Journal of World Energy Law and Business, 2024, **00**, 1–10
https://doi.org/10.1093/jwelb/jwae020
Article

OXFORD

Cybersecurity risks of automated (and autonomous) offshore oil and gas units—the IMO cybersecurity rules framework

Juei-Cheng Jao*,‡, Jason C.T. Chuah †,‡

ABSTRACT

Automated and/or autonomous offshore platforms or units are becoming more important in the energy sector, whether they are being used for oil and gas extraction or for carbon storage purposes. Automation means that harsh working conditions and risks of personal injury to crew could be cut to virtually zero. Automation also provides significant cost savings and helps make less attractive oil and gas fields more economically viable to exploit. However, automation does come with its own set of challenges—the notable one being the cybersecurity threat. Any regulation or international standard dealing with the cybersecurity risk which is relevant to automated offshore units is usually framed within those rules that apply to ships. This article examines to what extent that regulatory approach, especially that of the International Maritime Organisation's (IMO) regime, could and should apply to automated or autonomous offshore platforms. It argues that whilst, for now, the IMO cybersecurity guidelines are relevant, a more targeted regulatory approach is needed.

INTRODUCTION

There is very little discourse about the regulatory framework as applicable to Artificial Intelligence (AI) and cybersecurity concerns on automated (and/or autonomous) offshore oil and gas structures. In this article, AI is broadly taken as referring to computer systems which take autonomous or semi-autonomous decisions or actions based on certain parameters defined by the user. Automated drilling structures and platforms,[1] however, have become more mainstream. This is largely due to an increase in labour costs. Expert and specialist crew working on platforms are costly, and the support crew[2] too has to be factored in. Moreover, labour conditions on oil and gas platforms are challenging to say the least.[3] Automated platforms are also more efficient, as a

* Juei-Cheng Jao, Professor of Maritime Law, National Taiwan Ocean University, College of Ocean Law and Policy, No. 2, Beining Rd., Zhongzheng Dist., Keelung City 202301, Taiwan (R.O.C.). Tel: +886-2-2462-2192; Fax: +886-2-2462-0724; E-mail: jcjao@ntou.edu.tw
† Jason C.T. Chuah, Professor of Commercial and Maritime Law, Faculty of Law, Universiti Malaya, Malaysia and City, University of London, UK. Tel: 00603-79676500; E-mail: jason@um.edu.my, jason.chuah.1@city.ac.uk. Support for this research has been provided by the Ministry of Higher Education Malaysia via Fundamental Research Grant Scheme (FRGS/1/2022/SSI12/UM/02/10). The authors are additionally grateful for the assistance given by the National Science and Technology Council of Taiwan (NSTC 112-2634-F-019-001).
‡ Equal co-authors.

[1] In this article, both offshore drilling units and platforms will be considered collectively. The two are of course different but for ease of analysis of the challenge of cybersecurity, the terms may be used interchangeably.
[2] This includes staff carrying out support services such as catering, cleaning, security, technical work, etc.
[3] See survey results in Platform, Friends of the Earth Scotland and Greenpeace Report, '*Offshore Oil and gas workers' views on industry conditions and the energy transition*' (October 2020). The key findings as reported at p 6 are: '(a) 42.8% of oil and gas workers have been made redundant or furloughed since March 2020. (b) Satisfaction with health and safety standards was most commonly rated 3/5. (c) A high level of concern about employment and job security within the oil and gas sector. (d) A low level of confidence

general rule. They can operate without rest breaks and through treacherous weather conditions. That also means these uncrewed units could be used in high-yield oil and gas fields which are in some of the harshest climates in the world. Exploration and extraction would no longer be hampered by oppressive environmental conditions. Production yield per cost is thus higher. Remote control of the platforms can also allow for a quicker response in the event of an emergency. There is no need to await alerts from the crew as to any structural dangers.

Moreover, automated offshore platforms or units can be constructed much quicker than conventional units. There is no need to build living quarters, water supply, food storage, sewage facilities, etc. Safety checks may dispense with the human factor—for example, there is no necessity to provide for fire escapes beyond the most simple. In February 2019, Norwegian energy giant Equinor officially launched the world's first fully automated oil and gas platform. With no living quarters, the North Sea rig is entirely uncrewed and requires only one or two maintenance visits a year.

These advantages make it more feasible for countries with small fields to develop and exploit those relatively small deposits. In a country like Taiwan, for example, its state-owned China Petroleum Corporation makes it plain that Taiwan's offshore deposits are modest based on current (though limited) surveys, but the corporation continues its exploration of the area, demonstrating that as technology changes, relatively modest deposits can bring robust returns. It reported that it signed a Petroleum Contract for the Taiyang Block on 3 May 2017 with Total E&P Chine (TOTAL) and China National Offshore Oil Corporation. Approximately 8,131.6 km of 2D seismic survey data have been processed in 2021, and an additional 2,500 km^2 of 3D seismic commitment has also recently been made.[4] In 2022, it further announced its cooperation with Husky Energy International Corporation to search for oil and gas in deep-water areas in the Tainan basin. The joint venture has seen to completion of the relevant 2D and 3D seismic surveys in 2021. Other areas of the sea being studied include the Taishi and Tainan basins. But critically too is Taiwan's search for suitable offshore locations for carbon sequestration or storage. It also goes without saying that automated offshore units are ideally suited for carbon sequestration or storage activities. Indeed, offshore platform technologies could be re-purposed for carbon storage purposes. The drilling technologies used in offshore oil and gas exploitation activities can provide the fundamentals for drilling into saline aquifers or depleted oil and gas reservoirs for permanent CO_2 storage. These operations are capable of being conducted by robots—AI or digital intelligence.

Automation in offshore exploitation and production, and increasingly in carbon storage, is already a game changer. Moreover, with Taiwan's geopolitics, uncrewed units mean the risk of harm to human lives, unlike traditionally crewed offshore units. Many countries with smaller deposits or those seeking to gain socio-economically from carbon capture, the use of automated offshore units or platforms must surely look attractive.

However, the cybersecurity risk remains acute. Automation and AI-guided oil platform (and/or carbon storage) operations are subject to the same cyber vulnerabilities as autonomous ships are exposed to. This study will consider the extent to which International Maritime Organisation (IMO) principles on cybersecurity could apply to automated offshore platforms. It should be stressed that in this relatively modest work, the focus could only be cast on the cybersecurity principles, not the actual technical protocols and standards to be applied. Other than the constraint of space, a law-oriented study would not be best to do justice to those technical cybersecurity specifications.

in government support. (e) 81.7% said they would consider moving to a job outside of the oil and gas industry.' Broadly speaking, the Maritime Labour Convention 2006 (MLC) could extend to workers on offshore oil and gas platforms. The reason is that the MLC defines 'ship' as 'a ship other than one which navigates exclusively in inland waters or waters within, or closely adjacent to, sheltered waters or areas where port regulations apply' (art II (1)). There is actually therefore no explicit definition of a ship although there are exclusions as those vessels or vehicles that navigate exclusively in certain waters. The question as to whether the 'ship' has to be mobile, that is to say, be capable of navigating and actually is navigating before it is deemed a ship. If that is to be the case, platforms that have been fixed for a period of time would not be treated as a ship. The point here, however, is not so much that the MLC applied or not but the fact that where it does not, the workers' working conditions are purely a matter for domestic regulation. The point is that maritime law protection only applies to 'ships' and therefore 'seafarers'. This issue as to when an offshore unit is to be treated as a ship will be important when discussing the extent to which the cybersecurity protocols recommended by the IMO would be relevant and applicable.

[4] <https://www.cpc.com.tw/en/cp.aspx?n=2609> accessed 21 August 2024.

THE RESEARCH PROBLEM

The automated offshore units or platforms being used from Europe to Asia, whether for oil and gas or carbon storage purposes, show how essential AI and cyber systems are for drilling or reverse drilling functionalities of these units. It is not sufficient for automated and AI-guided robots to be working on platforms, which they already do with great frequency, but for maximum commercial value, the drill floor must also be automated. An oft-cited example of the automated drill floor solution is the one developed by Robotic Drilling Systems (RDS) and Siemens.[5] That system consists of drill floor robots, robotic roughnecks, multi-size elevators, and robotic pipe handlers. The entire system, as described by the developers,[6] works on the basis of every robot being used to be equipped with its own digital control system accommodated in a control cabinet. In this control cabinet, the software interprets sensor signals, translates process commands into motion control sequences, and coordinates the interaction of related robots.[7] The control cabinet essentially provides the digital or artificial intelligence required for handling pipes, positioning and attaching tools, and drilling.

The drill floor can thus be controlled remotely, often from onshore. That lack of physical proximity is necessarily a security risk. The technology therefore focuses on ensuring that communication between the control room and the robots is established through a highly secure system.[8] Industrial Ethernet switches are deployed to ensure that data are reliably transmitted between the various automation, drives, and visualization components. These switches are also designed to be used effectively in extremely harsh environments and for challenging applications such as drilling. Importantly, these switches are designed specifically for use in automation environments. As such, despite the absence of human intervention on the platform offshore, they are not easily susceptible to parts breaking down, needing service and maintenance, or requiring technical calibration by onsite manual assistance. Faults could be rectified by remote programming rather than onsite repairs of physical parts.

There are automated systems and devices on the platform or unit. These may include automated and intelligent choke systems, pipes and valves, mud injection systems, etc. The fully autonomous oil and gas platform is no longer in the future, it is here in the present.

The cyber resilience of the systems of the offshore platforms and their onshore control rooms are only as good as the technology. There is ample literature on the technical aspects of cybersecurity controls,[9] but advances must also be made with cybersecurity defensive practices, manual or otherwise. The problem is even more acute in offshore units because these units have a lifespan of 20–30 years. Cybersecurity defences installed now could well be out of date in 20–30 years' time,[10] even if there is regular maintenance. The matter is made even more pressing because traditional and conventional cybersecurity practices do not apply easily to industrial control systems (ICS). The former relates more to systems that collect, process, and move data, whilst the latter is used to *control* industrial processes such as manufacturing, product handling, production, and distribution. ICS include deploying data to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.[11]

[5] See <https://references.siemens.com/en/reference/robotic-drilling-systems-as?id=4DE60E28801F660010CB0CA91AB80D0D> also reported in the industry newletter, Offshore Magazine (8 March 2018). <https://www.offshore-mag.com/drilling-completion/article/16762142/robotic-drilling-system-improves-efficiency-safety-quality> accessed 21 August 2024.

[6] ibid.

[7] The technology is very well explained in the article above (n 5).

[8] In the RDS and Siemens automated drill floor, the security modules are labelled Scalance S. Siemens describe the system in this manner. Siemens' portfolio of Scalance switches comply with a broad spectrum of approvals required in the oil and gas industry. For example, ATEX, FM, IECEx, and UL HazLoc approvals for use in hazardous areas, as well as ABS, BV, DNV GL, and LR for marine applications. The Scalance X-200IRT managed Industrial Ethernet switches, operating in isochronous real time, have been specifically designed for stringent real-time applications. They can be used for high-performance machine-level applications all the way up to networked plant sections in Profinet environments (n 6).

[9] A targeted search on Web of Science will produce hundreds of related scientific articles.

[10] This point was also made with reference to ships by KD Jones, K Tam and M Papadaki, 'Threats and Impacts in Maritime Cyber Security' (2016) 1 Engineering & Technology Reference. https://doi.org/10.1049/etr.2015.0123.

[11] See US NIST SP 800-30 Rev. 1 under Industrial Control System from NIST SP 800-39.

Automated offshore units by virtue of their functions would connect their operational technology (OT) systems to their information technology (IT) systems to enable and expand enterprise-wide connectivity and remote access for enhanced business processes and capabilities. This integration of IT and OT networks unfortunately also provides malicious actors, including nation-states, common criminals, and insider threats, a conducive environment where they can exploit cybersecurity vulnerabilities to compromise the integrity of ICS and their data.[12] These malicious actors would gain access and thereafter corrupt or compromise data or system integrity,[13] hold ICS and/or OT systems ransom, damage ICS machinery, or, in the case of automated offshore oil and gas units, cause serious marine pollution. Hence, the importance of ensuring the right response.

At present there is no specific, explicit regulatory attention placed on the cybersecurity risks of automated offshore oil and gas units. The approach seems to be to leave it to the same standards applicable to ships.[14] The research question in this article is thus notably how and to what extent the IMO cybersecurity regime, especially the organization's cybersecurity regulatory principles, might apply. There are good reasons why the focus here is on the IMO regulatory approach.

First, offshore oil and gas platforms are often regulated as ships. Platforms can be fixed, floating, or mobile. Although it is not the intent of this article to venture in-depth into the subject of the definition of 'ships',[15] it seems to follow where offshore units are being repositioned or moved, they could be treated as ships and where they are fixed, they cease to be treated as ships.[16] That said, national law might provide that certain types of fixed oil units might actually be treated as ships where they are towed for placement at sea or for dismantling in or out of the sea. For example, Finnish legislation states that 'ship means a vessel of any type whatsoever, including floating craft, whether self-propelled or towed by another vessel … '.[17] In the event of marine pollution, Finnish law makes it plain that the fixed unit shall be treated as a ship, thereby attracting all the liabilities and defences available to a ship causing pollution.[18] Similarly, Spanish law considers fixed units as ships where it concerns dumping at sea.[19] In Taiwanese law, Article 3(1) of the Law of Ships[20] provides that '"Ship" denotes water vehicle that carries people or cargo on the surface or in water, including passenger ship, cargo ship, fishing boat, vessel of special purpose, yacht and small ship'. The Chinese language version[21] is perhaps closer in stressing that a ship is a moveable water vehicle. Regardless of the disputations about the definition of ships and offshore units, it suffices to state that there are *some* commonalities between the two and as a result, this gives us good cause to consider the IMO standards and guidelines. Adjunct to this is the fact that many offshore units are classed by maritime classification societies.[22]

[12] US NIST Special Publication 1800-10 Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector (March 2022) at p 1; also AS Mohammed, and others, 'Cybersecurity Challenges in the Offshore Oil and Gas Industry: an Industrial Cyber-physical Systems (ICPS) Perspective' (2022) 1 ACM Transactions on Cyber-Physical Systems (TCPS) 6.3.

[13] The X-Force Threat Intelligence Index 2021 (ibm.com) bears this out; it finds that manufacturing and production was the second-most-attacked industry in 2020, up from eighth place in 2019.

[14] See below generally.

[15] Indeed, the issue of whether an oil rig is a ship, legally speaking, has plagued maritime lawyers for a long time (M Summerskill, *Oil Rigs: Law and Insurance* (Stevens & Sons 1979) 12). See too references provided by M. Musi, *A Study on the Floating Units Operating in the Oil and Gas Offshore Fields: The Need for a Juridical Placement and the Quest for the Applicable Discipline* (Il Diritto Marittimo-Quaderni 2016) 95–130. On the subject more generally from an international law perspective, see H Esmaeili, *The Legal Regime of Offshore Oil Rigs in International Law* (Routledge 2017).

[16] Support for this view is not universal, but a good majority of domestic national shipping laws appear to place much emphasis on the ability of the 'ship' to navigate the sea. See Esmaeili (n 15) ch 3.

[17] Order No 710, 1972, UNLS, National Legislation and Treaties Related to the Law of the Sea, ST/LEG/SER.B/18 (1976) 195.

[18] 1983 Law on the Prevention of Pollution from Ships, as amended, art 1.

[19] Act No 21 (Dumping from Ships or Aircraft), 1977, United Nations Legislative Series, National Legislation and Treaties Related to the Law of the Sea, ST/LEG/SER.B/19 (1980).

[20] 船舶法 as amended on 28 November 2018.

[21] '船舶：指裝載人員或貨物在水面或水中且可移動之水上載具, 包含客船□貨船□漁船□特種用途船□遊艇及小船□

[22] See WM Hannan and JC Scherwin, 'Classification And Certification Of Offshore Units' *Paper Presented at the Offshore Technology Conference*, Houston, Texas, May 1978; also the offshore oil and gas units manuals used by Bureau Veritas, a classification society <https://marine-offshore.bureauveritas.com/rules-guidelines> accessed 21 August 2024.

Secondly, there are few cybersecurity rules applicable to large objects placed at sea. The IMO standards are targeted specifically at vessels at sea. The maritime context thus becomes relevant—even more so when there is no direct regulation on cybersecurity and offshore units.

Thirdly, the IMO standards are framed to work on the basis of mutual cooperation between operators—such as shipowners, charterers, port authorities, cargo handlers, freight forwarders, etc. There is a similar chain or network of stakeholders in offshore exploration and drilling. A reference purely to national cybersecurity law is not ideal. Cybersecurity laws are aimed at placing liability ultimately. It is not primarily to foster a culture of cybersecurity awareness and common endeavour amongst the participants in the 'food chain'.

Fourthly, most standard industry technical standards and operational guides for oil and gas platforms do not make explicit provisions for cybersecurity. For example, the widely used American Petroleum Institute manuals on safe operation of oil and gas platforms cover most physical and process-related safety issues, such as corrosion tests, structural integrity, human element, seismic resilience, choke systems, pipe design, etc. There is no mention of cybersecurity considerations—these manuals are largely directed at conventional platforms. To be fair, there are general cybersecurity guidelines in the public domain, although those may not directly address remotely controlled or automated oil and gas platforms.

Lastly and importantly, IMO standards are expressed to be applicable to offshore platforms and units.[23] It is common knowledge that there are no universally applicable definitions of ship types; there are specific descriptions and names used within IMO treaties and conventions. Under the International Convention for the Safety of Life at Sea, a mobile offshore drilling unit (MODU) is taken to mean a vessel capable of engaging in drilling operations for the exploration for or exploitation of resources beneath the seabed such as liquid or gaseous hydrocarbons, sulphur, or salt.[24] Of course, once a drilling unit is fixed onto the seabed and is no longer mobile, the relevant IMO provision ceases to apply. But as regards cybersecurity considerations, it is submitted that there is very little material difference between an automated fixed and mobile offshore unit.

A CAVEAT

Although the emphasis of this article is on IMO's cybersecurity regulatory framework, that is not to say that a maritime approach is *necessarily* best equipped to address the special issues and problems automated offshore units or platforms attract. Whether there should be some cybersecurity code applicable to such units must, however, form the subject for further study. For the purposes here, the proposition is that *for the time being* the IMO regulatory framework should be examined as to their suitability and adaptability to accommodate the challenges of automated offshore units. It is equally important to re-emphasize that it could not be the purpose of this *legal* research to examine the practicability and suitability of the precise technical and systems specifications.

EVALUATING THE IMO CYBERSECURITY APPROACH

As noted above, the IMO has provided recommendations[25] for addressing the cyber risks associated with the maritime industry and developing and implementing best practices through the shipping company's safety management system.[26] In this context, maritime cyber risk refers to 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.[27] In contrast, engineers would define cybersecurity in the domain of industrial automation and control systems, as 'actions

[23] part 1, Annex to the IMO Guidelines (IMO document MSC-FAL.1/Cir 3).
[24] SOLAS IX/1, MODU Code 2009, para 1.3.40.
[25] See para 1 Annex to the IMO Guidelines (n 23).
[26] M Caprolu and others, 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead' (2020) 58 IEEE Communications Magazine 90.
[27] Para 1 Annex to the IMO Guidelines (n 23).

required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets'.[28] The focus of the IMO is naturally on those functions, which are 'shipping-related' but shipping is undefined.

The IMO recommendations and the industry guidelines closely mirror the five-step framework of the United States National Institute of Science and Technology (NIST), that is identify, protect, detect, respond, and recover.[29] They have, since 1 January 2021, become mandatory for all ships following the onshore shipping company's first annual verification of the Document of Compliance. Its compliance will be inspected by Port State Control officers.

It is useful to refer to the highly influential guidelines produced by the shipping industry, which reflect the approach of the IMO Guidelines:

> Approaches to cyber risk management will be company- and ship-specific but should be guided by the requirements of relevant national, international and flag state regulations. These guidelines provide a risk-based approach to identifying and responding to cyber threats. An important aspect is the benefit that relevant personnel would obtain from training in identifying the typical modus operandi of cyberattacks.[30] (emphasis added)

The IMO's own characterization of its regulatory approach is expressed as being framed by three pillars:

a) guided by applicable technical and framework standards and legislation.

The IMO framework is expressly stated to be inexhaustive. It is nevertheless important because other regulatory, legislative, and even contractual control mechanisms adopted at industry, national, and international levels should reflect its high-level principles. A conflict between regulatory approaches would not be ideal.[31]

Therefore, although private and non-governmental organizations have developed separately, their own guidelines for the protection of ships, ports, and connected organizations from cyber threats,[32] these to an appreciable extent take the three-pillared approach of the IMO guidance. The IMO expressly refers to some of the good practices recommended by the industry in the guidelines.[33]

b) Two objects of control and monitoring—the company and the ship.

In the main, the 'private' industry guidelines, not unlike the IMO Guidelines, are directed at shipping and ports. The guidelines from DNV (Det Norske Veritas),[34] however, do explicitly state that they are addressed at the cybersecurity risk defence framework for '*mobile* offshore units in operation',[35] whilst Lloyd's Register's guide states that it applies to 'marine platforms', the American Bureau of Shipping guidelines uses even more generalized language, 'marine and

[28] IEC 62443-1-1 (2009) IEC 62443-1-1:2009, Industrial Communication Networks—Network and System Security—pt 1–1: Terminology, Concepts and Models. *International Electrotechnical Commission*, Geneva, p 15.

[29] para 3.5 Annex to the IMO Guidelines (n 23).

[30] The Guidelines on Cyber Security Onboard Ships Version 4 (2020) as produced by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, and WORLD SHIPPING COUNCIL, p 1.

[31] On the problem of inconsistent approaches in cybersecurity regulation, see A Marotta and S Madnick, 'Convergence and Divergence of Regulatory Compliance and Cybersecurity' (2021) 22 Issues in Information Systems 1. At a theoretical level, the problem of inconsistent regulatory approaches is examined in E Cauble, 'Exploiting Regulatory Inconsistencies' (2017) 74 Washington and Lee Law Review 1895.

[32] For instance, BIMCO has proposed a guideline for shipboard IT and OT systems for the identification of threats and vulnerabilities, their assessment, development of mitigation and contingency measures, and responding and recovering from such threats (ibid). The American Bureau of Shipping too has prepared guidelines for marine and offshore operations on cybersecurity, best practices, criteria for assessment of systems/assets and certification, concepts of data integrity, software systems verification, and quality management. (American Bureau of Shipping, *The Application of Cybersecurity Principles to Marine and Offshore Operations* (2016)). Lloyd's Register also provides guidelines for stakeholders on the design, installation, integration, and operation of digitally enabled systems onboard ships and marine platforms to understand the implications of technology in digital systems. (See Lloyd's Register, 'LR Issues Technical Guidance for Ship Design in a Digital Age'. 2016). So too has DNV-GL provided guidance on the application of standards such as ISO/IEC 27001 and ISA-99/IEC-62443 (standard for OT security of industrial control systems such as Global Positioning System). (See DNV-GL, 'Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation' (2016) DNVGL-RP-0496.).

[33] para 4.2 Annex to the IMO Guidelines (n 23).

[34] ibid

[35] Emphasis added.

offshore operations'. The latter two do not seem to make any distinction among mobile floating units, mobile units which have been fixed and fixed units.

The focus on navigational aspects is not helpful because it could misallocate the level of risk on an aspect of the operations of the automated offshore unit which is not central, or for that matter might even be non-existent where the unit is stationary.

c) A risk-based approach.

It is submitted that risk, as a legal notion, is not easy to define. It might be loosely described as a 'combination of the likelihood of an adverse event (hazard, harm) occurring, and of the potential magnitude of the damage caused' (the incident itself, the number of people affected, and the severity of the damage for each).[36] A risk-based approach therefore entails the regulators assessing the 'risk' (as described above) and the actions to be taken in response. It has also been said that it is a particular strategy or set of strategies that regulators use to target their resources at those sites and activities that present threats to their ability to achieve their objectives.[37]

The justification for the adoption of a risk-based approach by the IMO is patent:

> These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these Guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.[38]

The subject of the IMO risk-based approach merits further examination, especially in the context of increasing use and dependence on automation in offshore oil and gas activities.

THE HIGH-LEVEL PRINCIPLES

The IMO Guidelines are fairly generalized, or in other words, high level. They do, however, guide the approach flag states, coastal states, and port states should take vis-à-vis cyber threats. There are a few of these high-level principles, worth discussing in the context of automated offshore units.

Risk management approach

First, the guidelines are premised on the notion of risk management[39]—that, to an appreciable extent, it is submitted, depends on a principle of proportionality. Whoever has the authority or the person in charge should analyse and evaluate the risks involved and then decide what and to what extent a defensive or protective system is needed. These are of course technical issues but from a legal perspective, the exercise of this discretion must be tested. Analysis of the risk, it is argued, must entail at the very least the dissecting of:

- the potential sources of threat;
- the way or openings the attack could enter;
- the role of manual controls, their effectiveness, and vulnerabilities;
- the systems and processes that might be attacked;
- the extent of the potential physical and commercial harm;
- the exposure to regulatory sanctions for failure to prevent the harm;

[36] See *Introducing a Risk-Based Approach to Regulate Businesses* (World Bank Group 2014), (Introducing a risk-based approach to regulate businesses: how to build a risk matrix to classify enterprises or activities (worldbank.org)) accessed 21 August 2024. The legal notion of risk is been much airing in the field of financial regulation. It is useful to borrow from the increasing more common understanding of the notion amongst finance and banking regulators.

[37] J Black, 'The Emergence of Risk-Based Regulation' [2005] Public Law 512; also J Black and R Baldwin, 'Really Responsive Risk-Based Regulation' (2010) 32 Law & Policy 181.

[38] para 2.1.8 Annex to the Guidelines (n 23).

[39] para 1.4, Annex to the Guidelines (n 23).

- the moral hazard issue—notably loss of reputation; and
- the likelihood of contagion.

Evaluation of the risk should require a qualitative assessment of cost and convenience factors against the magnitude of the risk factors above. Evaluation, it is suggested, is often the weak link in the risk-based approach advocated in the IMO Cybersecurity Guidelines. At best, the person in charge could only look to industry practice but in the offshore oil and gas sector, where commercial secrecy is important, this could really only offer the slimmest of pickings. If that exercise of discretion cannot be tested or challenged legally, regulation becomes difficult. Whilst not disputing the relevance of a risk-based system, as the threats of cybersecurity continue to grow apace, decision-makers, whether persons in charge of cybersecurity or regulators from coastal states, could well benefit from some explicit rules. Indeed, a compliance approach or rule-based system is not inconsistent with the risk-based system preferred by the IMO.

This is especially the case with smaller operators or independents in the oil and gas sector. Given their resource limitations, there should be some essential rules or requirements that they should comply with, and then only use risk management for making exceptional choices and justifying the costly measures to be taken.

Similarly, a risk-based regime clarified by a compliance, rule-based system also has the advantage of providing guidance to emerging economies where the state of technical expertise is nascent. That is all the more critical in the context of automated offshore oil and gas units. Unlike the very vast shipping sector, offshore units are not subject to the same controls and monitoring by flag states, port states, and coastal states. They are materially only subject to the supervision of the state where the unit is intended to be pitched. That is even more the case with fixed offshore units.

The ancillary question then is what should be the role of the classification societies when classing offshore units. For them obviously, from a traditional emphasis of the classification exercise being placed on operations in the physical domain, shifting the attention to the software and hardware of systems dealing with operations and processes has raised a new set of challenges.[40] That is compounded by the fact that cybersecurity risk management must be applied from the inception, notably the design stage, right to the stage of asset disposal. The disposal of ships might be less complex and perceptibly less regulated than the disposal of offshore units.

Vulnerable functions

The IMO Guidelines do identify, though not exhaustively, the kind of systems which could be vulnerable to cyber threats. These include, but are not limited to:

1) bridge systems;
2) cargo handling and management systems;
3) propulsion and machinery management and power control systems;
4) access control systems;
5) passenger servicing and management systems;
6) passenger facing public networks;
7) administrative and crew welfare systems; and
8) communication systems.

It is immediately obvious that these are systems, which are commonplace in ships. Of course, the IMO Guidelines stress that this is not an exhaustive list, and it is open to reason that functionalities of automated offshore oil and gas units could well involve some of these systems. However, the generalized tenor of the guidelines does not inspire confidence as to their appropriate relevance to automated offshore units. The IMO guidelines do, however, refer to other international protocols. To that extent, some of the guidelines from the classification societies refer to what

[40] On the technical challenges, see section 2, DNV-GL. 2016 (n 32).

constitutes vulnerable systems which could embrace the functionalities of automated offshore units. That said, it would be fitting to devise a more platform or unit-specific regime of cybersecurity controls, as more and more oil and gas companies adopt automation for their rigs and platforms.

Separation between IT and OT systems

An important facet of the IMO guidelines is acknowledging the distinction between IT and OT systems.[41] As mentioned earlier, IT systems tend to focus on the use of data as information, whilst OT systems concern the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.

This aspect is critical for automated offshore units and platforms. That said, a survey of the guidelines[42] of the different classification societies reveals, as to be expected, a concentration on the operations on board vessels—the main focus is very much the cargo or passenger carrying functions of the vessel.[43] Navigational aspects too feature very starkly as part of the OT systems.[44] These are naturally not the conventional IT and OT aspects of an automated offshore platform or unit, especially a fixed, immovable one.

Effective cyber risk management should start at the senior management level

A central plank of the IMO's approach is to place cybersecurity risk management at the senior management.[45] This is consistent with its focus on ship and company operations.[46] Considering that legal persons cannot make autonomous decisions, the role of human agency becomes important where responsibility and subsequent liability or fault is to be attributed. However, with the intervention of AI in the OT systems, a *decision framework* for risk management must be given proper consideration. The decision-making chain in the case of an automated offshore oil and gas unit may be predominantly human, predominantly AI, and, human and AI 'cooperating'[47] with each other. It is suggested that a proper decision framework would help provide a clear structure for classifying risk decision problems and a procedure for execution of the related decision-making processes. It could also provide a checklist for what concerns, constraints, and challenges to address when seeking out the best decision alternative. It is submitted that this rule-based or checklist system is not inconsistent with the risk-based approach, as discussed above.[48]

This issue of having a proper decision framework was well-recognized in the offshore sector, at least in the UK. As early as 1999, the United Kingdom Offshore Operators Association (UKOOA) published guidance to develop a framework to facilitate and guide the process of decision-making.[49] That guidance was subsequently replaced in 2014 with several important upgrades as the industry continues to modernize. However, fast forward to the present decade of automated or autonomous offshore activities, work should be expended for the re-design of the guidance to accommodate the human–AI interface. Classification societies in their guidelines have also tried to do that, but as stated their guidelines are largely directed at ships, not offshore units. Of course, any updating of the decision framework guidelines, two observations should be made.

[41] para 2.1.2 Annex to the Guidelines (n 23).
[42] DNV-GL. 2016 (n 32).
[43] Eg, The Guidelines on Cyber Security Onboard Ships Version 4 (2020) (n 30) as produced by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, and WORLD SHIPPING COUNCIL provide in ch 3 (pp 13–14) the areas that concern the IT and OT division are in the bridge operations, propulsion and machinery management and power control systems, access control systems (ie digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic 'personnel-on-board' systems), passenger servicing and management systems, passenger facing public networks, administrative and crew welfare systems, and communication systems.
[44] ibid.
[45] para 3.3 Annex to the Guidelines (n 23).
[46] See section titled "Vulnerable Functions" above.
[47] Cooperating is used to describe the mutual reliance between human decisions and automated or autonomous decisions—eg, the algorithms manually programmed into the AI.
[48] See section titled "Risk management principles" above.
[49] UKOOA, 'A framework for risk related decision support—industry guidelines', UK Offshore operators association; 1999; UK now replaced by Oil and Gas UK, Guidance on Risk Related Decision Making Issue 2 July 2014 Final.

First, the guidance is largely directed at the UK oil and gas sectors, not internationally. Secondly, any revision or introduction by the industry or regulators of a decision framework for managing risks in the automated offshore sector should be made with some deference to the other 'applicable' rules and standards.[50]

The power of the senior management team to manage cyber risk must also embrace their role in making contracts with sub-contractors and suppliers. The risk management scheme in the international guidelines all recognize the role and importance of third parties—especially sub-contractors who supply parts of the IT and/or OT systems whether as hardware or software or maintenance and programming services. Using the American Bureau of Shipping's Guidelines as an illustration, those guidelines had *originally* recommended that the shipyard may utilize subcontractor integration services or provide those services in-house. Paragraph 5.2 provides that:

i) If the Ship Builder Integrator (SBI) provides in-house integration services, it is expected to provide developed technical and operational system integration information to the Company.
ii) If the SBI utilizes a third party for system integration services, the SBI is expected to aggregate and provide subcontractor-developed technical and operational system integration information to the Company upon delivery of the vessel.

In the most recent version, additional organizations or individuals are added to the parties that the cybersecurity risk management plan must encompass.

> 5.3 Service Supplier (SS) Service Supplier (SS) may be original equipment providers (OEMs) or software development entities responsible for software implemented in the system subject to verification for notation. Verification of integrated systems provided by multiple SSs requires that all SSs participate in the verification process.[51]
>
> 5.4 Sub-Supplier (Sub-System or Component Providers) A sub-supplier is a provider of equipment parts or subcomponents embedded in or connected to SS equipment systems and is included in integration testing and verification.[52]

These new provisions demonstrate amply that attention must and is gradually shifting to include participants in the contract chain. The ultimate responsibility, however, remains vested in the company with control of the offshore unit. Hence, the importance of that company ensuring that third parties in the chain or network of commercial and non-commercial participants are contractually bound to the same risk management priorities as the company (and ship/platform) in question.

CONCLUSION

This article has explored the extent to which the current cybersecurity principles and regulatory approaches adopted in the maritime sector, notably, the IMO Guidelines, could and should be extended to automated or autonomous offshore oil and gas units. It is concluded that although those maritime cybersecurity regimes are principally aimed at ships, there are reasonably sound reasons why the maritime sectoral approach is by and large a workable template for regulating cybersecurity for offshore units. That is despite the fact that often immovable offshore units are treated as ships. The inquiry then shifts to examining the effectiveness of the maritime cybersecurity strategy for automated offshore units. The conclusions are that the risk-based approach vaunted in the IMO guidelines should be tempered by a robust compliance or rule-based system given the peculiarities of the offshore business. An industry-wide code, for example, which takes on board the decision framework model in the Oil and Gas UK's Guidance on Risk Related Decision Making would be a good start.

[50] Such as those introduced or alluded to by the classification societies, etc.
[51] Introduced on 1 August 2023.
[52] ibid.

Journal of World Energy Law and Business, 2024, 00, 1–10
https://doi.org/10.1093/jwelb/jwae020
Article