A DISCUSSION CONCERNING THE INTERPLAY BETWEEN TRADITIONAL MARINE PERILS, GNSS/GPS SPOOFING AND CYBER EXCLUSIONS

The Inquiry

An inquiry was received by the Association as to whether a Shipowner is covered for damage caused by a grounding if that grounding was a result of (or contributed to by) "GPS spoofing".

Given the open nature of this inquiry, it has not been possible to provide a definitive view. All cases will be fact specific. In the opinion below, the Advisory Committee discuss what GNSS/GPS Spoofing is and some of the legal and policy interpretation issues which will arise, and in particular some of the aspects of the standard Cyber Exclusions (i.e. LMA5403) in grounding and similar cases where GNSS/GPS Spoofing may have played a part.

SUMMARY

GNSS/GPS Spoofing involves someone transmitting a fake GNSS or GPS signal which deceives the receivers on a vessel leading to the navigational and other equipment on the vessel reporting a false position for the vessel to the crew. The difference in position can be considerable and it can readily be seen that where a crew is relying on the GPS data, a vessel may be deceived into going in to shallow water and grounding.

The standard Cyber Exclusions found in Hull and Machinery policies (such as LMA5403) exclude:

> *"...loss, damage, liability or expense directly or indirectly caused by or contributed to, by or arising from the use or operation, as a means of inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system."*

It is clear that any GPS Spoofing will be derived from some form of *"electronic system"*.

The extent to which GPS Spoofing may play a part in any particular grounding will be fact specific. Below we discuss in more detail some of the issues with this and the extent to which GPS Spoofing may be considered to have directly or indirectly caused or contributed to a casualty.

The more difficult question is with regard to the exclusions requirement that the actions need to be a *"means on inflicting harm"* and on whom the burden of proving or denying this falls.

It is in the nature of GPS Spoofing that it may be difficult, if not impossible, to positively identify the party responsible. However, the overall context may be sufficient to give rise to a presumption that the motives behind spoofing have harmful intent.

For example, if a vessel is sailing through a known high-risk area with increased political tensions when suddenly she experiences GPS spoofing, the Courts may view that there is a rebuttable presumption that the spoofer intended harm. It would then be for the assured to offer up a plausible alternative argument which supports the view that the spoofing was in fact not intended to be harmful.

On the other hand, if some random GPS signal disruption occurs whilst the vessel is not in a "hot spot" area of the world, then insurers will have a much harder task to show harmful intent was involved and would likely have to establish more specific details to support their case, e.g the identity of the perpetrators, the motivation, etc. - in such circumstances the bar to meet the burden of proof on harmful intent would be much higher for insurers.

Conclusions

Whilst the question points to the fact that GPS spoofing may generally be intended to have some harmful intent, it is not inconceivable that the activation may be accidental or not intended to cause harm. Equally in most cases the spoofing having had a genuine causal effect on the grounding, but there may be cases where it can be shown this is not the case. We do not believe that it will be sufficient for an insurer to simply show that some element of GPS spoofing has occurred.

The reality is that it is not possible to draw definitive conclusions on how applicable the Cyber Exclusion will be in every case. It should also be emphasised that all cases will be fact specific. It may be dependent of the particular location of the loss, the likely party or parties who may have been involved and their motivations and, consequently, who may have the burden of proving or denying harmful intent.

If in doubt, assured's can always take out additional Cyber Buy-back clauses which, for additional premium, allow the insured to get cover for many losses which would not be covered as a result of the cyber exclusions. All such wordings would need to be reviewed in detail but many would cover a grounding resulting from GPS spoofing regardless of the motivation of the party responsible or the causal connection between the spoofing and grounding.

DISCUSSION

What is GNSS/GPS Spoofing?

GNSS and **GPS** (Global Positioning System) have been rapidly integrated in modern navigation and are generally highly reliable but may be susceptible to spoofing.

GNSS / GPS systems use signals received from a number of satellites to accurately calculate the vessel's position in real time. GNSS provided Positioning, Navigation and Timing (PNT) data inputs are also integrated with other navigational and communication systems onboard.

"GNSS / GPS Spoofing" involves transmitting a fake GNSS signal to deceive the receiver on a vessel, causing the system to compute incorrect PNT data. This will provide the crew with an inaccurate position for the vessel on the affected system and may indicate the vessel's position to be a considerable distance from her actual position. As a result, a vessel may ground despite her navigational system indicating that she is in a channel or deep water.

Whilst there maybe other iterations of manipulation of onboard systems which could lead to groundings, this discussion only considers the example outlined above.

Traditional coverage for grounding in marine policies

Accidental grounding is a peril of the seas and covered by all of the main Hull & Machinery standard policy conditions. As a result, if a vessel were to ground as a result of the crew being deceived by GPS spoofing, the loss would *prima facie* be covered by the policy.

It is perhaps noteworthy that there are various domestic and international standards of navigation and seamanship which should, in theory, mean that any manipulation of GNSS/GPS is detected by the watchkeepers on duty at the time and that these systems should not be solely relied on in any event. For example, the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978 (STCW) provides:

> *"…On taking over the watch the relieving officer shall satisfy himself as to the ship's estimated or true position and confirm its intended track, course and speed and shall note any dangers to navigation expected to be encountered during his watch…"*

The regulations only increase when close to shore or in dangerous or congested waters - and other systems such as the radar, echo sounders, bearings etc. should be used to confirm the vessel's position. However, even if the crew were negligent in not undertaking such verification work, the grounding would be considered a "peril of the seas" per s.55 (2) (a) of the Marine Insurance Act 1906, which states:

> *"…The insurer is not liable for any loss attributable to the wilful misconduct of the assured, but, unless the policy otherwise provides, he is liable for any loss proximately caused by a peril insured against, even though the loss would not have happened but for the misconduct or negligence of the master or crew…"*

In the absence of any exclusions regarding the issue, it seems clear that a claim can arise under most marine policies for a grounding, despite the fact that GPS spoofing may have played a role.

Effect of cyber exclusions

Once a "prima facie" claim has been established on a policy, the burden of proving that an exclusion applies falls on the insurers.

Most modern marine wordings, have exclusions for certain types of cyber risk. These are: -

- Institute Cyber Attack Exclusion Clause 10.11.03 (CL 380)
- Marine Cyber Exclusion LMA5402 (11.11.19)
- Marine Cyber Endorsement LMA5403 (11.11.19)

All of these clauses have similar wordings with regard to the issue and LMA5403 (currently the most commonly used) which states: -

MARINE CYBER ENDORSEMENT

1. *Subject only to paragraph 3 below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to, by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system.*
2. *Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.*
3. *Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.*

Sub-clause 2 merely emphasizes the need for the motive of inflicting harm.

Sub-clause 3 carves out of the exclusion those cases where an electronic system is used as a means for launching a weapon or missile which, self-evidently, would have harmful intent.

Sub-clause 1 comprises the actual exclusion and has three main requirements that need to be satisfied in order to take effect, namely:

1. The loss or expense must have been ***directly or indirectly caused by or contributed to, by or arising from***.....use or operation computer systems, etc.
2. Such use or operation must have been ***as a means for inflicting harm***...

3. The thing used to cause the spoofing must fall within one of: ***any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system***...

Electronic system

There is little doubt that a system which transmits a false GNSS/GPS signal or otherwise manipulates a vessel's onboard systems would fall within the broad definition provided for in point 3 above - in particular *any other electronic system*.

Directly or indirectly cause by or contributed to, by or arising from...

Under point 1, the insurers have the burden of proof of showing that the GPS spoofing has played a part in the causal chain leading to the loss. However, the question remains as to the degree of causal effect the spoofing must ultimately have had. Caused 'directly by' or 'arising from' are phrases relatively easy to deal with as they are legally akin to *proximately caused by*, a concept which marine practitioners are well versed in. If this was the only test, then it is suggested that the exclusion would not apply as the grounding would ultimately be either a marine peril or a shipowner could likely also point to some navigational negligence which allowed the grounding to occur.

However, the exclusion goes further to bring in situations in which the GPS spoofing has 'indirectly caused' or 'contributed to' the grounding. The words allow for insurers to rely on events in the causal chain, which may not be quite so immediate (or proximate) but which have certainly had some genuine effect on events. There is a useful analysis of these terms (or similar terms) in *Arc Capital Partners Limited v Brit Syndicates Limited [2016] EWHC 141*. Based on this widening of the causal 'net', we can see that it may be relatively easy for insurers to again reverse the burden of proof back to owners that spoofing has not had a significant role in a loss.

In such situations, it is perhaps difficult for a shipowner to rebut the insurers' reliance on the Cyber Exclusion, by pointing to the fact that the crew should have done better in terms of their reliance of navigational aids, etc. as the incorrect position reporting of the GPS spoofing is more often than not likely to have played some part in the decision making on deck.

In all cases an analysis of the specific facts would be required.

For example, it might be shown that a grounding was inevitable irrespective of any manipulation of the GPS system, simply by reason of inadequate passage planning or crewmembers having been asleep on watch, so that whether some element of spoofing had occurred is not material. Equally, the longer the spoofing occurs prior to the eventual casualty, the more opportunities would have been missed to have detect and counter the spoofing. At some stage, the spoofing should lose most (if not all) its potency so that it no longer plays a role in the causal chain. For example, and in view of the STCW provision cited above, if the spoofing occurs on one watch but the grounding does not occur until three watches later, there have been numerous points at which the real-time position and track of the vessel should have been checked independently of GPS.

Whether the spoofing still has enough of a causal connection to the grounding will be a question for the Courts based on the specific facts of every case.

Means of inflicting harm

Assuming that insurers have been able to demonstrate that the use of a computer system, etc. to spoof an insured vessel's GPS system has played a genuine causative role in a casualty, then they must finally be able to demonstrate that this was as "*a means of inflicting harm*" (point 2).

As this is an exclusion, the burden of proving this falls, initially, upon the insurers.

It is intuitive that anyone operating the electronic system which results in GPS Spoofing must intend some detrimental effect, or harm, will be felt by those targeted and, at best, indifferent to any impact it may have on those close by to the target who may be collaterally affected.

The exclusion does not specify any particular degree of harm that needs to be felt or that the harm needs to necessarily be physical damage. They may intend to just disrupt trade or inflict economic losses, etc.

It is in the nature of GPS Spoofing that it may be difficult, if not impossible, to positively identify the party responsible and, accordingly, their motives.

However, the overall context may be sufficient to give rise to a rebuttable presumption that the motives behind spoofing have harmful intent.

For example, if a vessel is sailing through a known high-risk area with increased political tensions when suddenly she experiences GPS spoofing, the Courts may take the view that there is a rebuttable presumption that the spoofer intended harm. It would then be for the assured to offer up a plausible alternative argument which supports the view that the spoofing was in fact not intended to be harmful (such as the spoofing was intended to try and disrupt the guidance systems of missiles or drones and which had no intent to cause harm (quite the reverse) but the ship becomes collateral damage).

On the other hand, if some random GPS signal disruption occurs whilst the vessel is not in a "hot spot" area of the world, then insurers will have a much harder task to show harmful intent was involved and would likely have to establish more specific details to support their case, e.g the identity of the perpetrators, the motivation, etc. - in such circumstances the bar to meet the burden of proof on harmful intent would be much higher.

In either case, we would suggest that the burden of positively proving harmful intent or denying it (if it can be inferred from the overall context of a casualty) may be quite difficult unless the responsible party identify themselves and provide their motivations (as is seen with terrorist groups claiming responsibility for bombing etc.).

Leena Mody **Joseph Shead** **Willum Richards**

ADR Panel
Association of Average Adjusters

9 July 2025