# SHIPPING OF THE FUTURE – CYBERSECURITY ASPECTS FOR AUTONOMOUS AI-DRIVEN SHIPS

Klemens Katterbauer*

*Artificial intelligence has become the centrepiece of the digital revolution, with many transformative technologies becoming game-changers. From automatic facial recognition to self-driving cars, artificial intelligence can be found in almost everyone's daily life. The maritime industry has experienced a considerable increase in the utilization of artificial intelligence in the operations of vessels. While technological changes have happened at ever-increasing speeds, regulatory changes have been slow to adapt to these new environments. The maritime environment is unique in this regard, given the significant importance of international law and the increasing importance of cybersecurity regulations that affect this realm. In this paper, I provide a comprehensive review of maritime regulations applicable to artificial intelligence within Australia, as well as focus on the impact of new Chinese and Australian cybersecurity regulations have on the utilization of artificial intelligence for autonomous or artificial intelligence driven vessels. Furthermore, I will provide specific legal recommendations for how artificial intelligence related regulations can be incorporated into Australian maritime regulations and the challenges that may arise in such context. The recommendations are demonstrated and discussed on recent artificial intelligence adapted Australian maritime legal cases covering both Chinese and Australian cybersecurity provisions. The recommendations in this paper may provide critical insights into the challenges of regulations of artificial intelligence driven vessels for Australia, specifically in relation to cybersecurity regulations.*

## 1. Introduction

Artificial intelligence ('AI') has gained considerable momentum in a variety of different fields, including the maritime industry.[1] AI may enable the introduction of autonomous systems, enhance the efficiency of the current processes and increase safety levels in the maritime space. The maritime industry is of considerable importance for global trade and the movement of both packages and people. Specifically, more than 90 percent of overall traded goods are transported by sea, and this significant trade volume makes the global shipping industry a highly complex area.[2] While the maritime space is of tremendous importance, maritime law is highly complex, consisting of various multilateral and bilateral treaties in addition to national legislation.[3]

Besides the complex web of laws in the maritime area, other challenges arise from the number of different parties that are involved in each shipping operation. As far as the sector is concerned, the shipping industry has heavily relied on people as well as their experience in the past centuries, and current maritime laws are heavily influenced by emphasizing the legal importance of humans commandeering the ships.[4] Advanced technology is already utilized on most ships where ocean cruisers attain the function of floating offices, with real-time communication capabilities in order to enable tracking, enhance operations and maintain communication with shipping companies, logistics providers, and authorities. Furthermore, most ships contain hundreds, or thousands of different sensors spread throughout the vessel that record in real-time crucial information about the ship and its surroundings, which is conventionally transmitted to the central command station as well as the central ship operations area. This implies that cybersecurity and digital data related regulations are increasingly significant when dealing with maritime disputes. Furthermore, ethical and legal concerns related to autonomous ships have arisen in the last several years.[5]

* Associate Professor of Earth Science and Global Management, EUCLID University.

[1] Baris Sayer and Andrew Tettenborn, *New Technologies - Artificial Intelligence and Shipping Law in the 21st Century* (Routledge, 1st ed, 2021).

[2] Karin Gourdon, and Christian Steidl, *Global value chains and the shipbuilding industry* (2019) OECD Publishing.

[3] Matthew Raffety, '"The law is the lord of the sea": Maritime law as Global Maritime history' in Lauren Benton and Nathan Perl-Rosenthal (eds), *A World at Sea: Maritime Practices and Global History* (University of Pennsylvania Press, 2020) 53.

[4] Ibid.

[5] William Stahl, 'The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity' (2011) 40(1) *Georgia Journal of International and Comparative Law* 247.

These new developments open up a variety of opportunities to achieve autonomy and optimization. While one of the first ideas that comes to mind are autonomous ships, there are more readily applicable AI applications. These involve AI-assisted support, such as troubleshooting, automatization of processes of loading and unloading, and the optimization of overall workflows to minimize cost (while achieving high efficiency and safety).

AI is the simulation of human intelligence in machines and go beyond the execution of a specific set of commands. AI allows the machine to learn independently, identify patterns and determine from these patterns actions to be undertaken. Specifically, self-optimization is a major component of modern AI systems that allow the systems to self-correct in order to optimize their actions. Furthermore, data can be processed more accurately and quickly as compared to what humans can process. Therefore, AI has been of great interest to be utilized in a variety of different applications.[6]

AI was first developed in the 1950s. Neural networks have been around for a very long time, and the biggest challenge of early neural networks was that the computational power was not sufficient for large and complex neural networks. Cloud and edge computing, as well as advances in processor speed and performance, have allowed for the training of large and complex AI models efficiently. Machine learning algorithms have experienced wide utilization in order to determine patterns and rules from collected and deliver solutions to the utilizer.

For maritime applications, robust and efficient AI systems require a significant amount of data in order to train the network. The data have to be sufficient in order to capture the possible patterns encountered in reality and react adequately to various environments. This is, for example, the control of a ship's movements in various situations, such as in the context of multiple ships roaming around in the area or a storm affecting the ship.[7]

However, the maritime industry is especially suitable for machine learning algorithms due to the large volumes of data that are generated on a daily basis. Specifically, the shipping documents, information about emission, and the metrics of the operations are recorded in vast numbers in addition to additional data from shipping sensors. These data can be easily utilized in order to optimize shipping performance and automatize the operations. Taking into account the enormous cost associated with many shipping processes, minor optimization may lead to considerable savings. In this competitive industry, even these optimizations may be attractive given the tight margins.[8]

AI may be increasingly utilized on ships in the form of a smart ship. These ships may be fully digitalized and autonomous without a crew. While cost optimization is a key part of utilizing AI in the global maritime industry, safety is a critical component as well in the implementation of AI in shipping.[9] More than 75 percent of the accidents happening at sea are the result of human errors that could be avoided by the use of AI algorithms. The Evergiven's accident in the Suez Canal was primarily caused by human error, failing to take into account the strong winds and dynamics in the waterway.[10]

Given the growing adoption of AI technologies in everyday life, governments have taken notice and realized that existing legal frameworks might not address some of the legal challenges that arise from these new technologies. These involve both regulations addressing the regulatory challenges on sea, as well as data and cybersecurity-related issues that have assumed ever-growing importance.[11]

---

[6] Julian Clark, 'The changing face of maritime law and risk - Cyber, E-Commerce, Automation of Vessels', *ICLG.com* (Web Page, 2020) < https://iclg.com/practice-areas/shipping-laws-and-regulations/1-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels>.

[7] Goh Wai Pheng, 'Steering With Artificial Intelligence To Combat Maritime Piracy', *Hellenic Shipping News* (Web Page, 24 September 2020) <https://www.hellenicshippingnews.com/steering-with-artificial-intelligence-to-combat-maritime-piracy/>.

[8] Henrik Ringborn, Erik Rosaeg, and Trond Solvang, *Autonomous Ships and the Law* (Routledge, 1st ed, 2020).

[9] Ibid.

[10] Jenny Gesley, 'Stuck in the Suez Canal – What are the Legal Implications?', *Library of Congress* (Web Page, 20 April 2021) <https://blogs.loc.gov/law/2021/04/stuck-in-the-suez-canal-what-are-the-legal-implications/>.

[11] James Rundle, 'Maritime Cyber Rules Coming in 2021 Are Outdated, Critics Say', *Wall Street Journal* (Web Page, 18 July 2019) <https://www.wsj.com/articles/maritime-cyber-rules-coming-in-2021-are-outdated-critics-say-11563442201>.

Building upon the first maritime law encoded in the Rhodian Sea Law by the Byzantine empire, one of the major assumptions in the legal framework is that every ship is directed by a crew.[12] While the Rhodian Sea Law of the Byzantine empire became gradually obsolete over time, it heavily influenced early the maritime laws of the medieval Italian cities and further regulations and body of laws until the present.[13] Given the potential deployment of autonomous ships and associated AI technologies in the maritime industry, legal frameworks have to be adapted to address the challenges presented by AI and the growing connection between maritime and cybersecurity regulations.

While AI is primarily connected to information technology and telecommunication regulations, given the fact that these are mostly algorithms and software, other law bodies have to take into account what such autonomous software-based systems imply for their own regulations. In the case of maritime laws, the question arises of how these autonomous or AI assisted systems affect the responsibilities of the crew and operators both on the sea as well as in coast and harbour environments.[14]

While AI-assisted decision making, such as the optimization of routes, is covered by existing frameworks where the person in charge bears the responsibility for the decision making, autonomy may represent a different challenge as the decision making and responsibility is born by the system.[15] When addressing the various scopes of autonomy, the International Maritime Organization ('IMO') has defined four levels of autonomy for maritime environments. The first level of autonomy includes ships with automated processes and decision support. This implies that the seafarers on board the ship both operate and control the systems and functions of the shipboard. However, some operations may be automatized and unsupervised, but the seafarers are ready to take control if needed. The second degree of autonomy is when a ship is controlled and operated from a distance. This implies that the seafarers are available onboard to take control and operate the systems and functions of the shipboard, but the ship is operated remotely.[16] The third-degree level of autonomy is that if a ship is controlled and operated from another location, and no seafarer is on board. The final degree of autonomy refers to fully autonomous ships where the operating system of the ship makes decisions and determines the adequate actions itself. It is crucial to note that autonomous ships do not necessarily have to be unmanned. There are several new initiatives where the ships are autonomous, but the ship is not unmanned but has staff onboard.[17]

The major challenge of existing maritime laws is that they are based on the premise that ships are manned, and the individuals are in control. Additionally, all information about the state of the ship, location, and other relevant data are assumed to be stored locally on the vessel. In 2017, the IMO's Maritime Safety Committee started a scoping exercise on articulating an adequate regulatory framework in order to deal with autonomous ships, both manned and unmanned. While the IMO is looking into these challenges, the focus is solely on IMO instruments and does not address any other impacts, such as those on the UN Convention for the Law of the Sea (**UNCLOS**) that require the duty of any flag state to have adequate manning of the ships.[18] Furthermore, there are several contracts for the carriage of goods by sea, and the agreements on the limitations of liability also impose a duty of the carrier to properly man the ship. This makes this a substantial challenge. Growing cybersecurity awareness and regulations may considerably affect the development of regulations as these have to be taken into account, and Australia has in the last several years considerably extended its cybersecurity requirements that encompass several areas of the maritime industry.[19] China has especially been on the radar of the Australian administrations, given the substantial amount of sea trade that is conducted between the two nations. Specifically, China is the largest trading partner with Australia and also shares considerable sea links with the nation.

[12] Robert Benedict, 'The Historical Position of the Rhodian Law' (1909) 18(4) *The Yale Law Journal* 223.
[13] Wolfgang Graf Vitzthum, *From the Rhodian Sea Law to UNCLOS III* (University of Chicago, 1st ed, 2003).
[14]Henrik Ringborn, Erik Rosaeg, and Trond Solvang, *Autonomous Ships and the Law* (Routledge, 1st ed, 2020).
[15] *Maritime Safety Committee, Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (MASS)*, UN Doc MSC.1/Circ.1638 (3 June 2021) 4.
[16] Ibid.
[17] Ibid.
[18] *Convention on the Law of the Sea*, opened for signature 10 December 1982, 1833 UNTS 397 (entered into force 1 November 1994) Art 94(4)(c).
[19] Shipping Australia, 'Australia tackles infrastructure cyber security' (Web Page, 27 August 2020) <https://www.shippingaustralia.com.au/australia-tackles-infrastructure-cyber-security/>.

In this research article, I will analyse existing Australian maritime and cybersecurity regulations and what impact they have on the deployment of AI driven ships, be it autonomous or solely assisted. I will specifically focus on the case of Chinese ships, be it operated from China or owned by a Chinese enterprise, and what this would imply in terms of regulations. I will address the following research questions: (i) how can cybersecurity be incorporated into maritime law for AI applications?; (ii) what challenges arise from changing cybersecurity regulations in the maritime law environment?; (iii) how can the Australian maritime law support the incorporation of AI for shipping?; and (iv) how can such regulations be applied to potential cases, and what effects do they have?

First, I will provide an overview of the existing regulations and then address the research questions with reference to sample cases and how these regulations would be applied in the context of Australian maritime and cybersecurity regulations.

## 2. Background

Autonomous shipping is amongst the prime examples of how AI may transform the maritime environment. One of the first autonomous ferries that were introduced in 2018 was the Falco, which operated in the waters outside Finland. The ferry measured 50 metres in length and can cover short distances. Furthermore, the operator was monitoring the ferry from around 50 kilometres away during the demonstration of the ferry.[20]

Such types of autonomous ships are limited in terms of their utilization but play an important role for short and monitored shipping trips. There is currently the ongoing development of advanced autonomous ocean-going vessels that may lead to the development of a first ship by 2035. Another project is the Yara Birkeland that is a container ship of 80 meters in order to transport fertilizers on journeys powered by electricity.[21]

The AUTOSHIP project of the European Union is another initiative to develop autonomous ships for short sea shipping and waterways and aims to complete the first prototype by 2023. The Mayflower trimaran ship is an autonomous ship that crossed the Atlantic fully autonomously in 2021. While fully autonomous commercial ships are at the early stage of development, there will be several new autonomous ships sailing the sea.[22]

While fully autonomous ships may still be in the research and development phase, partially autonomous solutions exhibit strong potential to bridge this gap. There have been collision prevention systems for ships that act automatically and autonomously in order to prevent the collision between two different ships. Another key area of how AI can be utilized is to optimize routes given the large volume of data that are available. Specifically, the Orient Overseas Container Line (OOCL) partnered with Microsoft to better predict the arrival times of ships and coordinate more efficiently with the port activities.[23] The cost savings are critical for such attempts to optimize shipping processes. Furthermore, there have been other attempts at utilizing the route across the Arctic Ocean via satellite data in order to ensure that the ships do not get stuck within the icy water.[24]

Another attempt at utilizing thermal and ultra-low light cameras involve utilizing image recognition in busy waterways to avoid collisions. A key part of avoiding collisions is to have a 360 overview and detect potential objects that ships may collide with. These systems may represent an opportunity to reduce collisions and will be key for fully autonomous ships.

Another key part of AI is security. Also, cyberspace has become essential for the autonomous shipping industry. Cybersecurity is a major challenge for many corporations and shipping companies, potentially affecting entire

[20] The Engineer UK, 'Falco makes world's first autonomous ferry crossing' (Web Page, 3 December 2018) <https://www.theengineer.co.uk/falco-autonomous-ferry-rolls-royce/>.
[21] Kongsberg, 'The world's first zero emission, autonomous container feeder' (Web Page, 29 September 2017) <https://www.kongsberg.com/maritime/support/themes/autonomous-ship-project-key-facts-about-yara-birkeland/>.
[22] Andrew Cox, 'China's first autonomous boxship readies to enter service', *Splash* (Web Page, 8 September 2021) < https://splash247.com/chinas-first-autonomous-boxship-readies-to-enter-service/ >; AutoShip, *About* (Web Page, 2021) < https://www.autoship-project.eu/ >.
[23] James Henderson, 'Microsoft partners with OOCL to apply AI in shipping industry', *SupplyChain* (Web Page, 18 May 2020) <https://supplychaindigital.com/technology/microsoft-partners-oocl-apply-ai-shipping-industry>.
[24]Vincent Wee, 'OOCL going all-in on digital with Microsoft', *Seatrade Maritime News* (Web Page, 5 July 2018) <https://www.seatrade-maritime.com/americas/oocl-going-all-digital-microsoft>.

ports and their ships as well as making them potentially inoperable. Cybersecurity is a major area for many AI projects and may also impact energy efficiency in shipping. Optimizing energy consumption overall based on AI algorithms is a major opportunity for many shipping companies to enhance operations and minimize their overall power consumption.[25]

The examples above have outlined the enormous opportunities available for the global maritime industry when it comes to the application of AI within its sphere. There are several challenges that may arise from this. First and foremost, validation and trust are crucial challenges for AI solutions. As compared to autonomous systems in the automotive industry, testing on the sea is considerably more complex and challenging. Most cars are limited in terms of their size as well as the actions they can take. For ships, considerably more challenges arise from determining the number of range of actions and the environments. The first challenge that AI systems face is that testing the applications at sea is far more complex and costly as compared to land-based systems. The chance of a serious accident happening may further considerably aggravate the consequences of such tests. In particular, unexpected situations may arise more frequently at sea and ports, and the ability of ships to react quickly and decisively is hamstrung by the physics of the sea.[26]

Another considerable challenge for AI applied in the maritime industry is data integration and transmission. While communication capabilities at ports and close to the shore are conventionally sufficient for real-time data integration and transmissions, sea transmission is considerably more complex given the fact that the communication is mostly via satellite-based internet. Another challenge arises from the varying jurisdictions in which the data are collected and that a considerable amount of the data will be collected on the open sea, which would represent international waters. Additionally, shipping supply chains are inherently complex and involve several service providers. This requires that all of the parties have to be willing to share their data and utilize common interfaces.[27]

A further challenge is the time required for most of these projects to be tested and evaluated in a sea environment. Specifically, employees need to be trained to operate the AI system as well as deal with situations that may not be well captured by the AI algorithms. From a legal perspective, the final responsibility lies with the shipping operator that has to ensure that the frameworks operate adequately and safely.[28]

## 2.1. AI Within Maritime Law

When considering the impact of autonomous ships and AI on the shipping industry, there have been several recent studies, such as the consideration of an international regulatory framework for unmanned ships by the Comite Maritime International ('CMI'). In order to address these regulatory challenges, they looked at several aspects such as the safety of life at sea, and the prevention of collisions on the sea.[29] The major focus for these regulations is safety at sea rather than any cybersecurity-related challenges which may significantly affect this work. This was extended by the IMO Legal Committee to analyse the nine IMO conventions, focusing on safety, the prevention of collisions, search and rescue as well as special trade passenger ships.[30] When addressing the legal committee's work for maritime autonomous surface ships ('MASS'), the IMO's Maritime Safety Committee provided interim guidelines for MASS trials. While this is an initial step, there are lots of international agreements that need to be adapted in order to enable MASS to stand on sound legal ground.[31]

[25] International Chamber of Shipping, 'Guidelines on Cyber Security Onboard Ships, Version 4' (Web Page, February 2021) < https://www.ics-shipping.org/publication/guidelines-on-cyber-security-onboard-ships-version-four/>.
[26] Oda Loe Fastvold, 'Legal Challenges for Unmanned Ships in International law of the sea', *The Arctic University of Norway* (Web Page, 2018) <https://munin.uit.no/bitstream/handle/10037/16077/thesis.pdf?sequence=1&isAllowed=y>.
[27] Ibid.
[28] Juan Pablo Delgado, 'The Legal Challenges of Unmanned Ships in the Private Maritime Law: What Laws would You Change?' in Massimiliano Musi (ed) *Maritime, Port and Transport Law between Legacies of the Past and Modernization* (Bonomo, 2018) 493.
[29] Comite Maritime International, 'Yearbook 2019 Annuaire', *Yearbooks & Documentation* (Web Page, 2019) < https://comitemaritime.org/publications-documents/cmi-yearbook/>.
[30] International Maritime Organisation, *Maritime Safety Committee, 103rd session (MSC 103)* (Web Page, 2019) <https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-103rd-session.aspx>.
[31] Ibid.

The first major challenge with existing regulations is the function that the master and crew have on an autonomous ship. Specifically, is there a requirement for them to be onboard, and who can this master be? The United Nations Convention on the Law of the Sea requires flag states to conform to several duties, such as ensuring that all ships have a master and officer that possesses the appropriate qualification. Furthermore, the crew shall have adequate qualifications, as well as be in acceptable number for the type of ship.[32] The number depends both on the size as well as the machinery and equipment of the ship. However, these conventions have powers that have to be regarded within the context of national law. Questions arise about how the remote control or autonomous control of ships would satisfy this requirement in terms of acceptable qualification. [33]

For example, Australia was open-minded in terms of considering the onshore remote controller to be the ship's master in terms of Australian law, even though there are uncertainties associated with it. The national law states that the master of the vessel refers to a person that commands or is in charge of the vessel but does not imply that it is a pilot.[34]

The uncertainty arises from the definition of whether "command or charge of the vessel" requires the presence of the master onboard (see *Navigation Act 2021* (Cth) s 14). However, remote controllers cannot constitute the "crew" of the remote-controlled vessel, as the national law requires the "crew" to be individuals that are onboard the vessel other than the master of the vessel or pilot. Unless modified, this implies that, in Australia, the crew has to be onboard.[35]

The first challenge that arises for the IMO Instruments refers to the International Regulations for the Prevention of Collisions at Sea.[36] Rule 2a states that the owner, master, or the crew of the vessel cannot request exoneration of the consequences of neglect on their side.[37] Furthermore, they need to exhibit sufficient precaution based on the circumstances. The obvious question that arises is whether the vessel itself can take on responsibility and who is the master of an autonomous ship. For example, does the maintenance crew, which are not seafarers, have to take on the responsibility for the mistakes of the AI algorithm, or is the provider of the AI algorithm responsible for any accidents.

Another part is Rule 3 that defines "in sight" and raises the question whether a camera and computer counts as "visual" or "sight". Furthermore, can just observing the situation from a distance via cameras be considered as proper observation.[38]

There are additional challenges that arise from the requirement that ships are sufficiently maned and also have a permanent watch. Furthermore, the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers permits officers to be a sole lookout during daylight hours under specific conditions. However, SOLAS regulation 10 requires that the crew has to be sufficiently staffed such that survival craft and launching arrangements can be ensured. Furthermore, SOLAS has the requirement for the masters of the ship to report dangers during the navigation, and both UNCLOS and SOLAS require the master of the ship to provide assistance for those in distress at sea.[39]

Remote-controlled vessels can be currently controlled from anywhere in the world with modern communication infrastructure, similar to what drone technology has demonstrated to allow to enter combat while the operator is far away. The question arises in this context which national laws apply if, for example, an Australian operator

[32] *Convention on the Law of the Sea*, opened for signature 10 December 1982, 1833 UNTS 397 (entered into force 1 November 1994) Art 94(4)(c).
[33] International Maritime Organisation, *Maritime Safety Committee, 103rd session (MSC 103)* (Web Page, 2019) <https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-103rd-session.aspx>.
[34] Australian Government, 'Autonomous Vessels Australia', *Australian Maritime Safety Authority* (Web Page, 4 January 2021) <https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/autonomous-vessels-australia>.
[35] *Navigation Act 2012* (Cth) s 14.
[36] *International Regulations for the Prevention of Collisions at Sea (COLREGS)*, concluded 20 October 1972, 1050 UNTS 16 (entered into force 15 July 1977.
[37] Ibid.
[38] Ibid.
[39] Ibid.

hands over a Panamanian-flagged ship to an operator in China or India and is then one of these operators the master in the context of the rules related to autonomous and AI-driven ships.

## 2.2. Australian Maritime Law and Cybersecurity Regulations

The Australian maritime law is fragmented into several pieces of separate legislation but builds upon the federal structure of the Commonwealth of Australia.[40] The Commonwealth of Australia consists of six states and two territories that have independent legislatures and court systems. The High Court of Australia is the senior appellate court, but every state or territory has their own Supreme Court. Appeals may be referred to them from a Court of Appeal or Full Court, or a Federal Court. The Federal Courts play a critical role as the first instance jurisdiction, where both admiralty and other specialized jurisdictions are taken care of. The Supreme Court has likewise admiralty jurisdiction.[41] In order to expand the Arrest Convention 1952, the *Admiralty Act 1988* (Cth) was introduced that enhanced admiralty regulations, giving admiralty jurisdiction to the State Supreme Courts in addition to the Federal Courts. The *Admiralty Act 1988* (Cth) defines the jurisdiction of the Commonwealth of Australia in terms of the ports and territorial waters.[42] Furthermore, it specifically defines the boundaries with international waters. This permits the arrest of ships and other properties for the enforcement of arbitration awards.[43] The Australian courts have the authority to make judgements within the boundaries of the Australian Territorial Waters. A crucial part is also the *Australian Maritime Safety Authority Act 1990* (Cth) that regulates the safety of shipping in Australian waters.[44] Furthermore, the *Carriage of Goods by Sea Act 1991* (Cth) regulates ships that load and unload at any of the Australian ports and also specifies what cargo can be carried.[45]

Another critical piece of law is the *Crimes Act 1992* (Cth) that creates a criminal jurisdiction for specific acts at sea. Additionally, the *Customs Act 1901* (Cth) enables customs authorities to board and inspect shipping and also arrest individuals that are suspected of trafficking illegal weapons, drugs, and other contrabands. Another important act is the *Limitation on Liability of Maritime Claims Act 1989* (Cth) that limits the maximum liability that may be incurred.[46]

When addressing cybersecurity law aspects, then there are several critical regulations that have to be taken into account, such as the *Privacy Act 1988* (Cth), *Crimes Act 1914* (Cth), the *Security of Critical Infrastructure Act 2018* (Cth), and the *Telecommunications Act 1979* (Cth). Amongst these, the *Security of Critical Infrastructure Act 2018* (Cth) the most crucial one. This Act addresses security risks related to sabotage, espionage, and coercion by foreign powers.[47] Specifically, the increased connectivity of critical infrastructure was taken as the common core threat that also included besides assets in the electricity, gas, and water sector, also assets in the ports area.

While the *Crimes Act 1914* (Cth) incorporates several provisions, such as outlining that several offences have to be "committed" and not "attempted" for them to be considered a crime.[48] Specifically, a person themselves cannot just attempt to commit unauthorized access, modification, or impairment with the intent to commit a serious offense but needs to have actually committed it.[49]

---

[40] See *Australian Constitution*, Preamble; Geoffrey Sawer, *Australian Federalism in the Courts* (Melbourne University Press, 1st ed, 1968).
[41] Geoffrey Sawer, *Australian Federalism in the Courts* (Melbourne University Press, 1st ed, 1968).
[42] *Admiralty Act 1988* (Cth); Federal Court of Australia, 'Admiralty Jurisdiction of the Federal Court' (Web Page, 4 October 2021) <https://www.fedcourt.gov.au/law-and-practice/national-practice-areas/admiralty/jurisdiction>.
[43] Ibid.
[44] Australian Government, 'National Maritime Safety Authority', *Australian Maritime Safety Authority* (Web Page, 4 October 2021) <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/maritime/maritime-safety/national-maritime-safety-authority>.
[45] Geoff Farnsworth and Nathan Cecil, 'In brief: carriage of goods by sea in Australia', *Lexology* (Web Page, 1 August 2019) <https://www.lexology.com/library/detail.aspx?g=c96d0df6-9d43-4d12-91c5-c1a49872a0e7>.
[46] Australian Government, 'General Maritime Claims', *Australian Maritime Safety Authority* (Web Page, 4 October 2021) <https://www.infrastructure.gov.au/infrastructure-transport-vehicles/maritime/maritime-business/maritime-liability-insurance/general-maritime-claims>.
[47] Department of Home Affairs, 'Security of Critical Infrastructure Act 2018' (Web Page, 4 October 2021) <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018>.
[48] Dennis Miralis, Philipp Gibson and Jasmina Ceic, 'Australia: Cybersecurity Laws and Regulations', *ICGL.com* (Web Page, nd) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia>.
[49] *Crimes Act 1914* (Cth) s 3ZA.

Another key area for autonomous shipping is the growing communication capabilities of autonomous vessels to communicate with their base station primarily via satellite data communication. Currently, there are no specific regulations in Australia addressing the distribution of satellite remotely sensed data.[50] The legal challenge that arises from this context is that the regulator has to decide on a case-by-case basis whether the data transmission and communication of data from vessels in the jurisdiction of Australia is permitted.[51]

The importance of port infrastructure and growing interconnectedness that is also driven by AI makes this an especially critical asset area for any maritime shipping operator to take notice of. As outlined in the *Security of Critical Infrastructure Act 2018* (Cth), the government needs to get access to the information related to these assets, and such information has to be provided by the asset owner, in addition, to also control information.[52] Since the register is not publicly available, this represents from an implementation point of view an information gap between the port operator and shipping companies.

## 2.3. Chinese Maritime Law and Cybersecurity Regulations

China has in recent years experienced a growing transformation and strengthening of its cybersecurity and information technology sector. The Data Security Law of the People's Republic of China (**Data Security Law**), passed in 2021, strengthened the protection regime considerably for the digital economy and also stipulates clear rules on how the data are collected, developed, and protected in China.[53] When relating to AI for the maritime industry, several key provisions in the new data security law are of importance. The first key provisions are the cross-border data transfer requirements. The management of cross-border data transfer is stipulated in Article 31 and Article 36. Article 31 states that data from critical information infrastructure operators are governed by the Cybersecurity Law, which requires that the data are to be stored within the territory of the people's Republic of China.[54] For any overseas transfer, a security assessment has to be implemented.

Whether data are considered important is dependent on the data classification and protection catalogues that are provided by the regions and departments, leaving sufficient ambiguity in terms of which data are considered critical. In terms of what critical information infrastructure is, this refers to industries in sectors, such transport, and water, as well as ports and shipping industry. With respect to AI assisted or autonomous ships, these ships are most likely to be classified as critical infrastructure.

This also implies that the security review measures have to adhere to the requirements by the state cyberspace administration. This represents a challenge as these specific rules on general data are currently not available and specified. The arising ambiguity and lack of clarity are challenging for the maritime industry to determine how data from autonomous or AI driven ships are to be handled and how they can be shared with port operators in another's jurisdiction.

However, the potential fines for violations of Article 59 and transfer the data illegally abroad are steep and range from 100,000 CNY to 1 million CNY.[55] In serious circumstances, the fines may range from 1 million CNY to 10 million CNY, and the business may even be requested to stop its business.[56] This implies that a shipping company may be suspended from operating if it violates the data transfer.

Companies such as Tesla have faced such dilemmas with their cars, as the collected information was deemed as potentially posing a security threat. The regulations make cybersecurity audits a critical part for any shipping

[50] Ram Jakhu, *National Regulation of Space Activities* (Springer, 5th ed, 2010).
[51] Australian Navigational Guide Explaining Laws for Space, 'Laws Applicable to Remote Sensing Activities', *ANGELS* (8 October 2021) <https://spacelaws.com/articles/laws-applicable-to-remote-sensing-activities/>.
[52] *Security of Critical Infrastructure Act 2018* (Cth) Div 3.
[53] Hui Xu and Kieran Donovan, 'China's New Data Security Law: What to Know', *Latham & Watkins* (Web Page, 21 July 2021) <https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to-know>.
[54] Clarice Yue and Michelle Chan, 'Are you ready? PRC Data Security Law was Passed and will Come into Effect on 1 September 2021!', *Bird & Bird* (Web Page, 1 June 2021) <https://www.twobirds.com/en/news/articles/2021/china/prc-data-security-law-was-passed-and-will-come-into-effect-on-1-september-2021>.
[55] *Data Security Law of the People's Republic of China* (China) People's Republic of China, Order No 84, 1 September 2021, Art 59.
[56] Ibid.

operator and an operator will have to address in greater detail the potential cybersecurity risks that arise from their AI and data-driven solutions utilized for shipping.[57]

Article 36 of the Data Security Law makes it also clear that there are requirements to be fulfilled when the data are provided to judicial and law enforcement authorities outside of China. Specifically, the organizations and individuals have to obtain approval from the respective authorities before handing any data over to the foreign authorities. Additionally, any international treaties and agreements shall act as guidance for the authorities to deal with these data.[58]

A challenge that may be experienced by the shipping industry are the requirements of data intermediary service providers. Specifically, autonomous or AI assisted ships may be controlled by specialized service providers that may support the data transmission as well as the acquisition of data. Such data intermediary service providers may be satellite internet companies, in addition to specialized ship operation providers. Furthermore, there may be shipping intermediary companies that utilize AI in order to optimize the assignment of cargo to various ships and optimize their overall fleet management and allocation.

For such applications, the Data Security Law has specific requirements in Article 33 that stipulates that the data provider has to explain the data source, check the identity of the parties to the transaction, and also that the examination and transaction records have to be maintained. This represents a critical part that has to be taken into account when the data are collected and utilized.[59]

While the Data Security Law has been recently implemented, the law has a strong relationship with the Cybersecurity Law of the People's Republic of China that was implemented in 2017. The Data Security Law has at its core the security of data and IT infrastructure and incorporated the requirement that companies operating in China store their data in China as well as implement respective measures against cybersecurity and data theft.[60] Furthermore, it also focuses on data sharing and the security reviews that have to be conducted for foreign data sharing.

Overall, these regulations provide solely a supervisory overview and general guidelines rather than specific implementations, which will make it interesting how they will be applied in reality.

I will focus on the Australian maritime law related to AI, as well as analyse the impact various IT and cybersecurity regulations have on the application of AI within the shipping industry. I will analyse a specific example of a Chinese ship, both AI assisted and autonomous, with respect to its impact on the hosting of collected data as well as remote control of it in Australian waters. I will subsequently outline potential regulatory approaches and implementation forms to enable the application of AI in such circumstances. A critical part of the recommendations will be addressing potential cybersecurity challenges and how these can be adequately addressed.

## 3. Regulation Opportunities and Challenges Of AI-Driven Chinese Shipping Operators in Australian Waters

I will analyse several example maritime law dispute cases that are adapted based on historical cases and judgments. The first sample case is based on the case *Orient Overseas Container Line Ltd v APL Co Pte Ltd*, where the MV APL England lost containers overboard close to the coast of New South Wales.[61] Further, a considerable number of containers onboard the ship were damaged. The investigation concluded that the lashing

[57] Eamon Barrett, 'Tesla changes its China data policy after government scrutiny', *Fortune* (Web Page, 26 May 2021) <https://fortune.com/2021/05/26/tesla-china-data-policy-storage-sharing/>.
[58] Jones Day, 'China's New Data Security Law Restricts Cross-Border Transfers of All Data to Foreign Authorities' (Web Page, 1 August 2021) <https://www.jonesday.com/en/insights/2021/08/chinas-new-data-security-law-restricts-crossborder-transfers-of-data>.
[59] Kasawna Campbell and Karan Chao, 'China: Data Security Law overview', *Data Guidance* (Web Page, 1 September 2021) <https://www.dataguidance.com/opinion/china-data-security-law-overview>.
[60] Rogier Creemers, Graham Webster and Paul Triolo, 'Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' *Stanford University* (Web Page, 29 June 2018) < https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>, Art 1-2.
[61] *Orient Overseas Container Line Ltd v APL Co Pte Ltd (No 2)* [2021] FCA 606.

arrangements for the cargo were improper and also heavily corroded. The vessel owners failed to have the cargo properly loaded, handled, stowed, carried, and kept. The vessel owners were therefore found to have contravened Article 3(1)(c) and (2) of the Amended Hague Rules.[62] I will analyse several various cases where the ship incorporates various AI technologies, including being an autonomous ship, and the ship's owner is either incorporated in China or has its data operations there. In the case that the ship is autonomous, the ship would have to steer autonomously through the sea. The ship lost its propulsion and power during high seas, which led to an overall power outage.[63] Typically, the AI driven steering and control system have power backups that keep the software and control system up and running even in the case of a general power outage. In case the AI operated system fails overall, then this would imply that the ship is inoperable. While a force majeure defence may be applicable, this will be, in most circumstances, rather unlikely. Hence, the ship operator will be charged with neglect of due diligence to implement measures such as power backup to maintain basic operation functionalities.

Modern AI driven ships incorporate a variety of different sensors that also encompass checking at frequent intervals the integrity of pipes and the machinery during transportation. In the above-mentioned test instance, this would lead to the frequent recording of sensor data by the ship and indicate a possible breakdown. Furthermore, most autonomous ships are permanently monitored, which would allow them to detect via image driven AI possible breakdowns and issues. Furthermore, the image information may also be used in court cases in order to outline due diligence.

When it comes to data recording, several legal challenges arise. Both the Australian and Chinese cybersecurity regulations require the storage of data within their boundaries and have a cybersecurity assessment for the transfer of data outside the jurisdiction. Specifically, most autonomous ships have frequent sensing and image recordings that are particularly relevant during docking operations in ports.

Therefore, the existing regulations would not permit automatic recording and storage of this information outside of Australia without a security assessment and permission.

There has recently been an important case regarding how ships are defined in the Admiralty Act 1988. While this is uncontroversial for conventional ships, remotely controlled vehicles may not have some of the common attributes of ships. In *Guardian Offshore AU PTY LTD V SAAB Seaeye Leopard 1702 Remotely Operated Vehicle* [2020] FCA 273,[64] the Federal Court of Australia judged that an ROV is not a ship.[65] One fundamental question that arose is whether the element of 'used in navigation' requires that people or property needs to be transported, or not, in order to consider a vessel a 'ship', which has been widely rejected given that it would exclude floating cranes or deep-water mining vessels. The main decision arose from determining the features of this ROV as compared to a ship. The ROV is small, is not buoyant on water, and also travelled on board another ship. Additionally, the ROV is not able to navigate open waters as well as leave the jurisdiction on its own.

There are several aspects that have to be taken into account when aiming to generalize the ruling to other remotely operated vehicles. The parameter of leaving a jurisdiction on its own is easily resolved with modern autonomous ships. Whether a vessel is considered a 'ship' depends on the quality of artificial intelligence, whose threshold has been left unanswered. While the decision on what constitutes a 'ship' will be furthermore precisely defined in the context of shipping, the critical question is to determine the impact of how cybersecurity regulations will be applied depending on whether a vessel is a 'ship' or not. While both vessels may be autonomously or remotely controlled, questions arise in terms of whether there will be any distinction in how these two different forms of the vessel will be treated under cybersecurity regulations.

[62] Maurice Lynch, 'MV "APL England" loses containers overboard, again. Protect your rights in cargo interests', *Mills Oakley* (Web Page, 1 May 2020) <https://www.millsoakley.com.au/thinking/mv-apl-england-loses-containers-overboard-again-protect-your-rights-in-cargo-interests/>.
[63] The Maritime Executive, 'Video: APL England Loses Containers Overboard Near Australia' (Web Page, 25 May 2020) <https://www.maritime-executive.com/article/video-apl-england-loses-containers-overboard-near-australia>.
[64] *Guardian Offshore AU Pty Ltd v Saab Seaeye Leopard 1702 Remotely Operated Vehicle Lately On Board The Ship 'Offshore Guardian'* [2020] FCA 273.
[65] Alan JS de Rochefort-Reynolds, 'Finding the 'Ship': Guardian Offshore AU PTY LTD V SAAB Seaeye Leopard 1702 Remotely Operated Vehicle [2020] FCA 273' (2020) 34 A&NZ Mar LJ 50.

While most ships will be utilized for cargo and passenger transportation and will most likely dock in Australian ports, ROV such as submersibles may be utilized for exploration, military, and other operations. Therefore, the criticality of these data for these AI solutions, as well as their impact, may have to differ.

The final case that will be analysed is the case *Australian Maritime Safety Authority v Globex Shipping S.A.* [2018] FCA 1477.[66] In this case, the MV Regina is alleged to have caused an oil spill off the coast of North Queensland. In the case of environmental catastrophes, the question arises for autonomous and AI driven ships of how these data can be utilized for the prevention, as well as tracking of the oil spill.

With respect to oil spills by autonomous ships, several sensors would detect an abnormal loss of oil by the ships and would record this abnormality, as well as indicate remedial measures such as informing the emergency services. In case the ship's data are stored in China, the first legal question would arise whether such data are considered relevant to national security. A distinction needs to be drawn between the different types of vessels. For military vessels or other state-owned vessels, any such data recorded would be considered confidential, and since this information is stored within the jurisdiction of the People's Republic of China, data transfer outside China will be very unlikely to be permitted by the authorities. For other commercial vessels, the master of the vessel has to request from the authorities the transfer of the data abroad. This may again depend on whether such spill data may be considered critical or of importance and how local authorities observe such data.

The three analysed cases demonstrate the importance of cybersecurity regulations for maritime law when it comes to the increasing number of autonomous and artificial intelligence driven vessels. This implies that the Australian maritime law, specifically the *Admiralty Act 1988* (Cth), has to incorporate provisions that specify the requirements of data storage and location as well as who is the master on an autonomous ship. Specifically, the jurisdiction has to incorporate also the cyberspace and data recorded and collected on such vessels. This would ensure clarity and make the *Admiralty Act 1988* (Cth) a single point of reference when it comes to jurisdictional questions.

A key aspect is the stronger linkage between the *Cybercrime Act 2001* (Cth) and *Admiralty Act 1988* (Cth). Specifically, accidents at sea may involve components of cybercrime where there may be a party that hijacks the controls of the ship, causing an accident on purpose.

The challenges from such a strong interlinkage are that the concept of master onboard and the primary assumption in the maritime law that the master of the ship is able to manually control the vessel may be unfounded and inadequate for the maritime law environment. Furthermore, existing cybersecurity regulations are strongly dependent on national jurisdiction, and questions arise about how these regulations may be applied in the international maritime space. This requires that the data collected on ships have to be addressed in terms of under which jurisdiction they fall and whether the jurisdiction can be expanded or adapted to cover these ships.

The major challenge from such an approach is that data communication on sea is via satellite-based communication that faces its own considerable legal challenges when it comes to requesting jurisdiction over the transfer and collection of data.[67] While satellite communication on land is covered by the specific jurisdiction of the nation where the receiving person is located and the satellite that services it, maritime data communication represents a grey zone where the data communication is in international waters. Given that the Chinese cybersecurity law requires any Chinese company to enforce Chinese cybersecurity regulations within its domestic jurisdiction and support the Chinese government in a foreign jurisdiction, AI driven or autonomous ships will face challenges between the overlap of jurisdiction and data transfer of AI driven or autonomous ships. For Australia, this also implies that without any dedicated legislation on remote-sensing data communication, each case has to be decided on a case-by-case basis. This represents a considerable uncertainty for operators as it requires for each case an assessment, mostly taking into account national security concerns.

[66] *Australian Maritime Safety Authority v Globex Shipping S.A.* [2018] FCA 1477.
[67] Frans von der Dunk, 'Legal Aspects of Satellite Communications — A Mini Handbook' (2015) 4 *Journal of Telecommunication and Broadcasting Law* 1.

A potential solution would be to make the ship totally autonomous and not provide data communication when on sea. This would make such vessels totally autonomous and offline, allowing to avoid any data transfer when being in different jurisdictions. Practically however, this would be rather challenging given that the strength of AI driven solutions is the data connection and integration of various data forms (weather, position of other ships, port traffic, etc.).

## 4. Conclusion

The maritime industry has undergone a significant transformation with growth in AI in various industries. Autonomous cars have become commonplace in many jurisdictions challenging traditional laws that assume that these cars are steered by a human being and are disconnected from other systems. Similar advances have been experienced in the maritime industry, where autonomous ships are currently in development. Likewise, maritime law has been slow to adapt to these technological changes, in addition to the growing interaction between cybersecurity regulations and maritime law. This paper addresses the challenge of adapting maritime law to AI driven vessels in an Australian legal context and demonstrates the application of both maritime and cybersecurity regulations on cases involving China and Australia. Given the significant relevance of such cases in the maritime law environment for Australia and the significantly changing cybersecurity regulations in both nations, this provides a comprehensive overview of how such legal cases may be dealt with under current regulations. Furthermore, the article provides recommendations towards the adaptation of Australian maritime regulations, specifically the incorporation of cybersecurity aspects into maritime laws.