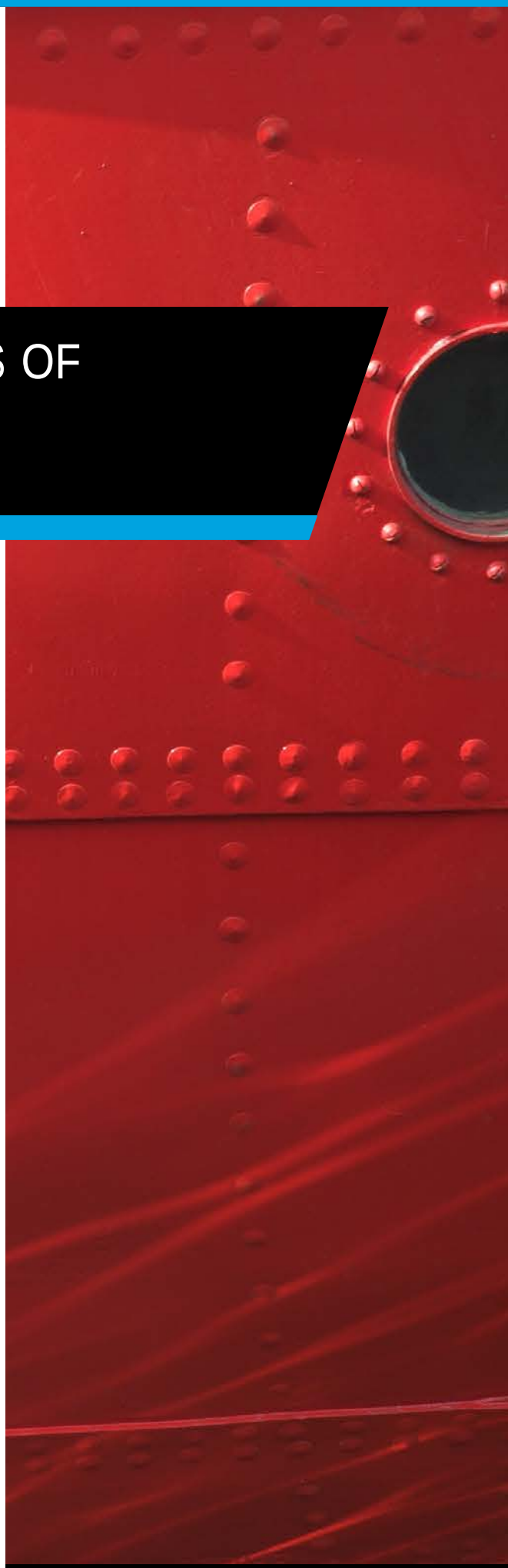
# ASSESSING THE CYBER RISKS OF MARITIME NAVIGATION

December 2017



You have most certainly heard of it before and have probably had enough of it. The pre-fix “cyber” is ubiquitous. It all began with “Neuromancer” by William Gibson, although it is unlikely that you have read it and it is of little concern to you. However, you will not be able to remain carefree for much longer - unless you have decided to go back in time to rely solely on a wind sail. However, as you have not, you cannot be immune to the cyber risks of navigation.

Together with the traditional navigation risks (the so-called risks of the high seas), nowadays merchants and insurers have to worry about the emergence of a new category of risks that arise from maritime navigation; risks that arise from the increasing dependence on the use of silicon chips in black boxes.

Cyber risks are inherent to the use of computers. It is rare that a boat, to some extent, is not dependent on the omnipresent information technology, which converts a vessel into a potential target vulnerable to cyber attacks.

On the one hand, the attacks could be deliberate - a hacker attempting to take control of the vessel – or, alternatively, merely the result of incompetence - a crew member downloading a virus to the on-board computer by error.

The more sophisticated, specialised and interconnected the boat or its port interface is, the more options there will be for a hacker to gain access. This cyber-pathology can only be further escalated if we consider the foreseeable growth that will occur with autonomous navigation.

Therefore, it is no surprise that BIMCO, INTERCARGO, INTERTANKO, OCIMF, IUMI, CLIA, ICS, DSTL, US coast guard and the IMO have already taken some initiative by issuing guidance and instructions as to how maritime cyber security should be managed.

Kennedys

In light of the above, in this article we propose to:

- Identify the cyber risks of navigation.
- Briefly analyse its coverage in the maritime insurance market.
- Study the impact that cyber security could have on SOLAS, ISPS, PSC, as well as the requirement of seaworthiness of the vessel under charter policies.

## IDENTIFICATION OF NAVIGATION CYBER RISKS

The biggest problem that we have when identifying the potential cyber attacks on a vessel is that, with few exceptions, merchants are reluctant to make them public, thereby hiding any financial damage and - more than anything - protecting their reputation (without mentioning any intention to avoid sanctions for breaches of data protection legislation, when appropriate.)

This "law of silence" has a pernicious effect: the merchant community and insurers do not have a claims history that can be used to assess the level of risk that exists, with the impact that either cyber risks are excluded from the policies or that premiums rise.

Nevertheless, information about some cyber attacks to the land based IT systems of the maritime-port sector have been published, including:

- In 2014, a transport company deposited a bond of US$10 million thinking that it was the vessel owner's account.
- In June 2017, Maersk and its subsidiary APM suffered losses of up to US$300 million due to ransomware NotPetya.
- A container terminal in the Port of Antwerp suffered various cyber attacks between 2011 and 2013 allowing smugglers to distribute narcotics with impunity.
- A bunker supplier suffered from a fraud of US$18 million when responding to a false order from US Defence Agency for a tanker vessel located on the Ivory Coast.

As a potential target of a cyber attack, a vessel has various vulnerable points: its IT systems and Operational Technology (OT).

The OT system controls the operative elements of the vessel. The information or electro-mechanic system of the bridge which controls, amongst others, the systems of propulsion, positioning, ballast and manoeuvre is part of the OT system. The IT only refers to the electronic communication of data, such as the intranet and email on board, without affecting, in principle, the operative machinery of the vessel.

The security system of the IT system is known as "cyber security", whereas the security system of the OT system is known as "cyber safety", although both form part of the concept of "cyber security."

Traditionally, the OT systems were isolated within the vessel without the possibility of online access so that any risks could only come from crewmembers or non-authorised intruders that gained direct access to the on-board hardware.

However, the trend has changed. Currently, it is common for vessels to have multiple sensors that monitor and control, in real time, the functioning of the online machinery and transmit information via remote to the merchant courtesy of the IT system of the vessel. In other words, the OT and IT systems of the vessel are becoming more interconnected - to the extent that the existence of a vessel without crewmembers (controlled entirely remotely) is a future reality.

Naturally, when the IT or OT system is internet accessible, the risk of a cyber attack increases greatly. But, to gain access remotely to the IT or OT systems, the hacker needs to breach the satellite, 4G or Wi-Fi connections of the vessel.

Although breaching the communications by satellite (for example, the GPS) is possible, it is not a simple process and requires a well-financed, organized and meticulous cyber attack, beyond a common "cyber delinquent". Nevertheless, the common cyber delinquents have an easier task to pirate the 4G or Wi-Fi network when the vessel is docked.

What are the profiles of our cyber delinquent? They range from the "hacktivist" that have economic and commercial disruptive motives to the "ethical hacker" that seeks to highlight the vulnerability of information technology systems; from the extortionist that seeks a ransom to disinfect the vessel's malware to the industrial, military or competitor's spy. Naturally, the hacking will have its own economic logic - nobody will take the time to pirate a satellite network if they are not going to obtain an economic award proportional to their efforts.

Once the hacker has gained access to the vessel's network, various offences against data protection legislation could be committed, exposing companies, for example, of cruise liners (with respect to passenger and employee data) or freight vessels (exposing details of electronic boardings).

In addition, hackers could go further and access the most sensitive elements of the vessel's IT systems.

There are cases of hackers that have managed to inhibit or falsify the GPS signal of a vessel, or pirate the AIS and ECDIS systems which could affect the course of the vessel and cause the vessel to run aground in conditions of poor visibility.

Finally, although various firewalls should prevent it, the cyber delinquent could reach the hard nucleus of the vessel – its OT systems – and manage to take control over the dynamic positioning systemthe propulsion, the ballast system or manoeuvring of the vessel. Hackers have previously managed to modify the location of a petroleum platform off the west coast of Africa and, in February 2017, a container ship on route from Cyprus to Djibouti was hacked for 10 hours, during which the captain lost control of the manoeuvring system. In addition to the potentially catastrophic nature of such a situation (port blockades, collisions) there could also be more modest consequences in which hackers manage to leave a vessel "off-hire" under a fixed time charter policy.

Therefore, it can be seen that a vessel will be less vulnerable to a cyber attack if it is less dependent on its IT and OT systems.

## COVERAGE OF NAVIGATION CYBER RISKS IN MARITIME INSURANCE POLICIES

Ship-owners, as any business person susceptible to cyber attacks, now have coverage for cyber risks available (as a non-maritime risk). In the strict ambit of maritime cyber risks, it is helpful to differentiate between the P&I clubs and insurance companies.

In general terms, in contrast to insurance companies that insert the well-known "Institute Cyber Attack Exclusion Clause 380" (Exclusion 380) in their hull, machinery and freight policies, the P&I clubs (at least, those of the International Group) do not automatically exclude coverage for losses or civil liability resulting from cyber risks.

In fact, being aware of the application of Exclusion 380 by insurance companies, the clubs offer specific coverage for claims that are usually excluded (for example, the Norwegian Hull Club's "Cyber-Clause 380 buy-back").

The P&I clubs expect their members to adopt all of the recommended measures to manage cyber risks, both in port and on-board the vessels, which is why many clubs make reference to compliance with the cyber security guidelines issued by the BIMCO.

In contrast with this, insurance companies expressly exclude cyber risks by way of Exclusion 380 in relation to hull and machinery coverage as well as freight (although in this case there is a sweetened version of Exclusion 380 by virtue of which the exclusion is not applied if the use of a computer has contributed to the theft or appropriation of the insured merchandise).

Exclusion 380 leaves ship-owners without coverage for damage and loss of profits caused by cyber attacks. Under Exclusion 380, it is sufficient that the damage has been caused remotely by a cyber attack and that the cyber attack has been used to cause damage through the introduction of, for example, a malicious code or virus with intent to cause harm.

This provides an obligation to the ship-owners to obtain a specific ad hoc insurance. Currently there are not a lot of specific insurance products for hull and machinery against cyber attacks, although some insurers have indicated that they would be willing to abolish Exclusion 380 if ship-owners are willing to report cyber attacks (thereby allowing insurers to obtain information and quantify, consider and grade the insurable risk) and to comply with determined practises and preventative audits.

## LEGAL IMPACT OF CYBER-SECURITY

The IMO is conscious that the maritime-port sector cannot remain on the fringes of the management of cyber risks, both on-board and on-land.

For that reason, the following documents have been published:

- A multiple language glossary of "Cyberterms" that serves as a general guide.
- Circular MSC.FAL.1/Circ.3 that provides the "Guidelines on Maritime Cyber Risk Management" (which also makes an express reference to the Guidelines on Cyber Security On-board Ships from BIMCO).

Specifically, the IMO has given ship-owners a deadline of until **1 January 2021** to incorporate the management of cyber security in their ISM code. From that date, vessels can be detained for inspection by the Port State Control (PSC) for not having implemented the recommended measures of the IMO for "cyber safety" (applicable to the OT systems of the vessels) or for "cyber security" (applicable for IT systems of the vessel).

Because of these risks, it is likely that the IMO will shortly demand similar measures with respect to the ISPS Code.

Therefore, a new source of obligations are on the horizon for the already saturated ship-owner: management of cyber security, not only to prevent cyber attacks (with its associated costly insurance coverage) but also to avoid fines and detentions of vessels.

As a result of the above, another question arises: Could we see a vessel "cyber-unseaworthiness"?

In accordance with sections 3(1) of the Hague Visby Rules and 212 of the Maritime Navigation Act, a ship-owner is obliged to guarantee the navigability (in the sense of both seaworthiness and cargoworthiness) of their vessel, applying due diligence to conserve this condition of navigability at all times. Charter policies also demand the same. In summary, seaworthiness is a basic necessity to operate and insure a vessel.

What happens then if a ship-owner does not comply with the guidelines for the management of cyber security on board as required by the IMO and BIMCO? Can it be implied that the non-compliance will lead to "uncargo-worthiness" or "unseaworthiness" under a charter policy or a bareboat charter lease?

If a ship-owner omits to take preventative cyber security measures and, for that reason, a hacker gains access to the systems of freight, manoeuvres, ballast or propulsion of the vessel and causes a loss, the question arises as to whether the vessel was really navigable and ready to receive and transport freight securely.

In the same way, this unseaworthiness due to a lack of cyber security could constitute a situation of "off-hire" under a charter policy. For example, a cyber attack could leave a vessel without machinery, ballast and, therefore, inoperative.

The danger can only increase with the emergence of the autonomous navigation, which will be more vulnerable to cyber attacks (and from which the concept of seaworthiness will need to be re-evaluated as it is intended that such vessels go without crew, something which will need an express reform of the SOLAS).

## COMMENT

No ship-owner is immune to the cyber-risks, although the level of vulnerability will be proportional to the level of automation and interconnectivity of the fleet.

The IMO has set a deadline of the 1 January 2021 for ship-owners to incorporate the management of cyber security into the ISM code; in the event of non-compliance, we anticipate seeing the first cases of detention for such reasons. It is foreseeable that the IMO will incorporate similar demands in the ISPS.

It is not beyond the realms of possibility that omissions in the area of cyber security will affect the concept of seaworthiness of a vessel, with all of the associated consequences not only resting with the relevant authorities – fines and detentions – but also contractual, relating to insurance policies for hulls and charter.

With the increasing regulatory pressure over cyber security in the maritime sector and the progressive automation and interconnection of nautical technology, it will be inevitable that there will be a need for new insurance products that specifically cover the maritime and port cyber risks.

## FURTHER INFORMATION

To find out more about our services and expertise, and key contacts, go to: **kennedyslaw.com**

## KEY CONTACTS


**Olivia Delagrange**
Partner
t +34 91 523 7210
olivia.delagrange@kennedyslaw.com

**Jose Pellicer**
Lawyer
t +34 91 523 7210
jose.pellicer@kennedyslaw.com