Maritime Cybersecurity and the Australian Cyber Security Strategy

Dr Md Saiful Karim,[*] Dr Samuli Haataja,[**] Dr Simon McKenzie,[***] and Dr Michael Guihot[****]

Submission on the 2023-2030 Australian Cyber Security Strategy Discussion Paper

We welcome the Australian government's initiative for the adoption of the 2023-2030 Australian Cyber Security Strategy and the opportunity for submission on the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

We are a group of legal researchers from the Queensland University of Technology (QUT) and Griffith University with expertise on the law of the sea, maritime law, cyber law, technology law and public international law generally.

Our submission is mainly relevant to Question 5 of the Discussion Paper relating to Australia's contribution "to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space".[1] However, the future Cyber Security Strategy should give equal importance to the development of international law for **responsible behaviour of non-state actors** in cyberspace. A robust international legal structure for the responsible behaviour of non-state actors is of paramount importance for ensuring global maritime cybersecurity. The same can be said for some other sectors.

Australia should take a leading role in the International Maritime Organisation (IMO) for the development of international law for enhancing maritime cybersecurity.

The international maritime transport industry is currently facing exponential growth in cyber-attacks.[2] Ships, ports, shipping companies and offshore infrastructures (e.g., offshore hydrocarbon structures) face unprecedented cyber threats. For example, recently, a cyber-attack on ShipManager software of DNV affected the operation of 1000 ships.[3] Cyber insecurity is further increased due to the digitalisation and automation of the maritime industry in the post-COVID world.[4]

The IMO[5], as the global "machinery for cooperation" for the development of international law

---

[*] Associate Professor and Leader, Ocean Governance Research Group, School of Law , Queensland University of Technology (QUT).
[**] Senior Lecturer, Griffith Law School, Griffith University.
[***] Lecturer, Griffith Law School, Griffith University.
[****] Senior Lecturer, School of Law, Queensland University of Technology (QUT).

[1] 2023 - 2030 Australian Cyber Security Strategy Discussion Paper, https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

[2] Frank Akpan et al. Cybersecurity Challenges in the Maritime Sector, (2022) 2(1) *Network* 123; Victor Bolbot et al., 'Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis' (2023) 39 *International Journal of Critical Infrastructure Protection*, article number l100571; UNCTAD, Review of Maritime Transport 2020, https://unctad.org/system/files/official-document/rmt2020_en.pdf.

[3] Jamey Bergman, DNV confirms ShipManager cyber attack hit 1,000 vessels, 18 January 2023, https://www.rivieramm.com/news-content-hub/news-content-hub/dnv-reports-cyber-attack-on-its-shipmanager-software-74466

[4] Akpan et al., above note 2; UNCTAD, above note 2.

[5] The organisation was established as the Inter-Governmental Maritime Consultative Organisation (IMCO) after its constituent legal instrument entered into force in 1958. The name of the organisation was changed to the

and policy for the maritime industry,[6] is the main forum for international cooperation in developing effective international legal structures for combating maritime cyber threats. In the last six and half decades since its founding, it has become the main forum for international legal development for ensuring maritime safety, security, and prevention of marine pollution from ships.

The IMO's initial focus was maritime safety, and the organisation assumed the administrative responsibility for the International Convention for the Safety of Life at Sea (SOLAS), which was first adopted in 1914 following the Titanic accident. The IMO took the initiative for several revisions of the SOLAS, and the current version of the Convention was adopted under its auspices in 1974. This version of the Convention, with subsequent amendments, is the cornerstone for maritime safety. In 2004, a new chapter incorporating the International Ship and Port Facility Security (ISPS) Code was added expanding the ambit of SOLAS to encompass maritime security.[7] This was not the first legal development enhancing maritime security led by the IMO. The organisation undertook the legislative development after the *Achille Lauro* incident by adopting an international legal instrument for combating maritime terrorism, namely the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, including its Fixed Platform Protocol in 1988. [8] Both legal instruments were further amended in 2005 as a response to increasing threats of terrorist attacks.

This history suggests that the IMO is best placed to grapple with how international law should be developed to enhance maritime cybersecurity. Much work needs to be done. Cyber risks are only mentioned inconsequentially in the non-binding part of the ISPS Code and other than this, the IMO has adopted non-legally binding guidelines and a resolution on integrating cyber risk in ship safety management systems.[9] However, as the recent maritime cyber-attacks show, this initiative by the IMO is inadequate for ensuring a cyber secure maritime industry.

Considering the growing threats of cyber-attacks to the maritime sphere there is an urgent need for an IMO initiative for further international legal development for enhancing maritime cybersecurity. The 2023-2030 Australian Cyber Security Strategy should include a clear strategy for Australia to take a leadership role in the IMO for the development of maritime cybersecurity-related international regulations.

Australia should contribute to agreement about how international law applies in cyber context as this has implications for various areas of law, including international maritime law.

Australia's leadership at the IMO will be enhanced if it further develop its national position on how it considers international law to apply in the cyber context. While there has been considerable progress over the last decade, there continues to be uncertainty about crucial legal issues including those related to sovereignty, jurisdiction, and the attribution of responsibility for non-State cyber actors. These uncertainties can only be addressed by participation in

International Maritime Organisation (IMO) in 1982. For further detail see IMO, Brief History of IMO, https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx.

[6] Ibid.

[7] Md Saiful Karim, 'Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?' (2022) 143 *Marine Policy*, article number 105138.

[8] Md Saiful Karim, *Maritime Terrorism and the Role of Judicial Institutions in the International Legal Order* (Brill-Nijhoff, 2017).

[9] Karim, above note 7.

international law making, whether by contributing to customary international law by continuing to make public Australia's legal position on important issues in cyberspace or engaging in forums for multilateral law-making.

The continued uncertainty in general international law has consequences for specialised regimes, such as maritime law. It is more difficult for specialised forums - such as the IMO - to respond to and address cybersecurity issues when uncertainty remains about the some of these essential legal questions. Moreover, these questions are particularly acute in the maritime sphere where there are multiple and overlapping legal regimes and jurisdictional arrangements.[10] To take one very tangible example, international agreement on when State criminal jurisdiction applies to criminal cyber activities is a crucial part of determining how a regime for investigating and prosecuting cyber criminals that attack offshore maritime installations, or where cyber criminals are located on an offshore site that is beyond the territorial jurisdiction of any State. Australia can contribute to legal certainty by having a clear national position on these issues, ensuring that it is well-placed to contribute to strengthening the IMO legal regime in relation to cybersecurity.

Conversely, there are opportunities for Australia in supporting these specialised regimes to develop and trial novel approaches to the legal regulation of cyber activities that, if successful, could be applied more widely. The IMO offers an example of an international law-making forum that has generally been successful in developing and amending the regulatory regimes it administers. The IMO's focus on the safety and security of international shipping, combined with the range of State actors, industries, intergovernmental organisations, and non-governmental organisations involved in IMO processes, will help ensure that any regulatory framework is acceptable to a wide range of ocean users. The legal solutions for cyber regulation that emerge through this process may well be able to be adapted and applied in other regulatory contexts. Through consistent engagement with these specialised forums – such as IMO processes related to maritime cyber security - Australia has an opportunity to shape international law from the ground up.

Australia should clarify its position on the relationship between international law and norms of responsible state behaviour in cyberspace, particularly in relation to due diligence and the protection of critical maritime infrastructure.

Australia's national response to ensure the security of onshore and offshore critical maritime infrastructure must be consistent with international law. However, the relationships between the legal obligations of states to ensure the safety of ships and the safety of navigation or maritime traffic and the emerging international law of cyberspace still need to be clarified.[11]

As noted above, developing an approach to maritime cybersecurity at the national level requires clarity about Australia's international obligations. However, there continues to be uncertainty about the extent of the due diligence obligation of States for the protection of critical infrastructure. At the UN level, states have agreed to non-binding norms of responsible state behaviour in cyberspace.[12] However, there remains confusion about the relationship between

[10] Karim, above note 7.

[11] See generally, Karim, above note 7, 2.

[12] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (22 July 2015) (hereafter, Report of the Group of Governmental Experts); Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/70/237(30 December 2015).

some of these non-binding norms and binding international law obligations. For example, many maintain that the due diligence obligation is part of customary international law and that norm (c)[13] has the potential effect of reducing binding obligations into non-binding recommendations.[14] Similarly, norm (f)[15] seeks to limit cyber operations against critical infrastructure and makes express reference to a state's (binding) 'obligations under international law', resulting in what has been described as a 'contradiction in terms.'[16]

The status and scope of non-binding norms and how they relate to existing obligations from international law have implications for maritime security law. It will clarify the extent of Australia's responsibility for ensuring the cybersecurity of critical maritime infrastructures and when it can look to other States to manage and respond to cyber risk. After all, maritime infrastructure is critical to the economic and security interests of States: working ports and consistent shipping are essential parts of the supply chain for almost all goods, ranging from pharmaceuticals, consumer electronics, natural resources, and food.

The Cyber Security Strategy should recognise that strengthening maritime cyber security requires a multi-faceted approach including security-by-design as self-regulation, co-regulation at the national level, and cooperation to develop international law.

Artificial intelligence (AI) is playing a role in both the propagation of cyber-attacks and the defence to them. Cyber criminals using AI can amplify the scale and effectiveness of cyber-attacks through automated phishing attacks, speech synthesis, exploiting software vulnerabilities, and data poisoning. The problems with global regulation of AI were set out by Scherer who noted that (1) they could be developed without the need for large scale production frameworks, (2) that projects could be carried out anywhere in the world and transported globally, (3) that AI development can be carried out using discrete components that can create consequences unintended by the original developers of those discrete components and (4) that the technologies underlying AI models can be opaque to most regulators and even users.[17] These problems could also be ascribed to the inherent problems in the cyber context. Cyber-attacks can also be carried out from anywhere in the world without the need for deep infrastructure, transported globally, easily developed and implemented, and are opaque to regulators and targets alike.

This makes problems with regulating cybersecurity, as with problems associated with AI development, intractable—almost wicked. However, as with AI regulatory movements around the world,[18] Australia must participate in global efforts to regulate cybersecurity as set out elsewhere in this submission while maintaining a strong local regulatory stance. It can be argued that "systems need to be resilient to cyber threats, including the possibility of espionage, sabotage or manipulation by nefarious actors. Robustness may be achieved ex ante through

[13] 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'. Report of the Group of Governmental Experts, ibid, 8.
[14] Dapo Akande, Antonio Coco and Talita de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99 *International Law Studies* 4, 31.
[15] 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'. Report of the Group of Governmental Experts, above note 12, 8.
[16] Akande, Coco and Dias, above note 14, 32.
[17] Matthew U Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29 *Harvard Journal of Law and Technology* 354, 369.
[18] Michael Guihot and Lyria Bennett Moses, *Artificial Intelligence, Robots and the Law* (LexisNexis, 2020) see Chapter 10.

careful design choices..."[19] This type of security-by-design needs to be regulated, supported and reinforced at national and international levels for achieving legitimacy.[20]

In the maritime sphere, ship owners and shipping companies have a vested interest in developing and instituting protection against cyber-attacks by designing and operating systems to combat cyber incidents. Australia's regulatory approach can support and reinforce these self-regulatory approaches while co-regulating to support more robust international law efforts. These twin efforts can have important practical and signalling effects not only for how other States deal with maritime cybersecurity, but also for other industries grappling with how to manage cyber risk.

[19] Ibid,75.

[20] See generally, Lee A Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 8 *Oslo Law Review 126*.