GLOBAL FINEX - CYBER & TMT

War exclusions in cyber policies: the important details

By Andrew Hill
Global FINEX Head of Cyber Coverage & Innovation, Cyber & TMT

June 2023

Executive Summary

Lloyd's minimum requirements for war exclusions used in standalone cyber policies underwritten by its members (Market Bulletin Y5381) has led some buyers of cyber insurance to question whether the value of the product has been materially compromised.

Why have Lloyd's introduced these changes?

Lloyd's are concerned that war exclusions traditionally used in cyber insurance policies do not adequately address the inherent systemic loss risk associated with cyber threats. A single cyber-attack that has a widespread impact across multiple organisations could, Lloyd's says, affect the insurance market's ability to pay any covered losses.

Given their resources, Lloyd's believes that nation states pose the greatest threat in terms of the development of malware capable of causing widespread, systemic destruction. It follows that Lloyd's requirements have a particular focus on nation state cyber activity, both in the course of war or independently of war.

What war exclusion is being used by Lloyd's members and how does it work?

The war exclusion, referred to as LMA5667A, has emerged as the most widely used of the war exclusions that meet Lloyd's guidelines. This exclusion excludes all losses arising out of war and cyber operations that are part of war. Cyber operations deployed by nation states outside of war may or may not be excluded depending on the specific facts. Only those losses arising from affected computer systems located in countries that meet the criteria for an "Impacted State" are excluded. This approach addresses the systemic loss concerns expressed by Lloyd's.

Controversy

While some buyers of cyber insurance have welcomed the greater clarity of LMA5567A (and its variants), others have questioned whether that clarity comes at the expense of cover. Specifically, some buyers argue the absence of clarity in the war exclusions that have been traditionally seen in cyber insurance policies could be used to the policyholder's advantage in the event of a coverage dispute.

Misconceptions

Owing to the complexity of LMA5567A, it is not surprising that misconceptions around the scope of cover have emerged. Perhaps the most notable of misconceptions to have emerged is that Lloyd's is no longer covering nation state cyber-attacks. This is inaccurate.

'Traditional' war exclusions vs Lloyd's model war clauses

'Traditional' war exclusions approach the issue of war and nation state cyber activity differently to the Lloyd's model war clauses. As such, it is invariably an over-simplification to suggest one approach to the war exclusion is 'better' for the policyholder than another.

In many cases, for those buyers of cyber insurance who have a strong view on the matter, it can come down to whether they prefer the approach widely used in these 'traditional' war exclusion over and above that used in Lloyd's model war clauses.

The WTW war exclusion

In response to some of the issues that have been raised in response to LMA5567A, WTW has developed its own war exclusion. It is largely based on LMA5567A, but introduces several amendments, including a carve back of cover for certain losses arising out cyber operations deployed in conjunction with war.

Reinsurance

Given that Lloyd's insurers are unable to use war exclusions that are non-complaint with Lloyd's guidelines and many non-Lloyd's insurers are happy to continue using those 'non-compliant' exclusions, it seems unlikely insurers are going to reach a consensus on the matter any time soon. It follows that the prospect of one war exclusion that every insurer is prepared to support is remote at the present time.

A significant proportion of the direct cyber insurance market is reinsured. Should those reinsurers, that have historically given terms that provide for back-to-back cover of the war exclusion in the direct cyber insurance policy, provide terms which are subject to a Lloyd's-compliant war exclusion, the emergence of a greater consensus on the issue arguably becomes a greater possibility.

Detailed Review

Introduction

War exclusions in cyber insurance policies have received considerable attention in recent months. The driver for this scrutiny is well-rehearsed – Lloyd's underwriting requirement that any war exclusion used in standalone cyber policies underwritten by its members must meet certain specified minimum requirements (Market Bulletin Y5381). In support of those requirements, the Lloyd's Market Association (LMA) published two groups of four model clauses (LMA5564 – LMA5567 A & B) in January 2023.

An overview of the LMA model war clauses

In essence, these LMA model clauses share a common approach to coverage for the following events:

1. **war** (a defined term);

2. **cyber operations** (a defined term) carried out as part of war; and

3. **cyber warfare** (i.e. cyber operations outside of war attributable to nation state that meet certain systemic event thresholds).

The model clauses adopt a scaled 'less cover to more cover' approach with LMA5564 excluding all loss arising out of the events specified in 1-3 above through to LMA5567, which excludes losses arising out of the events identified in 1 and 2 above, but does not exclude losses arising out of events at 3, provided the affected assets giving rise to a loss are not located in a nation state that meets the specified thresholds for cyber warfare.

The only distinction between the 'A' and 'B' versions of each LMA model clause is that the 'A' version includes language addressing attribution whereas the 'B' version is silent on attribution.

Controversy

While many organisations that buy cyber insurance have accepted the move across to the LMA model war clauses (specifically LMA5567 A/B), these clauses have not been universally welcomed by all insureds. A number of notable large institutional buyers of cyber insurance, for example, have questioned whether the LMA model clauses materially compromise the value of the cover.

The objections that are commonly raised can be broadly categorised as follows:

(a) The threshold points that determine whether a cyber operation falls within scope of 'cyber warfare' (see item 3 above) above are ambiguous – specifically the requirements that the cyber operation:

(i) disrupts at least one "Essential service" (a defined as *"a service that is essential for the vital functions of a state ..."*) in a nation state; and

(ii) the disruption of that "Essential service" leads to a "major detrimental impact" (not defined) on the functioning of that nation state; and

(b) the attribution clause in the 'A' versions of the model clauses (which specifies the standard of evidence insurers can rely upon in support of any attribution of a cyber operation to a nation state (see items 2 and 3 above)) leaves it open for insurers to rely upon evidence which may lack credibility (e.g. uninformed presidential tweets).

Of particular concern is the absence of a definition for the "major detrimental impact" threshold, which, critics argue, is too open to interpretation. The LMA has, however, stressed that the specific language used clearly captures the scale of impact required for the threshold to apply, thereby protecting insureds against the exclusion being invoked arbitrarily.

Misconceptions

While the objections noted above are not without merit, other concerns with the model clauses have been advanced, suggesting that certain concepts within the clauses may have been misinterpreted.

The most commonly aired of these misconceptions include:

(i) the LMA model clauses exclude all nation state cyber activity. This is incorrect. While it is true LMA5564 does indeed exclude all nation state cyber activity, this clause is rarely, if ever, used in cyber insurance policies (at least the ones WTW place on behalf of its clients). The more widely used LMA5567 A/B does not apply a blanket exclusion on the nation state cyber activity; and

(ii) the LMA model clauses provide no cover for insureds whose activities fall within the meaning of an "Essential service". Again, this is incorrect. The disruption of an 'essential service' is simply a threshold point that insurers must prove led to a "major detrimental impact" of the nation state at issue.

Other (non-LMA model) war exclusions

It should be stressed that, at present, only Lloyd's members are required to use a war exclusion that meets the guidelines outlined in the bulletin above. Most Lloyd's members have opted to use the LMA model clauses as published (although at least one Lloyd's member has opted to develop its own war clauses based on the principles of the model clauses). It follows that non-Lloyd's insurers are free to continue using whatever war exclusions meeting their own internal underwriting criteria.

While several insurers outside of Lloyd's have elected to use the LMA model clauses (or something similar), the most notable of which is Munich Re, many of those insurers have elected to use either their own modified war exclusion specifically for cyber policies (most notably, Chubb) or to continue using whatever war exclusion they have historically been comfortable with (AIG, for example). The majority of non-Lloyd's insurers are willing, however, follow the LMA model clauses on insurance programmes.

Are the historical issues with 'traditional' war exclusions flying under the radar?

Those insurers hitching their wagon to the 'traditional' war exclusion based on NMA464 (which dates back to the 1930s – i.e. long before the advent of cyber risk, and which was widely used by all cyber insurers prior to Lloyd's guidelines), have been able to offer an alternative to those insureds who are uncomfortable with the inclusion of LMA5567 A/B (or similar) on their cyber insurance programme.

However, while the spotlight is at present firmly on the LMA model clauses, in the interests of balance, it is important not to overlook the inherent ambiguity in many of those 'traditional' war exclusions which led to Lloyd's arriving at the position it's at today.

The LMA model clauses have certainly brought the scope of cover within cyber insurance policies for nation state cyber activity into greater focus. Broadly speaking, the majority of 'traditional' war exclusions are completely silent on such nation state activity. These exclusions typically exclude some or all of the following acts: (i) war, (ii) warlike operations, (iii) hostilities, (iv) military force and (v) terrorism. Generally speaking, these concepts are not defined, and are therefore capable of being interpreted widely (thereby potentially encompassing both physical and non-physical (i.e. cyber) acts.

'Cyber terrorism' is invariably a defined term and it has become standard practice to include a 'cyber terrorism' carve-back to the war exclusions. However, the definition does not always address whether 'cyber terrorism' encompasses nation state cyber activity. Moreover, the cyber terrorism carve back is almost always subject to its own carve-back, which states that the cyber terrorism carve-back shall not apply when such activity is used as part of 'war', 'military force' etc.

Any suggestion that 'traditional' war exclusions are better for insureds than, notably, LMA5567 A/B, is an over-simplification of the complexities associated with the war exclusion issue.

Losing the battle, but capable of winning the war?

It seems hard to dispute with the benefit of hindsight, that Lloyd's strategy for the roll out of the LMA's model war exclusions didn't go the way it had hoped. There are arguably three independent but related reasons for this:

1. While Lloyd's seemingly wanted to preserve its respective members' discretion to underwrite risk associated with nation state cyber activity, the publication of four and then later eight model war exclusions led to an almost unavoidable obfuscation of the messaging around the exclusions (suggesting that one model clause, i.e. LMA5567, would have allowed for clearer messaging);

2. The scope of the model war exclusions was too ambitious and complex to allow for an effective socialisation of the language across the full range of cyber insurance buyers. Focussing on LMA5567 A/B, as the most commonly used version, it seeks to address war, cyber operations in conjunction with war and cyber warfare (which, in turn, introduces thresholds built around infrastructure (i.e. "Essential services") and systemic risk (i.e. "major detrimental impact").

3. The two factors noted above contributed to a swathe of negative press coverage around Lloyd's strategy on war and nation state cyber activity. Moreover, because of the complexity associated with the model clauses, the press consistently misreported on the scope of the exclusions, which, in turn, caused uncertainty amongst some buyers.

Redressing the balance

In an industry that prides itself on relationships, it could certainly be argued that, notwithstanding Lloyd's ambitions to preserve the sustainability of the cyber insurance market, buyers of cyber insurance interests were not given sufficient weighting. **If those buyers determine there is not sufficient value in the cyber insurance products they purchase, this poses an equal, if not greater threat, to the future sustainability of the cyber insurance market.**

WTW has to date neither publicly nor privately formed any fundamental objections to LMA5567 A/B (or its predecessor), although the value LMA5564 – LMA5566 add to process is questionable. In several respects, LMA5567 A/B deliver much needed clarity (e.g. the inclusion of a definition of "war" and an affirmative position on nation state cyber activity), that should be welcomed. While taking a different course, Chubb has also attempted to deliver a war exclusion that is fit for purpose in the context of standalone cyber insurance.

The LMA model exclusions do not provide answers to all the key questions, particularly with respect to cyber warfare (e.g. the severity of a nation state cyber operation required to meet the "major detrimental impact" threshold), but then neither do the overwhelming majority of the 'traditional' war exclusions that remain in circulation. In an arena where we are still arguably waiting for an event to test the parameters of the war exclusion, it is perhaps unrealistic at this juncture to expect to arrive at a war exclusion that does provide all the answers.

The WTW approach

The proliferation of approaches adopted by different insurers to war exclusions has brought into sharper focus the value of a clear and accurate broking advisory service.

Providing cyber insurance buyers with the facts (as opposed to uninformed, unfounded, or broad-brush opinions) is critical to the process of allowing those buyers to make informed decisions.

Notwithstanding the layered complexities of the LMA model war clauses, they are capable of being broken down and explained to buyers in a digestible and understandable way. They can be compared and contrasted with 'traditional' war exclusions and other war exclusions specifically drafted for use in standalone cyber policies.

As already stated, **in many cases, any analysis which sets out to demonstrate one war exclusion is 'better' than another exclusion risks overlooking the finer nuances of such a comparison. WTW firmly believes that its approach of breaking down complexity puts the client at the centre of the decision-making process and gives clients confidence that the solution being purchased delivers value.**

The emphasis WTW has placed on understanding and accurately advising on the scope of the LMA model war clauses does not mean that WTW has simply accepted those clauses. In fact, WTW has drafted several variations to LMA5567A, which narrow and/or clarify the scope of the exclusionary language.

Notably, the 'WTW war clause' seeks to redress the balance of the LMA5567A in three material respects:

1. It introduces consistent causation language (i.e. "arising from" rather than "directly or indirectly arising from") across the clause, which is intended to limit the application of the exclusion beyond established principles of proximate cause;

2. It reinstates cover for cyber operations carried out in conjunction with war (e.g. the ongoing Russia/Ukraine conflict) where the losses arise from assets neither located in a nation state that is party to the war nor in a nation state that has suffered a "major detrimental impact"; and

3. It introduces the requirement that any evidence put forward by the insurer in support of attributing cyber activity to a nation state must be "credible".

Reinsurance

It would be misplaced optimism to suggest that the issues surrounding the war exclusion are likely to reach a settled resolution in the near future. This ongoing absence of a settled position on the scope of war exclusions may be further compounded by reinsurers (a significant proportion of direct cyber insurance is reinsured) who, until recently, have seemingly been content to provide terms to direct cyber insurers regardless of the war exclusion that is being utilised. Whether those reinsurers are content to provide terms for direct insurers that are prepared to support war exclusions that provide cover for cyber operations deployed in conjunction with war (see point 2 immediately above) moving forward remains to be seen.

Looking forward

While there continues to be an absence of consensus on war exclusions within the cyber insurance market, appetite for cyber risk transfer is as strong as ever and there remains a clear commitment within the industry to develop insurance solutions that deliver value to clients. WTW will continue to lead from the front in terms of advancing and accurately articulating our clients' interests on the issue in the marketplace, as evidenced by the WTW approach and the WTW war exclusion.

Contacts

Andrew Hill
Global FINEX Head of Cyber Coverage & Innovation, Cyber & TMT
T: +44 (0)203 124 8278
hillanx@wtwco.com

Jason Krauss
FINEX NA Cyber Thought & Product Coverage Leader, US
+1 212 915 8374
jason.krauss@wtwco.com

Benjamin Di Marco
Cyber and Technology Risk Specialist, ANZ
T: +61 478 312 988
benjamin.dimarco@wtwco.com

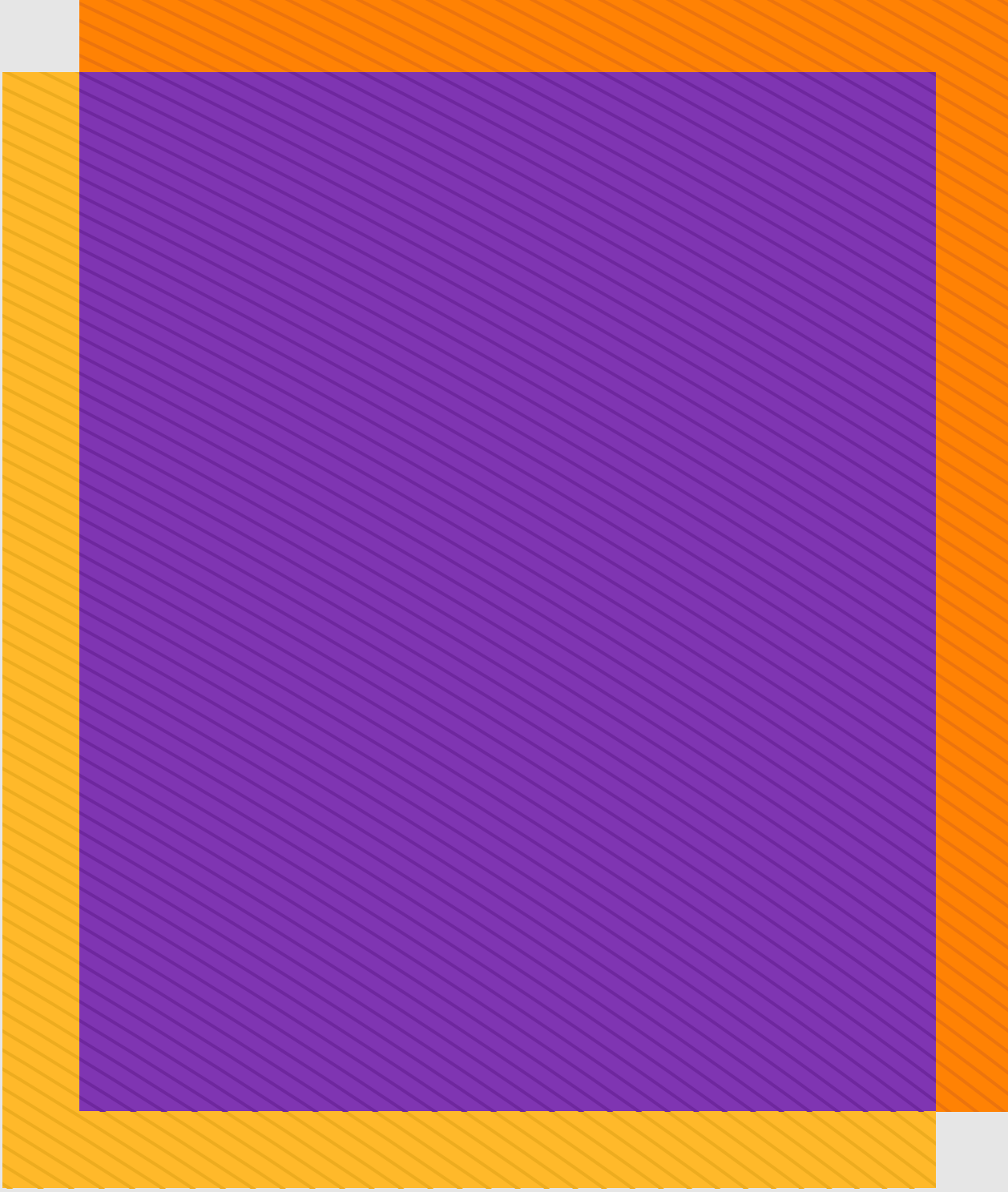
Elliot Boreham
Cyber Lead Associate, Asia
T: +65 6958 2544
elliot.boreham@wtwco.com

Michélle Lawson Hughes
Cyber Practice Leader, Canada
T: +1 416-646-3161
michelle.lawson@wtwco.com

Marcela Visbal
Regional Cyber Risk Product Leader Latin America
T: +57 1 742 4001
marcela.visbal@wtwco.com

Rodrigo Flores
Regional Cyber Manager, Latin America
T: +52 55 4383 8517
rodrigo.flores@wtwco.com

Laure Zicry
Head of FINEX Cyber, Western Europe
T: +33 (0) 6 73 92 89 16
laure.zicry@wtwco.com



About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organisational resilience, motivate your workforce and maximise performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

FPS4952039 WTW-FINEX 553603/06/23

wtwco.com