THE FUTURE OF CYBER COVER IN THE NORDIC MARINE INSURANCE MARKET

Written by Preben Helverschou (Senior Lawyer) and Sanne Bygholm (Associate).

1. INTRODUCTION

In recent years, the shipping sector has faced an increasing threat of cyber related incidents. Shipping has gone "online". Vessels and offshore units are constantly growing in sophistication and in the use of digital solutions, making them vulnerable to cyber-attacks. The threat of cyber-attacks has only increased following the Covid-19 pandemic, as criminals take advantage of changes in working routines and the increased use of remote access systems.

On the shore side, these risks may translate into financial losses caused by interruptions of commercial operations. Examples that received wide publicity were the ransomware attacks on Maersk in June 2017 and on Norsk Hydro in March 2019.

On the offshore side however, these risks are not only financial in nature. There are safety concerns linked to potential cyber-attacks on navigational-, engine-, cargo- and ship management systems. These systems have all become progressively digitalised over time. Therefore, the possibility of an attack against a vessel or offshore unit appears real and could lead to disastrous results. With further advances in technology we may safely anticipate that problems related to cyber risks will rather increase than decrease in the time to come.

In response to the development, the International Maritime Organisation (IMO) has issued guidelines on cyber security on board ships. Shipowners and operators now have until 2021 to incorporate procedures on cyber risk into their ship safety management systems.

The marine insurance market is also reviewing their approach to cyber risks. Traditionally, the Nordic insurance conditions have been "all risk" covers, meaning that whatever risk is not explicitly excluded – is covered. Thereby, some policies have covered cyber risks "silently" because these risks have not been expressly excluded.

Critics to the practice argue that silent cyber cover has been provided by many insurers without fully considering, pricing and reserving for such risk, thereby creating market vulnerability. They further argue that the practice results in an unclear scope of cover and thus uncertainty for assureds, insurers and reinsurers alike.

Supporters to the practice argue that there is nothing which prevents insurers from pricing and reserving for "silent cyber cover" as long as the risks are known, which presumably is the case today. They further argue that silent cover of cyber risks does not result in any more uncertainty than other "silent" risks covered under the NMIP.

Notwithstanding the foregoing, many insurers have excluded cover of cyber risks through the Institute Cyber Attack Exclusion Clause 380 from 2003. However, the clause is to some extent ambiguous, and only excludes cover for cyber-attacks, not also accidental cyber events. Critics therefore argue that the clause is no longer suitable for the cyber risks the shipping industry faces today.

On 30 January 2019 the UK financial supervisory authority (PRA) issued an instruction to all UK insurers that from 1 January 2020, all first party property damage insurance products must either positively affirm, or explicitly exclude cover for cyber risks. Silent cyber cover is thus no longer allowed in the UK market. These changes are also likely to affect the Nordic marine insurance market, as it is influenced by UK requirements through reinsurance programmes and UK co-insurers.

The aim of this article is to examine the cyber cover provided in the Nordic market today, and how this may be affected by the changes in UK requirements. In our review, we will focus on the Hull & Machinery cover ("H&M") provided under the Nordic Marine Insurance Plan 2013, version

2019 (the "NMIP"), based on Norwegian law. However, the article will also have relevance for other insurance terms, e.g. the Norwegian Cargo Clauses (Cefor Form 261).

For the purpose of this article, we will refer to "cyber risks" as any risk associated with financial loss, disruption or damage to the reputation of an organisation from failure, unauthorised or erroneous use of its information systems.

2. CYBER COVER IN THE NORDIC MARKET TODAY

As stated above, the Nordic insurance conditions are traditionally "all risk" conditions. Thus, they provide silent cover for cyber risks unless explicitly excluded in the insurance contract.

This can be illustrated by NMIP Clause 2-8 reading "An insurance against marine perils covers all perils to which the interest may be exposed, with the exception of: [...]". Clause 2-8, does not list cyber as an excluded risk. Cyber risks are therefore at the outset covered.

The silent cyber H&M cover under the NMIP is however restricted by the general exclusion of war perils in Clause 2-8 (a), cf. Clause 2-9. War perils are customarily covered by a separate hull and machinery war risk insurance ("War H&M"). The distinction between which cyber risks are considered respectively as marine perils and war perils under the NMIP must be drawn based on the wording in Clause 2-9.

Cyber-attacks conducted as part of a war effort, i.e. so-called cyber warfare, clearly qualify as war perils, as per Clause 2-9 (a), whether or not the assured is the target of the attack, or collateral damage only. Most of the major cyber-attacks which have taken place in the last decade fall within this category e.g. Stuxnet, WannaCry etc. For less coordinated attacks or events the position is less clear. "Sabotage" and "acts of terrorism" qualify as war perils and may by its wording comprise certain cyber-attacks. However, under Norwegian law, the term "sabotage" is construed narrowly, in that it presupposes that the action leading up to the loss pursues a specific political, social or similar goal.

This is illustrated by the decision published ND 1990.140 NA "PETER WESSEL". In the decision, the court found that the costs of interrupting the ship's voyage due to a bomb threat was recoverable under the H&M insurance against marine perils, as costs of measures to avert or minimise the loss. The crux was that the external circumstances of the threat clearly indicated that this was an act that had no background in political, social or similar circumstances.

Similarly to the construction of the term "sabotage", the Commentary to the NMIP prescribes that the term "act of terrorism" requires that the "purpose is to promote a political, religious or ideological cause". Thus, also here, a distinction must be drawn between such acts and ordinary criminal acts, including blackmail, bomb threats, etc., purely for the purpose of financial gain (cyber-crime).

A main factor in determining whether a borderline case qualifies as respectively marine or war perils under the NMIP is therefore the purpose behind the malign act. This creates a special challenge for cyber risks, as it often is difficult to determine the culprit and their true intentions. This is especially the case when the assured is not the target of the attack, and merely an affected party.

This can be exemplified by a ransomware attack. Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it, unless a ransom is paid. Given that the purpose by nature is to get the ransom payment - a financial gain - ransomware attacks will as a starting point be considered as marine perils under the NMIP.

Nevertheless, ransomware can also be used as a tool to achieve a specific political or social goal, or to promote a political or ideological cause, e.g. if the main aim is to intercept trade to or from a specific country, while the potential financial gain is a mere bonus, or a means to finance the attack. In such case, the attack would likely qualify as a war peril. The problem is that the true purpose of a cyber-attack may be challenging to unveil, and even more challenging to prove. This results in legal uncertainty for both insurers and assureds alike.

3. IMPLICATIONS OF THE UK CHANGES

The new PRA instruction - that all first party property damage risks either must positively affirm, or explicitly exclude cyber cover from 1 January 2020 - has already impacted the UK insurance market.

As a result, and in order to regulate cyber coverage in insurance contracts, the Lloyd's Mar-

ket Association has issued new model clauses: LMA5402 – Marine Cyber Exclusion, and LMA5403 – Marine Cyber Endorsement.

- The LMA5402 – Marine Cyber Exclusion is drafted as a paramount clause and excludes all cyber related losses from cover under the policy.

- The LMA5403 – Marine Cyber Endorsement affirms cover for so-called "non-malicious" cyber, provided that the subject loss otherwise would be recoverable under the policy. The exception is where the clause is included in a war policy, in which case certain losses related to cyber-attacks against electronic missile/weapon systems also are recoverable.

In accordance with PRA guidance statements, cyber risks are considered "non-malicious" when they are not explicitly motivated to cause harm. This includes e.g. cyber errors, accidental loss of data, and use of information technology failures that result in physical damage to infrastructure and/or business interruption losses.

In contrast, cyber risks are considered "malicious" when they are explicitly motivated to cause harm. This e.g. includes intentional cyber-attacks such as Distributed Denial-of-Service attacks, and infection of an information technology system with malicious code.

The distinction between non-malicious and malicious cyber in the LMA clauses is similar to the distinction between cyber considered as respectively marine perils and war perils in the NMIP. In both sets of terms, it is the intent that is the deciding factor for which category a cyber-event falls within. However, this is also were the similarities end: whereas a malicious cyber-event under LMA clauses only requires that the event is motivated to cause harm, the NMIP war peril cover also requires that the event's purpose is to achieve a specific political or social goal, or to promote a political or ideological cause.

The difference can again be illustrated by the ransomware example. Under the LMA clauses a ransomware attack will probably qualify as a malicious cyber-attack irrespective of whether its purpose is pure financial gain or a specific political or social goal. Under the NMIP a pure financially motivated attack will as an outset probably be considered a marine peril, and only a war peril if it serves a specific political or social goal.

The differences between the two sets of insurance terms create certain challenges for shipowners, operators, insurers and reinsurers. In the event a shipowner takes out H&M insurance based on the NMIP, and War H&M based on UK conditions, or the other way around, there will either be gaps or overlaps. The same issue may potentially arise if a Norwegian H&M insurer, which sells insurance based on the NMIP, buys re-insurance in the UK market. Although, it should be noted that this will not be an issue if reinsurance is purchased on the same terms as the underlying insurance, with an express exclusion or endorsement of cyber risks.

The issue of gaps between the NMIP and UK conditions is not new. In the commentary to the NMIP, this is highlighted in relation to piracy. In a H&M policy based on NMIP, piracy would be considered a war peril according to NMIP clause 2-9, and thus excluded from cover. However, under UK conditions, piracy in principle is regarded as a marine peril and as such excluded under a UK war policy. In such a case, the insured would be uninsured against piracy altogether.

The new UK instructions may also have implications for H&M policies written on the NMIP with UK co-insurers. Without an express cyber endorsement or cyber exclusion clause, the policy will not satisfy UK requirements. Further, in the event one wishes to solve this problem by incorporating the LMA5403 – Marine Cyber Endorsement clause, this must also be coordinated with the war policy to avoid gaps in the shipowners' insurance cover.

In summary, the new UK cyber instructions and the introduced LMA clauses are not directly compatible with the silent cyber cover provided by the NMIP. This can result in unintended gaps in cover, and ambiguity for shipowners, operators, insurers and reinsurers, unless specifically resolved in the relevant insurance contract.

4. WHAT IS THE FUTURE OF CYBER COVER IN THE NORDIC MARKET?

The changes in the UK regulations and the introduction of the LMA model clauses may result in more explicit regulation of cyber in insurance contracts under the NMIP in the years to come.

This raises the question of how the Nordic Insurance market should respond to this development. We would argue that there are two options going forward to adapt to the new UK regulations.

The first option is that insurers and assureds go on as before, and negotiate whether cyber should be excluded or endorsed for each policy. As advised, silent cyber is not an option for any policy tied to the UK. The LMA model clauses can to some extent be used for this purpose, but the fact that they are not directly compatible with the NMIP implies that certain adaptations should be made.

The second option is to regulate cyber risks explicitly in the NMIP and the Norwegian Cargo Clauses, making the use of such additional clauses superfluous. It is arguable that explicit cyber regulation would increase legal certainty, and make the regulations more accessible for the assureds. It could potentially also accommodate for better operability between the NMIP and UK conditions and ultimately decrease market vulnerability to silent cyber risks. However, the potential downside is that this could make the terms more stringent and leave less room for individual solutions directly in the policies. It is also a solution which to some extent goes against the concept of "all risk cover", which is a cornerstone in the NMIP.

In the event one would decide to pursue an express regulation, there seem to be two viable alternatives. The first alternative would be to exclude cyber entirely. The exclusion would likely be coupled with an option to buy-back such cover, i.e. so that the assureds have the flexibility to only buy the cover that they need. This solution provides predictability and sets a clear price on cyber cover under the NMIP. However, the solution may result in an unnecessary administrative burden, if a majority of the assureds are interested in buying cover for cyber risks in any event.

The other alternative is to expressly incorporate cyber cover along similar lines as the LMA Cyber Endorsement Clause. This must probably be based on a bespoke wording, adapted to the NMIP, and considering the above-mentioned issues. In particular, one could e.g. consider adopting the distinction between malicious and non-malicious cyber events in the LMA model clauses. As advised, the distinction between marine and war perils in the NMIP is largely based on the intent behind the malicious act. This can be difficult to determine in case of a cyber-attack. To instead draw the line between malicious and non-malicious cyber events, which we understand could be easier to determine from a technical standpoint; may thus provide more predictability and legal certainty for all parties. This would also ensure better interoperability with UK conditions, as there would be no clear gaps between the two sets of conditions.

Which solution will be chosen remains to be seen. The revision of the NMIP is a formalised and complex procedure. The NMIP has status of an agreed document, meaning that changing the current mechanics on cyber would need the approval of all involved parties.

On balance, we anticipate that a factor which may tip the scale, is the respective solutions effects on reassurance costs, and thus in turn premium.

5. SUMMARY

In conclusion "silent cyber cover" is no longer an option for any policies with ties to the UK. This raises the question of how this should be addressed moving forward, i.e. either by bespoke policy adaptations or by amending the NMIP.

How the Nordic market decides to approach this situation waits to be seen. Fortunately, there is some time left to find a flexible and mutually agreeable solution. The new version of the NMIP will not be published before 2023.

CONTACT US:

Preben B. Helverschou

Senior Lawyer

phe@kvale.no
+47 920 59 672

Kristian Lindhartsen

Partner

kli@kvale.no
+47 930 03 313

www.kvale.no