A New Era, a New Risk!

Dr. Julia Constantino Chagas Lessa[1] & Dr. Belma Bulut[2]

Current technological developments have brought the shipping industry into the era of digital shipping. Today, it is possible to monitor and control sea traffic, navigate with automated navigation systems (e.g. GPS - Global Positioning System, AIS - Automatic Identification System), ECDIS -Electronic Chart Display and Information System,), and track the location of ships and cargoes in real time. As shipping technology has been developing at a fast pace, unmanned and autonomous ships, drones as well as smart containers are becoming an ever more feasible reality. Indeed, the industry has never been more technically advanced no only due to the new forms of advanced vessels and offshore unit but throughout the entire shipping logistic chain, from operational offices to port, contractors and commercial partners.

Nevertheless, practical developments often bring new risks attached to them and accordingly the necessity of creating a new regulatory framework to accommodate these. The more sophisticate the industry developments are, the more sophisticate policies seem to be necessary. It is questionable if the shipping industry as stands, known for its traditional roots and resilience to untraditional changes, is prepared to the risks attached to these recent technological progresses.

Undoubtedly, the increased use of and reliance on technology in trade has made the shipping sector vulnerable to cyber attacks. Indeed, significant weaknesses have been identified in the cybersecurity of critical technology used for navigation at sea. GPS, AIS, and ECDI, as mentioned above, essential aids to navigation, have been identified as potentially vulnerable to attack. The recent cyber attack in one of MAERSK' ports clearly demonstrated the devastating affect that these might have, even in one of the largest and most solid shipping company in the word. The attack confirmed that irrespective of how big or small, any shipping stakeholder is susceptible of cyber attacks, which, as it was evidenced by the above example, will likely generate financial loss, business disruption, reputational damages and so forth. The more digitalised the shipping sector, the more it will encounter cyber threats, such as attacks on navigation, communication and remote control systems and programmes.

Given the potential risks arising out of cyber attacks and their possible impacts on businesses, shipping stakeholders inarguably need proper cyber risk insurance policies. At the moment, most traditional marine insurance policies are silent on cyber risk whereas others expressly exclude cyber risk from its coverage, such as hull covers by the CI.380 exclusion. There are a limited number of standalone cyber insurance policies available. However, these are unlikely to cover all potential risks arising from cyber attacks as their scopes are generally limited to financial and reputational risks. The fact is that due to lack of understanding on the extent of cyber risks, being this a new threat with new risks emerging on a regular basis it is not easy for companies to produce truly efficient plans and procedures for cyber risk managements and much less for insurers to provide efficient coverages, which will not expose unrestrictive liabilities.

---

[1] Assistant Professor Erasmus University Rotterdam

[2] PhD (Soton), LLM (Manchester), LLB (Marmara) E-mail: blmblt@hotmail.com

Moreover, to steer the issue even further, it can and it has been questioned whether an autonomous/ unmanned vessels comes within the current definition of a ship according to the current *lex maritime*, with numerous papers being written in the subject including the publication of a CMI position paper on unmanned vessels and the establishment of a working group to deal with the topic. Nevertheless, even if established that autonomous and unmanned vessels are indeed ships, the question that follows relates to the obligation of owners to provide a seaworthy vessel at the commencement of the voyage. Currently, the Hague Visby Rules, as well as the Marine Insurance Act 1906 (MIA) for instance, provided that such obligation includes, amongst other requirements, the maintenance of properly trained a crew, a task which is clearly not possible for an autonomous vessel upon a strict interpretation.

This paper aims to address different types of cyber attacks, the effects of these in marine insurance, especially in terms of cargo claims and the current security given to ship industry stakeholders in face of these type of attacks. Nevertheless, in order to achieve this, the paper will start with the basic, but unavoidable discussion, if autonomous and unmanned vessels can be considered ships, followed by a short discussion about general insurance issues raised by the used of such vessels, after which, focuses will be given to the concept of cyber attack; which types of attack fall into the scope of cyber attack and which do not; secondly, assesses the possible extent of cyber risk by analysing the core issues such as tangible-intangible losses, and proximate causes of loss. This paper will present the current position under marine insurance policies and provide some suggestions on how cyber attacks would be properly insured thereunder. Finally, this paper will concurrently address issues such as liability of the crew in case of autonomous vessel, the cyber attack falling in the category of piracy and if as such could be considered a peril of the sea, among others.