.9653	2.669	704.5464	4.001
2022/01–11	18.255	4,790	26.24	6,748	36.97	963	5.274	1,239	6.788	986	5.398	1,988	10.89	600	3.287		0	160	0.877	782	4.282

The table shows Taiwan's LNG sources from different countries.
Source: Energy Statistics Information System (Taiwan); https://www.esist.org.tw, accessed 18 July 2023.

Table A2. LNG Carriers being the Lifeblood of Taiwan

Year	Natural Gas Supply			Transformation Input			Natural Gas Consumption							
	Unit 10^3m^3													
	Total	Indigenous Production	Import	Total	Petroleum Refineries	Power Generation and Cogen.	Total	Energy Sector Own Use	Industrial Sector	Transport Sector	Agriculture Sector	Service Sector	Residential Sector	Non-Energy Use
2003	8,131,636	830,893	7,300,743	5,632,271	–	5,632,271	2,484,491	487,258	861,906	–	–	269,994	865,332	–
2004	9,868,080	795,353	9,072,727	6,963,871	10,457	6,953,414	2,664,738	491,325	956,165	–	–	313,253	903,995	–
2005	9,920,460	547,470	9,372,990	7,536,033	9,290	7,526,743	2,639,045	387,400	951,798	–	–	361,905	937,942	–
2006	10,627,387	462,958	10,164,429	7,788,823	33,486	7,755,337	2,619,765	362,471	987,028	–	–	373,292	896,974	–
2007	11,267,198	416,832	10,850,366	8,635,077	26,871	8,608,206	2,720,911	424,064	1,012,292	–	–	379,856	904,699	–
2008	12,236,091	357,356	11,878,735	9,542,745	25,173	9,517,572	2,765,086	468,651	959,639	–	–	418,875	917,920	–
2009	11,949,513	350,660	11,598,853	9,105,456	45,377	9,060,079	2,798,363	470,747	954,911	–	–	434,313	938,393	–
2010	14,822,026	296,200	14,525,826	11,665,149	23,941	11,641,208	3,185,737	591,394	1,180,670	–	–	507,053	906,620	–
2011	16,294,822	330,157	15,964,665	12,645,279	34,787	12,610,492	3,555,040	728,645	1,476,863	–	–	451,850	897,683	–
2012	17,136,367	442,049	16,694,318	13,007,469	40,823	12,966,646	3,876,987	747,875	1,845,878	–	–	403,309	879,925	–
2013	17,094,960	381,067	16,713,893	13,379,991	27,513	13,352,478	3,853,626	579,341	2,009,160	–	1,084	451,555	812,487	–
2014	18,068,487	379,356	17,689,131	14,265,147	31,153	14,233,994	3,847,580	330,660	2,214,200	–	3,100	493,104	806,516	–
2015	19,321,513	373,775	18,947,738	15,443,745	58,622	15,385,123	4,029,430	355,124	2,379,793	–	3,313	501,903	789,296	–
2016	20,065,721	321,471	19,744,250	16,221,022	14,055	16,206,967	4,138,256	243,177	2,563,893	–	3,785	517,536	809,864	–
2017	22,237,472	265,701	21,971,771	17,853,263	40,727	17,812,536	4,521,442	344,740	2,841,719	–	3,684	528,724	802,574	–
2018	22,628,371	197,587	22,430,785	17,814,742	74,003	17,740,740	4,904,890	379,936	3,144,522	–	4,356	504,067	872,009	–
2019	22,240,632	167,223	22,073,409	17,263,933	106,327	17,157,605	5,031,529	396,856	3,256,618	–	4,124	510,677	863,254	–
2020	23,785,910	105,340	23,680,570	18,877,144	57,496	18,819,649	5,350,577	536,712	3,396,182	–	3,992	500,305	913,385	–
2021	26,085,098	110,196	25,974,902	20,371,128	71,118	20,300,010	5,883,655	574,329	3,910,284	–	4,418	474,897	919,727	–
2021/01–11	23,628,376	100,567	23,527,810	18,582,163	63,806	18,518,357	5,365,885	529,530	3,561,808	–	3,708	428,257	842,583	–
2022/01–11	24,533,545	87,037	24,446,508	19,262,190	57,293	19,204,897	5,628,604	527,276	3,751,101	–	3,764	467,952	878,511	–
Compared with last month (%)	−7.2	−2.7	−7.3	−9.7	−55.4	−9.5	0.5	−5.3	−1.8	–	52.8	5.3	16.1	–
Compared with the same month of last year (%)	−4.5	−14.2	−4.5	−10.1	−71.4	−9.9	−1.1	15.6	−5.1	–	−39.5	3.3	4.8	
Compared with the same period of last year (%)	3.8	−13.5	3.9	3.7	−10.2	3.7	4.9	−0.4	5.3	–	1.5	9.3	4.3	–

LNG carriers has become Taiwan's lifeblood. According to the following data counted by the Bureau of Energy, the import figure saw a steady increase, showing a growing tendency in these years.
Source: Energy Statistics Information System (Taiwan); https://www.esist.org.tw, accessed 18 July 2023.