Cry cyber and let slip the dogs of war

Exploring the issues of attribution in the context of war and cyber
Preface

The following paper presents an objective discussion around some of the complex issues associated with the Cyber Peril, specifically in relation to war.

Our objective is to help the wider (re)insurance market better understand why the inability to easily attribute cyber losses following a cyber incident presents a real challenge to (re)insurers, and look at how the market has begun to address the issues.

We discuss the significance of the “Attribution Line”, the shortcomings of historical definitions of war and war exclusions, and why the role of the reinsurer is crucial in reaching a working and accepted solution, fit for the future.

This paper does not pretend to offer any definitive answers, but we hope that it will encourage a positive market dialogue, and we look forward to your comments and feedback.

Cyber is a peril, not just a class of business. The risk landscape has evolved and the historically well-defined line between excluded acts of war and otherwise covered perils has become blurred in the context of cyber. As a market it is our duty to redefine the boundaries to ensure that we are able to continue to provide certainty of cover to our clients.

Ian Newman  Global Head of Cyber, Capsicum Re
Introduction

A definitive line must be drawn between insurable cyber losses and uninsurable acts of war. The ambition of this paper is to help the (re)insurance market towards that goal.

The 2017 NotPetya cyber-attacks were purportedly carried out by state actors targeting Ukraine. In their wake, the debate surrounding the issues of silent, non-affirmative, embedded, and assumed cyber exposures has reached fever pitch. It is perhaps the single most widely discussed topic in the Property & Casualty marketplace.

NotPetya’s fallout has raised unresolved questions about what constitutes an ‘act of war’ in the context of cyber-attacks. The clash of NotPetya-related cyber losses with exclusionary language in respect of ‘war’, and the ensuing high profile litigation, has amplified the discussion, and revealed the real-world implications of this debate.

The main issue of war in the context of cyber stems from an attribution problem: the lack of either a credible or traditional identifiable party claiming responsibility for a cyber-attack, or the inability to determine the proximate cause of an event and/or a loss.

By their nature, it is almost impossible to determine the motivations and origins of the vast majority of cyber-attacks. The implication? The (re)insurance market cannot rely on traditional reference points such as time, location and attributable person(s) responsible.

This challenge becomes all the more contentious when cyber-attacks are suspected destabilisation plots orchestrated by state actors. As a consequence of this challenge it is the contention of this paper that the cyber peril has not only transcended traditional lines of business, but also that it challenges the very concept of war as the (re)insurance market historically has understood it, arguably rendering current war exclusionary language unfit for purpose.

“in the cyber space it is extremely difficult to attribute aggressive behaviour without doubt and even more difficult to pinpoint motivation. This in turn has led to difficulties in enforcing war exclusions in a fair manner. It is incumbent upon the insurance industry to demonstrate that it is not seeking an ‘easy way out’. Instead, we should be deploying our efforts to strive for contract certainty, and adapt war exclusions to reflect the realities of the modern world.

Likewise we must refrain from letting the pendulum swing to the other extreme, which would be to let war exclusions be weakened or even removed without having an alternative concept in place. If we think of the intrinsic value of insurance as the promise to pay valid claims, it would be unethical for underwriters to make financial commitments that the balance sheets of private companies are incapable of meeting."

Anthony Cordonnier  Head of Cyber Product Management, Swiss Re and Chair of the Cyber Reinsurance Committee, International Underwriting Association

“The potential impact from a large scale cyber-attack is now catastrophic due to the increasing interconnectedness of, and reliance on, the digital world. Additionally, due to the well-known difficulties around attribution, cyber-attacks are currently very low consequence (and therefore very appealing) endeavours for states wishing to do harm to their enemies.

The insurance and reinsurance communities must work together to prepare for the eventuality of cyber war by proactively creating fit-for-purpose exclusions that appropriately ring fence the loss potential to ensure the long term sustainability of the market.”

Devin Page  Head of Specialty, Hiscox Re
Framing the issue:
The grey band of attribution uncertainty and the attribution line

Traditionally an act of war goes beyond the realm of insurable interest. As such, attribution, whereby the parties involved are readily identifiable, becomes a critical test of whether indemnity can or cannot be provided following a cyber attack.

With subterfuge, misinformation and third-party proxies, this test can seem fluid. In order to resolve this issue, the market must strive to agree a line at the crossroads between the unattributed and the attributed. We will call this crossroads the ‘Attribution Line’.

If the challenge of attribution prevents the market from clearly delineating between state-sponsored attacks and simple criminal or otherwise-malicious cyber events, then we are duty bound as a (re)insurance market to focus on redefining what constitutes an ‘act of war’ and a ‘state of war’ in the context of ‘Cyber as a Peril’, as illustrated in Figure 1.

The single critical requirement that must be fulfilled for an attack to cross the Attribution Line is that the responsible party must be identifiable. At the most basic level, this must constitute identification of the responsible person or persons that represent the party, and the party’s physical location.

It follows that an ‘act of war’ can only be identified when it is recognised as such by the person or persons representing one or another of the parties themselves (whether the aggressor or the victim of the attack).

When these conditions are met, a loss event which was territorially ambiguous at the point it crossed the Attribution Line becomes a territorially explicit act attributed to a specific party.

We contend that when considering war, when a cyber attack crosses the Attribution Line, the line between an insurable cyber attack, and an uninsurable act of war is also crossed.

Grey band of attribution uncertainty

<table>
<thead>
<tr>
<th>Non-malicious cyber incidents</th>
<th>Malicious attacks, terrorism</th>
<th>Suspected state sponsored cyber attacks</th>
<th>Cyber crime, vandalism</th>
<th>(Cyber) Act of war</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grey band of attribution uncertainty</td>
<td>Attribution line</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1
Insuring cyber risk

The cyber insurance market has remained focused on end clients – insureds – and determined that it is willing, or at the very least required by those insureds, to provide indemnification under cyber heads of cover after a cyber attack, even when an attack cannot be attributed to a specific party.

The key issue for the cyber market, in the context of this paper at least, arises when cyber heads of cover are not clearly defined. It can also be unclear if cover has been granted under write-backs, such as for cyber terrorism (which often contradict a war exclusion), or indeed when no war exclusion has been specifically inserted.

For the wider P&C insurance market, the issues are more fundamental. The very question of attribution is arguably indicative of a general lack of understanding of the rapidly changing cyber exposures under traditional lines of business. Current high-profile litigation highlights not just potential shortcomings of existing cyber policies, but explicitly reveals the failure of traditional all-risk property policies to adequately address the cyber peril, even with an endorsement.

In this instance it is all too easy to focus on those risk managers or insurance brokers who have pushed for broader terms of coverage (or silence on cyber coverage) which has ultimately led clients into litigation or worse, being left without appropriate cover/limits.

We advocate for a renewed focus on ‘cyber as a peril’, and consideration of where in the insurance universe cyber can, could, or should be covered. Illustrated in Figure 2.

Cyber as a peril: Understanding the threat

![Diagram of the (re)insurance market: all lines of business](Figure 2)
Consequences of the current approach: The challenge of attribution

As discussed above, the issue of attribution can become contentious when the involvement of state actors is suspected. Logically, however, if the market opts to refuse or reduce cover for state-sponsored attacks (whether proven, claimed, or otherwise suspected), the heads of cover would be of far less value. This is especially perilous to the emerging cyber insurance marketplace whereby the effect would be much the same if cover was limited or refused for attacks perpetrated by organised crime syndicates.

Outside of the actual war market, no (re)insurer, and critically no end client, expects their policy to extend to provide indemnity for losses resulting from an undisputed act of war, whether cover is being given specifically under cyber heads of cover or not.

There is an argument, however, that the best solution would be to remove war exclusions entirely, thereby removing any and all ambiguity.

Nonetheless, in the absence of a dedicated cyber war market, and until markets such as Lloyd’s and the large European reinsurers are prepared to accept cyber war risk onto their balance sheets, some form of cyber war exclusion will always be required by the (re)insurance market.

“One of our challenges as a market is to address an ill-informed perception that the cyber insurance product is overly complex. In order to do so, we must seek to avoid introducing exclusions which can be either imprecise or differently interpreted. Attribution in the context of War Exclusions is one such problem, which the market would do well to prevent by precisely defining the circumstances when it may be applied.”

Matt Northedge Managing Director, AmTrust Cyber Risks

“Given the current absence of judicial precedent, coupled with a high evidential barrier to attribution, it is of utmost importance that reinsurance contracts are as clear as possible as to the extent of coverage afforded for cyber losses from war, however defined. In order to increase contract certainty, some reinsurers may be willing to limit explicitly the scope of the blanket war exclusions presently found in many non-proportional cyber treaties. By doing so, such reduced ambiguity would not only align treaty wordings with the underlying policy forms, but also as a direct corollary minimise both the frequency and severity of post-loss disputes.

However, the provision of broader coverage for a peril as systemic and potentially catastrophic as this will come at a cost, both in terms of pricing and aggregate management/reporting. As such, alongside any provision of broader coverage, even if only de jure, cedants must also develop systematic methods of identifying and quantifying vulnerabilities to the peril itself and determining suitable PMLs, which will help improve their own understanding and pricing of their exposure.”

Rob Ashton CEO, Radius
The issue itself:
Defining acts of war

When considering the Attribution Line, it is essential to define what constitutes an act of war.

Please note that we do not suggest that this is a full exploration of what might be considered ‘war’, nor are we suggesting that this definition should be accepted unequivocally.

**War is considered to be:**

“A state of **armed conflict** between two or more parties. It is generally characterized by extreme violence, aggression, destruction, and mortality, using regular or irregular military forces.”

“**Warfare** refers to the common activities and characteristics of types of war, and Total war is warfare that is not restricted to purely legitimate military targets, and can result in massive civilian or other non-combatant suffering and casualties.”

**A ‘declaration of war’ versus a ‘state of war’**

Albeit without reference to a body of academic rhetoric and historical evidence, we argue that a ‘declaration of war’ need not be a prerequisite to the existence of a ‘state of war’. For example, the Vietnam conflict was undeclared but almost certainly constituted a war in practice and tactics.

In reference to the definitions of war above, we also question whether a declaration should be considered a defining circumstance of War.

We contend that an ‘act of war’ can be carried out only by parties in a ‘state of war’, and furthermore that the associated armed conflict must fulfil some if not all of the associated characteristics of ‘war’.

Clearly the definitions of war and warfare used here have been framed in the context of conflicts humanity has experienced to date. We argue, however, that weaponized non-physical assets, for example covert, coded intelligence networks, and internet infrastructure, such as cloud service providers and their associated server farms, could and should be included as legitimate ‘military targets’. We would also not exclude their use from the ‘common activities’ of warfare.

We argue this recognizing that the impacts of cyber-attacks may not be among those that have traditionally been associated with the characteristics of war as defined above, that is, ‘extreme violence, destruction, bodily injury, and mortality.’

Finally, we note that the motivations for war do not form part of any definition of war itself, nor does attribution require any specific motivation to be identified.
Knock on consequences:  
Addressing the issue of escalation

We accept that qualification as an ‘act of war’ requires either a) the simultaneous escalation to, or b) a pre-existing ‘state of war’ between two or more parties.

Many would argue that a ‘state of war’ need not be declared in order for an ‘act of war’ to be carried out, or that upon the declaration of war, events leading up to it could retrospectively be considered ‘acts of war’.

Logically however, during the period of escalation, when attribution remains indeterminate and when the Attribution Line has not been crossed, it is untenable to deny cover on the basis that an event occurring during this period is considered an ‘act of war’. Denial is tenable only when a loss or another, or a ‘state of war’ has been recognised.

Prior to this point, hostile acts are simply that. The cyber reinsurance market should be prepared to provide reinsurance on this basis.

**What constitutes cyber warfare?**

Within the above-stated definitions of war, activities involving the use of the internet and non-physical assets could be considered ‘cyber warfare’, but should be referred to as such only where and when a ‘state of war’ exists.

**Recognizing a state of war:  
The kinetic assumption**

It is commonly assumed that in order for a ‘state of war’ to exist, physical assets must be active and mobilized. This so-termed ‘kinetic military action’ is increasingly associated with war rhetoric, particularly in the direct cyber market, which we discuss below.

We do not dispute this position, but simply suggest a potential ‘what if?’ scenario: what if a declaration of war is made and a ‘state of war’ arrived at, without the mobilization of any physical assets? The ‘aggressive’ use of ‘cyber military forces’ could result in ‘massive non-combatant suffering’. Consider, for example, taking out a city’s power for a prolonged period, or an attack that crippled critical healthcare providers’ infrastructure. Both could lead to civilian suffering and even mortality.

While a ‘state of war’ is extremely unlikely to be recognized until ‘kinetic military action’ occurs, we believe it is important to appreciate the nuances of the possibilities to inform discussion. For example does Russian action in Ukraine in fact constitute war?

---

**Cyber terrorism:  
Is the term relevant?**

‘Cyber terrorism means any actual, alleged, suspected or threatened attack against a Computer System or a threatened Security Incident, both with the direct or apparent intention to cause harm and further social, ideological, religious, economic or political objectives, and/or to intimidate any person(s) or entity in furtherance of such objectives.’

The preceding definition is commonplace in cyber insurance contracts, primarily as a write-back to many war clauses. When one considers the cyber peril, it is difficult to depict definitively a cyber-attack scenario which couldn’t feasibly be described as cyber terrorism under this definition.

Furthermore, with direct reference to our ‘grey band of attribution uncertainty’, we argue that the term itself is irrelevant in the context of delineation of insurable cyber attacks and uninsurable ‘acts of war’.

As alluded to earlier, cyber terrorism write-backs contradict the war exclusion in almost all original policies. It remains unclear how insurers would respond to a NotPetya-like loss which is systemic across portfolios.
Capsicum Re’s challenge to the status quo

The goal of this paper is not to redefine the market. Instead our aim is to provide a framework for discussion, so the market can begin to resolve this issue.

Cyber-insurance markets are yet to clarify what they offer by often failing to adequately include or exclude cover for war; we suggest that the reinsurance market has an opportunity to determine what the exclusion and coverage should look like.

The status quo: A “hard war” exclusion

Firstly, we ask the reader to consider a traditional war exclusion, which arguably remains the status quo.

“Notwithstanding anything to the contrary contained herein this Policy does not cover Loss or Damage directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), hostile acts of sovereign or government entities, civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority.”

Second, based on our market experience to date, and in the interests of inciting an objective discussion, this paper considers two alternative war exclusion policy language possibilities, which are perhaps more suited to tackling the issue of war in the context of the evolving Cyber Peril.

The assumption

Purchasers of cyber insurance may operate from more than one territory, with interlinked Information Technology & Operating Technology systems spanning continents. However, they invariably maintain physically recognised domiciles for their P&L centres, making each and every one of them a definable party with a verifiable location (and coincidentally, but not insignificantly, a target for attack).

1. Reinsurance-led war exclusion

This clause is in current use (albeit with a preceding paragraph which excludes losses incurred when war has been declared). It remains consistent with existing policy language but without introducing distracting terminology such as cyber terrorism. We still however believe that there will be improvements to be made, and greater clarity of coverage provided, as the discussion develops between markets, brokers, and clients.

“Loss, liability, cost or expense, or any other amount incurred by or accruing to the Reinsured directly or indirectly arising out of, originating from, resulting from, caused by and/or contributed to by, regardless of any other cause contributing concurrently or in sequence to the loss or otherwise in connection with acts of war, civil war, invasion, insurrection, civil uprising or military or usurped power when there is no declaration of war. This exclusion is only applicable:

(i) if these acts are part of, directly connected to, or in support of kinetic military action; and

(ii) to original interests located and/or domiciled within the nation state(s), where such nation states are directly executing or being positively targeted by the kinetic military action.”
Capsicum Re’s challenge to the status quo

2. Cyber–centric war exclusion

Alternatively we propose what is a ‘fresh look’ option which avoids traditional insurance–led definitions of war as well as potentially misleading and ambiguous references to cyber terrorism and focuses on the issue of attribution:

((i)) PARTY shall mean a sovereign country, government or nation–state recognised as such by the United Nations.
((ii)) A STATE OF WAR shall follow either an official declaration of WAR by a representative of a PARTY or upon affirmative KINETIC MILITARY ACTION by one of the PARTIES, whichever occurs first.
((iii)) KINETIC MILITARY ACTION shall mean military action involving active physical warfare, usually, but not necessarily, including lethal force.
((iv)) CYBER LOSS shall mean losses covered under original policies [falling within the Class of Business / allocated by the Reinsured to its Cyber account].

Conclusion:
Attribution, the unavoidable issue

We believe that attribution presents the most uncertainty in the (re)insurance of risks exposed to the cyber peril.

We conclude by acknowledging that even where a recognised ‘state of war’ exists, attributing specific cyber attacks to an aggressor may still present a challenge. For example, if State A and State B are at war, and a company domiciled in State B suffers a cyber attack but even so State A denies responsibility for the attack, and instead points the finger at neutral State C, the issue of attribution clearly remains.

Nonetheless, we contend that the market’s confidence as to the position of the Attribution Line will greatly improve with advancements in policy language such as that proposed above, which will ultimately ensure greater certainty of cover.

Finally, we believe it is the reinsurance market that now has the opportunity to drive advancements and instill good and appropriate market practice, not just in relation to the issues of war, but in all aspects associated with the preeminent cyber threat.

Note: We do not expect either of the two exclusionary language possibilities above to be met with unanimous conformity. However, we hope that they will serve as a step towards that end by encouraging a sensible, productive dialogue between markets, brokers, and clients, while simultaneously promoting a mutual improvement in understanding of this highly contentious topic.