Callidus News

ADVOCATES, CONSULTANTS & NOTARY

BRANCHES : DUBAI | SINGAPORE | DELHI | MUMBAI | KOLKATA | CHENNAI | COCHIN info@calliduscmc.com

Dubai
Business Avenue Building
Office # 713,Port Saeed Road,
P.O. Box # 90992, Dubai, UAE.
Tel : +97142956664
Fax : +97142956099

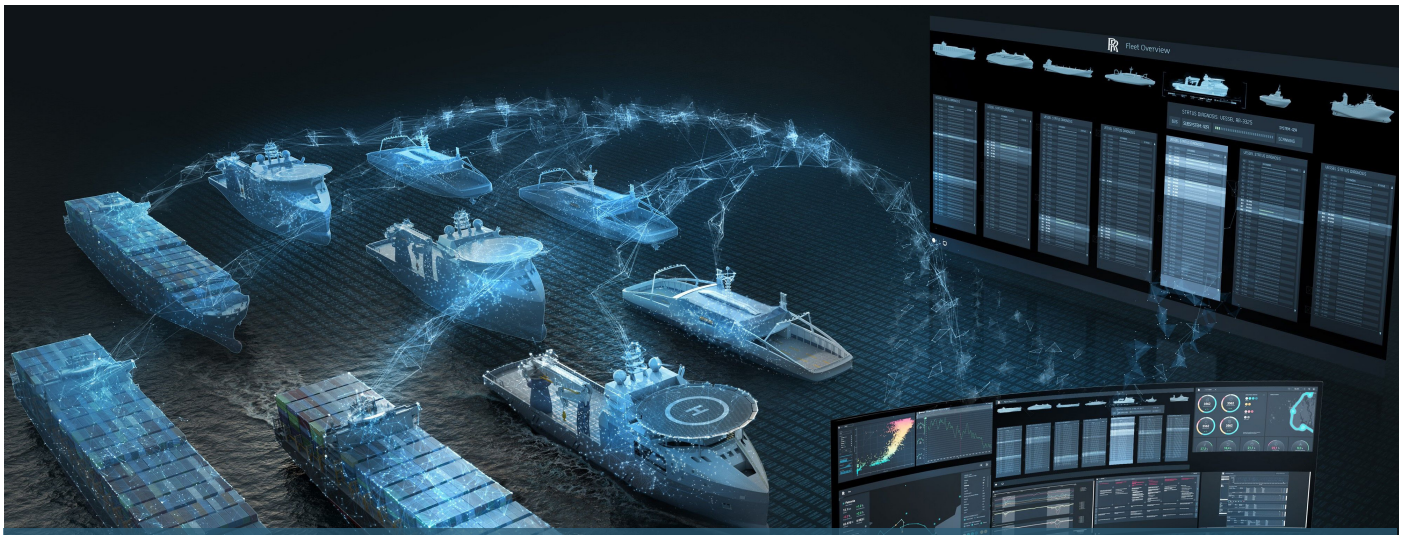
Singapore
20 Maxwell Road
#04-02 D, Maxwell House
Singapore - 069113
Tel: +65 6221 4090

Delhi
D 1st 145 Basement (Rear)
Lajpat Nagar R 1
New Delhi - 110 024
Tel: +91 11 4132 1037

Mumbai
8-B, Dariya Building
2nd Floor, In between American
Dry Fruits & Zara, Dr. D.N.Road
Fort, Mumbai 400 001
Tel: 022-22853371

Chennai
Old No. 123, New No.255,
3rd Floor, Hussiana Manzil,
Ankapanaiken Street,
Parrys, Chennai - 600 001
Tel: +91 98 40 844463

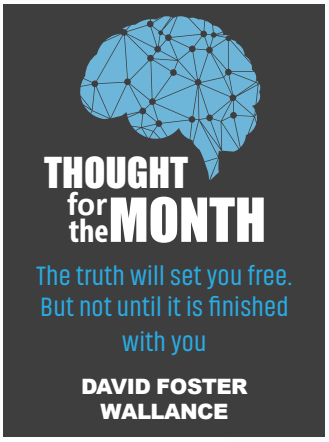
Cochin
Near St.Joseph's High
School Chittoor Road,
Cochin - 12, India
Tel : +91 484 2391895
office@callidusindia.com



NAVIGATING JURISDICTIONAL WATERS: THE COMPLEXITIES OF CYBERSECURITY IN MARITIME LAW

Archisha Warrier,
Jindal Global Law School, Sonipat, Haryana

Navigating uncharted waters is a gamut of strange elements intermingling together. With the advent of technological innovations came a completely strange world. This strange world intermixed with the uncharted waters and the laws that govern them posited a world of danger that needed to adapt to this constant change. Cybersecurity is commonly defined as "the protection of cyberspace as well as individuals and organizations that function within cyberspace and their assets in that space" also re-defined cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure de facto property rights". In the aspect of maritime cyber risk, it has been defined as 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. Cyber-attack incidents have



Callidus

resulted in unquantifiable losses of monetary assets, intellectual property, and customer confidence.

Ships are becoming much more environmentally friendly and operating more efficiently owing to new digital technology. More and more digital technologies are being used in communication, logistics, and navigation, which increases energy efficiency and lowers emissions.

The risk posed by cyber security threats in maritime law has increased over the years because of this rapid evolution of technology. While technology in a holistic sense has been a boon for the maritime industry with the digitalization of ships and infrastructure, it comes with this imminent danger.

Digital technologies are advancing at a quick pace, and with them are the potentially harmful systems. Shipping is a popular target for cyberattacks due to its critical role in global supply networks and the threat it poses from state-sponsored actors and cybercriminals. Traditionally, risk management has been limited to the physical domain but, with the advanced pace of growth of cyber threats in recent times, maritime laws must incorporate uniform guidelines and strategies for implementing cohesive cybersecurity risk management.

Because IT and OT systems are so intricately operationalized, cyber threats to the maritime industry have become more serious. Malware, phishing, man-in-the-middle, and ransomware are all potential threats to these systems. Such attacks may be motivated by a variety of non-state objectives, including hacktivism and cyberterrorism, as well as more conventional purposes like espionage and naval warfare.

I. RECENT EVENTS

Recent events have brought the issue of cybersecurity in maritime law into the limelight. In 2011, at the Port of Antwerp, hackers remotely accessed the Port's network to identify containers in which they had hidden illegal goods, and removed the goods before they were searched by authorities. The source of this hack was a Trojans that were sent to the Port's staff. What is even more interesting is that this criminal activity allegedly went on for two years.

In June 2017, A.P. Moller-Maersk fell victim to a major cyber-attack by a malware- NotPetya. It caused huge problems for the world's biggest carrier of seaborne freight. Its operations in transport and logistics were disrupted. Maersk's container ships stood still at sea and its 76 port terminals around the world ground to a halt. It took almost three weeks for the company to recover, and the organization suffered financial losses of up to USD300m covering, among other things, loss of revenue, IT restoration costs and extraordinary costs related to operations. The aftermath of this event led the company to incorporate stringent guidelines and drills for managing maritime cyber risks.

DP World Australia was targeted by an unauthorized access to the company's Australian corporate network. It led to the suspension of port operations for about three days impacting 40% of goods flowing in and out of the country.

II. REGULATIONS

Until relatively recently, the phrase 'maritime cyber security' was not recognized globally. A 2011 study on maritime cybersecurity by the European Network and Information Security Agency (ENISA) stated that, at present there is no common definition of 'cybersecurity' shared among the various nations at the EU or at international levels. It is only very recently that international guidelines for maritime cyber risk have come into the picture.

The International Maritime Organization (IMO) in April 2017, introduced guidelines for high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. Through the International Safety Management (ISM) Code and the International Ship and Port Facility Security (ISPS) Code, IMO has tried to address the need for proper guidelines and the increasing need for a maritime cyber security management system.

The International Association of Classification Societies (IACS) has posited new unified requirements (URs) for cyber security which is to take effect from 1st July 2024. It puts forth an obligation on the owners, yards, and suppliers to build cyber security barriers into their systems and vessels, requiring compliance across the full spectrum of critical on-board control and navigation systems.

Cybersecurity rules and regulations tailored to regional marine environments have been produced by regional bodies and coalitions, including the ASEAN Regional Forum (ARF) and the European Union's Network and Information Security Directive (NIS Directive). EU Directive on Network and Information Systems (NIS2) is also set to be implemented from October 2024 focusing on obliging EU states to adopt cyber security strategies and establish competent cyber security structures across their jurisdictions. Several other regions have national-level guidelines for minimizing this threat.

There are certain Industry Standards and best practices such as the Baltic and International Maritime Council (BIMCO) which provides detailed guidelines for cyber risk management on board ships, covering areas such as risk assessment, protection measures, and incident response.

III. UNCHARTED WATERS AND JURISDICTIONAL PROBLEMS: LEGAL IMPLICATIONS

A major lacuna with the regulations pertaining to maritime cyber risk is the obscureness that it exhumes. The global nature of marine cyber threats gives rise to jurisdictional complications, which make it challenging to identify the legal jurisdiction that oversees cyberattacks in international waters or the high

seas. The complexity of initiating and prosecuting legal measures stems from the existence of conflicting national laws, differences in regulatory frameworks, and challenges in attributing cyberattacks to specific individuals or locations.

International law determines jurisdiction to prescribe crimes by assessing five core principles of the territory affected, the law of the offender's country, the law of the nation affected, the law of the country with protected rights, and the law of the global community recognized through universal jurisdiction.

The complex nature of attributable legal regimes over the waters makes it even more pertinent to have a uniform set of regulations that extends to all.

1. Flag State Jurisdiction

Flag states, which are the countries by whose laws a ship is governed, primarily exercise jurisdiction over ships. As per international maritime laws, it is the flag state's responsibility to make sure that their ships conform with both global and national standards. Yet enforcement of cybersecurity norms and dealing with cyber incidents remain difficult. Many flag states lack adequate resources or knowledge to manage cybersecurity initiatives well while regulations in different nations are stringent to varying degrees.

2. Coastal State Jurisdiction

Coastal states have jurisdiction over maritime activities within their territorial waters and exclusive economic zones (EEZs). These states can enforce regulations concerning port security, including cybersecurity measures for ships entering their ports. However, the enforcement of such regulations can be inconsistent, and jurisdictional overlap with flag states can lead to conflicts or gaps in enforcement.

3. Port State Control

Port states, where ships dock and conduct cargo operations, also play a critical role in maritime cybersecurity. Port state control (PSC) authorities can inspect foreign ships to ensure compliance with international regulations, including those related to cybersecurity. Nevertheless, the effectiveness of PSC varies widely, and not all countries have incorporated comprehensive cybersecurity checks into their PSC regimes.

IV. THE INDIAN SCENARIO

The maritime cyber threat is an emerging concern for India. India still hasn't put forth any solid plans to navigate or regulate this uncharted terrain. India needs to introduce legislation and guidelines to protect its maritime industry from this evil. Under its Amrit Kaal Vision 2047 and Maritime India Vision (MIV) 2030, India hopes to create mega ports, contemporary port infrastructure, and transshipment hubs. More automation as well as improved facilities and management systems would be needed for this. Consequently, increased cyberattack susceptibility of India's marine critical infrastructure would result from increased interconnection with internet networks. Moreover, with the "Sagar" project, India must aim to have robust laws.

More adversarial cyberattacks will target Indian ports and the marine sector as geopolitical tensions rise. This is especially true with initiatives like the India-Middle East-Europe Economic Corridor that could jeopardize established trade routes. India's JNPT was the victim of a cyberattack in 2022 that rendered its automated system unusable and made it switch back to offline operations, revealing the system's inadequacies.

More reliable, safe, and secure digital systems at India's ports are needed to further improve the country's logistics performance in the category of foreign shipments. Sagar-Setu is one such tracking tool designed to make business easier. India needs to create a thorough policy for its marine domain to handle this.

V. CONCLUSION

Maritime cyber security is an emerging concern that must be addressed globally. Uniform regulations must be brought about to minimize the jurisdictional problems that have surfaced. It is imperative to prioritize bringing about sustainable and long-term plans to mitigate the loss suffered by such attacks. India, especially, should prioritize on implementing nation-wide goals and guidelines to ensure that this threat does not overpower the maritime industry. Finally, companies should inculcate maritime cyber risk management plans to mitigate any loss that they may face due to such an attack. Moreover, companies should revise these plans to move forward with the digital age ■

DELIVERY OF CARGO WITHOUT ORIGINAL BILL OF LADING: THE RIGHT OF THE BANK TO SUE THE CARRIER

In UniCredit Bank AG vs Euronav NV [2022] EWHC 957 (Comm) (The Sienna), the Claimant (The Bank), brought a claim for damages against Euronav NV, the registered owner of the Vessel MT Sienna ("The Vessel') for an alleged breach of the Bill of Lading contract in delivering part of a cargo of LSFO to a third party without the production of the Bills of Lading. The claim was for USD 24,701,600/- in damages.

The vessel was originally chartered out to BP Oil International Ltd, who subsequently sold the cargo of LSFO ("the Cargo") to Gulf Petroleum FZC. The Bill of Lading was issued at Rotterdam and signed by or on behalf of the Master of the vessel, and in signing the Bill of Lading, it was acknowledged in it that the cargo on board the vessel was

in apparent good order and condition for carriage for its delivery at Fujairah, UAE. The Bill of Lading was made out to the order of BP or their assigns. By way of a Letter of Credit, the Bank "UniCredit" financed the purchase of part of the cargo of Low Sulpher Fuel Oil (LSFO) by Gulf Petroleum FZC, from BP Oil International Ltd.

The Bank alleges that Euronav delivered the cargo to someone other than the lawful holder of the relevant Bill of Lading or without authorization of the lawful holder of the Bill of Lading. Euronav contends in response that the lawful holder of the Bill of Lading at the time of the discharge of the cargo was either BP or Gulf and that the delivery/discharge was authorized by BP and alternatively Gulf Petroleum. The Bank accepts that it had – vis-à-vis Gulf – authorized delivery of the Cargo to six identified sub-buyers (the "Sub-Buyers", also called the "Off-Takers") on payment terms that required those Sub-Buyers to pay UniCredit directly, 90 days after delivery. However, UniCredit says that the Cargo was discharged from the Vessel - Mt Sienna to two other vessels without production of the Bill of Lading. UniCredit says that it does not know to whom the Cargo was delivered.

In this case, the Court found the Bank's Bill of Lading was not a contract of carriage giving the right to sue, but a mere receipt. The Court mentioned that the Carrier and the BP, who was the previous holder of the Bill of Lading were parties to a charter party for the hire of the ship – so the contractual relationship between them was covered by the charter party and not the Bill of Lading. The Bill of Lading was a mere receipt for the cargo. The charter party by BP was later novated to Gulf Petroleum, another charterer, and the Bill of Lading was later passed to the Bank.

The Court found that the Bill of Lading remained a receipt and not a contract in this claim and therefore the Bank never obtained the right to sue the carrier under it.

Though the judgment by the Court is appealable, this outcome of the case shall alert the financial institutions to consider in each trade whether they have become party to the contract of carriage or whether they are merely been passed a receipt of the goods, before they extend financial help to the Shipper and /or the consignee ■

ADV. JOY THATTIL REPRESENTS AT PRESTIGIOUS WTC EVENT IN THAILAND

Adv. Joy recently had the honor of being invited to the World Top Cargo (WTC) Alliance event held in Thailand. The three-day event was a gathering of influential leaders and professionals from various industries, providing a platform for insightful discussions and networking opportunities. Adv. Joy actively participated, gaining and sharing valuable insights that promise to benefit our community

Address: Near St.Joseph's High School, Chittoor Road, Cochin- 12, India, T:+91 484 2391895, office@callidusindia.com

Disclaimer *The materials contained in our News Letter and our accompanying e-mail have been prepared solely for information purpose. Neither Callidus nor any of its affiliates make any warranties in relation to the use or reproduction of its contents. The information contained in the news letter is solely for academic and discourse purposes, meant for private circulation; this e-mail message and it's attachments may be confidential, subject to legal privilege, or otherwise protected from disclosure, and is intended solely for the use of the intended recipient(s). If you have received this communication in error, please notify the sender immediately and delete all copies in your possession.*