Risky business: managing geopolitical security threats

Due to pandemic restrictions, Gard held its 16th annual Charterers and Traders Geneva seminar as a webinar. The topic of global maritime security threats was addressed through role play with panellists representing a shipowner and a charterer. To kick-off, our guest speaker from Risk Intelligence, took us through an overview of the current and emerging security risks for shipping.

Published 12 January 2022

Written by Sammy Christopher Smallbone

Introduction

In our recent Charterers and Traders webinar, our guest speaker, Henrik Ehlers Kragh COO of Risk Intelligence, discussed cyber threats, war risks and current emerging risks in connection with global shipping and trade. Our Gard panellists, Craig Johnston as moderator, Balvinder Ahluwalia as a shipowner, Helena Biggs as charterer, and Arek Glaas in his role as underwriter, performed a role play considering the commercial and legal issues and insurance solutions connected with these various threats and risks.

The event was recorded and is available here . This Insight addresses questions put to the panellists together with some key takeaways.

Overview

Henrik, could you please give us an overview of the current global security picture? As a global overview – Risk Intelligence recorded 273 incidents between 1 January and 18 November 2021, so about one a day. The most challenging areas - those circled in red on the map below- include the Persian Gulf, Western Indian Ocean, Red Sea, Eastern Mediterranean and Gulf of Guinea – primarily off Nigeria due to kidnap and ransom of crew.

Areas in the yellow circles are elevated risk areas. The South-East Asia cluster shows incidents due to robbery, theft and corruption. The Eastern Black Sea incidents are primarily due to ongoing tension between Russia and Ukraine and finally in Central America – incidents were largely theft, armed robbery and drug smuggling. So – different regions present different security threats.

Cyber threats

Henrik, what is a 'Cyber threat' and should we expect the situation in the Black Sea to get worse before it gets better ? First,when Risk Intelligence talks about a 'Cyber threat', we are really talking about three types of possible attack - malicious attacks, jamming and spoofing. A malicious attack is aimed at a companies' IT systems with criminal intent. An example would be the NotPetya malware attack of Maersk Line in 2017. Jamming is the disruption of electronic devises with "white noise". Jamming is used offensively and defensively by military forces and can also be used by criminals to jam GPS devices on valuable assets. Jamming is usually easy to detect and does not affect navigation.

Spoofing interferes with electronic signals and places electronic plots in a different geographical place. If your vessel suddenly appears on land – you are being spoofed. To be affected, the vessel must be within range of weaponry, so spoofing is more likely to happen when close to land. Spoofing technology is not as easy to obtain as jamming technology and generally requires advanced technology used by military forces to disrupt, command and control systems.

As for the situation in the Black Sea, this is indeed a good question and perhaps one that only Russia's President Putin can answer. In my view the situation is unlikely to get better any time soon, and in fact it may turn worse.

From a geo-political perspective Russia may have several strategic objectives that could be met by a successful invasion. However, an invasion is not without risk. If Russia anticipates that the international community (primarily Europe and the US) have limited options left as regards sanctions and if they have the sense that any new sanctions will only have limited effect on Russia, then it really is only the risk of military failure that points towards Russia wanting to maintain the status quo.

From a commercial maritime perspective, I think the shipping community should prepare for how any changes in sanctions may affect trade patterns. In any event, it is my belief that sanctions, current and potentially future, will remain "the norm" for quite some time.

Balvinder, who pays for the time lost due to jamming and/or spoofing? * *From what we currently know, jamming and spoofing attacks take place as a result of malicious third-party cyber activity. Such incidents may be very short, and may go unnoticed, or may be for a more significant period of time, with consequent time loss. If that happens, and assuming your charterparty does not have a specifically negotiated clause addressing liability for such time loss, charterers may look to place the vessel off-hire. Under most of the standard form charterparty off-hire clauses time loss as a result of jamming or spoofing is not addressed and so it is unlikely that such an off-hire claim would succeed.

In any event, as a defence to any such claim for time loss owners may say that the vessel has only been the subject of such a cyber incident because of the charterers' instructions to go to the particular port. Owners would therefore rely on any implied or express indemnity that may be available as a result of complying with charterer's employment orders. See, for example Clause 8 of NYPE 1946.

Similar considerations may apply under voyage charter terms in the context of interruptions and/or exceptions to laytime and demurrage. Again, we have not seen voyage charter terms that seek to except time lost as a result of jamming or spoofing

incidents from the calculation of laytime, or interrupt laytime for any such time loss periods. Of course, if any such incident causes time loss before the commencement of laytime then that would be for Owner's account.

Arek, if all cyber risks are excluded, does that mean damage caused by a guided missile or a drone is excluded if any computer systems are used to guide them to the target? It's a very relevant question, as there's very likely some sort of software or a computer programme in most types of modern weaponry including missiles or drones.

The policies of our charterers Members' which renewed on 20 February 2021 or later include Marine Cyber Endorsement (LMA 5403) which excludes cyber risks. This exclusion became necessary to harmonise our terms with market practice and the governing reinsurance arrangement. The Marine Cyber Endorsement is currently the most common cyber exclusion used across the markets. It's a relatively broad exclusion referring to "any computer" and "any electronic system" but it is limited only to instances where a computer programme or system is used to inflict harm.

There is an exception to the exclusion introduced by this endorsement. Where it is endorsed on war policies or, as in the case of our charterers' entries, on policies including war risks, the exclusion is not meant to operate to exclude claims caused by weapons of war where a computer or an electronic system is used in the launch or guidance systems or firing mechanism of a weapon.

Instances where damage is directly caused by a weapon of war would be covered, even if electronics are used in the launching, guidance or firing mechanisms. But the exclusion would kick in where the damage is caused directly by a malicious code, or software used as a means of inflicting harm.

War risks

Henrik, with the increased naval presence in the Gulf of Guinea is there still a need for private security guards? The use of armed guards in the Gulf of Guinea is a complex issue and different coastal states have different legislation to regulate this.

Of course, all vessels trading in the Gulf of Guinea should recognize and apply the recommendations given in the Best Management Practices West Africa .

Employing armed teams and escort vessels is not without risk and any decision to use such should be based on the result of a specific voyage risk assessment, that factors in the threats, the vulnerabilities of the vessel in question, the route, and any potential external support - for example, naval assets and the concentration of such assets.

* *Balvinder, would an occurrence of a prior limpet mine attack render a port unsafe under English Law?* * This is really a question of whether owners are entitled to refuse a voyage order on the basis of contractual unsafety of a port as a result of a single prior incident.

There is legal authority that the particular 'unsafety' must be in the port to where the vessel is ordered and not simply the general vicinity of that port. The UK Supreme Court in *The Ocean Victory* [2017] 1 Ll.R 521 provided clarification on what constituted abnormality and in essence the matter comes down to the knowledge of the charterers at the time that orders were given to the owners. A single prior attack

correspondents, or other contributors.

may be considered to be abnormal where a charterer can demonstrate that at the time orders were given there had been no recent attacks and adequate precautions were now in place/being taken against any such attack, and thereby rendering any subsequent attack to be viewed as an abnormal occurrence.

In the case of a prior limpet mine attack the question of port safety is likely complicated by the fact that currently the situation is still evolving in terms of what adequate precautions would be required and therefore charterers would be advised to seek specialist advice, without which it may be the case that one prior limpet mine attack may well render a port unsafe.

Helena, if a ship is laden and ends up going to an alternative discharge port because of concerns about the safety of the original port, who picks up the additional costs of getting the cargo to destination? Owners' ability to discharge cargo at a port other than the port identified in the bill of lading will depend on the terms of the bills of lading. If those terms contain a liberty clause permitting the shipowner to discharge the cargo as close to the discharge port as they can safely reach, then owners may be entitled to discharge at an alternative port or place. If additional costs are incurred in trans-shipping the cargo to its end destination, which party ultimately pays those costs would depend on whether or not the port was indeed unsafe as a matter of fact. If the port were to be considered unsafe, Charterers would have to meet the trans-shipment costs and this approach has more recently been codified in some of the industry war risk clauses, such as the BIMCO clauses.

Arek, what if it's not possible for the charterers to agree all conditions which you say are needed for the policy cover for damage to ship caused by war risks? Our standard charterers' entries include cover for damage to or loss of the chartered ship caused by War risks, but this cover is conditional on the following provisions being included in the applicable charter agreement:

1. Owners can refuse to send the ship to a place which is dangerous by reason of war risks.

2. Owners have liberty to insure Hull and their other interests against war risks.

3. Charterers reimburse owners the war risks premium incurred as a result of the ship being ordered to such a place.

The rationale behind these conditions is that parties choose an insurance solution rather than an allocation of responsibility. Therefore, if charterers pay the additional war risks premiums, as long as the charterparty provides suitable protection, there is support for the view that charterers would be protected from a subrogated claim by war risks underwriters. There is uncertainty around how an English court of law might decide in such a case, but if the claim against charterers is indeed allowed, then our charterers Liability policy will provide protection.

If charterers cannot get owners to agree these three conditions, or conditions similar and equally favourable, we are able to review individual circumstances and adjust cover if notified in advance, but we would normally have to charge charterers an additional premium for such buy-backs. We are also able to provide a cover extension to buy back this condition on an open basis for some or all of the assured's chartering activity. If charterers members want to avoid paying this additional cost, our suggestion would be to work with owners to include these points in the charter

party.

We thank our guest speaker , Henrik Ehlers Kragh and Risk Intelligence *for the participation in our webinar and follow up question and answer session. *

For information about ship-board cyber security, see our training video on Cyber Awareness . For a discussion of piracy in the Gulf of Guinea see our previous webinar Maritime Security – unsafe seas, insecure crew .