Liberty Specialty Markets

UNIQUE PERSPECTIVES

CYBER

# DRAWING THE BATTLE LINES – WHEN DOES A CYBER ATTACK BECOME WAR?

The scale and pace of the WannaCry and Not-Petya attacks demonstrated very powerfully the gravity of the cyber threat facing modern society. Such attacks are frightening enough when perpetrated by a misguided teenager in a bedroom; but when the spectre of state sponsorship is raised, the insurance industry starts questioning whether they should be classified as an act of war. Liberty Specialty Markets (LSM) examines the issues.

**Author**
Matthew Hogg

*Vice President and Underwriting Manager & Chair of LSM's Cyber Underwriting Group*

**Office**
London

It has been estimated that the average financial impact on an organisation in the UK can be as much as

**£7.21m**

rising to over $17m in the US.

## Increasing suspicions of state involvement

Both the WannaCry and Not-Petya attacks impacted a wide range of state-owned organisations, including variously the UK's NHS, Ukraine's national airport, plus power grids, nuclear power stations and numerous commercial organisations all around the world. In the case of the latter, it has become apparent that what was originally perceived as a ransomware attack for financial gain was probably something much more sinister. Media reporting increasingly suggests that Not-Petya was a state-sponsored attack on the Ukraine and that commercial organisations impacted by the virus were mere 'collateral' damage.

This damage can be significant. It has been estimated that the average financial impact on an organisation in the UK can be as much as £7.21m[1], rising to over $17m in the US. These types of losses are potentially covered by cyber insurance policies.

However, if proved to be state-sponsored or a declaration of war, many of these policies could be subject to broad war exclusions, stranding the affected organisations with no useful cover. Policies that have war exclusions, or which are silent on state-sponsored acts, without a war declaration, bring more certainty to the insured, but complexity and aggregation uncertainty to an insurer.

## When is an attack an act of war?

There are two important factors to be explored:

- What is the definition of war linked to cyber war and terrorism?
- To what extent can an attribution be made to a specific attack and the actions of a foreign government?

Unsurprisingly, the answers are not clear cut.

For example, the US government's definitions of cyber war and cyber terrorism, though vague, are important as the US is the most advanced market in terms of this cover. Definitions made here provide a reference point for considering whether a war and terrorism exclusion would apply to a cyber liability policy.

Over the past few years, the US government's stance on what kind of cyber attack constitutes an 'armed' attack has evolved, but still leaves the matter open to interpretation.

1. Ponemon Institute Cost of Cybercrime study, October 2016: http://tinyurl.com/y8qf6g5j

The problem lies in the fact that there is no definitive statement on how to treat cyber attacks because they do not use traditional weapons – such as bullets and bombs – even though there is no doubt they can inflict significant and widespread physical injury and property damage. For example, if a cyber attack caused destruction to major infrastructure or created a widescale threat to personal medical data putting lives at risk, it could possibly constitute an armed attack.

## Where to draw the line?

Although most cyber liability policies typically contain a war exclusion, the challenging issue of trying to identify the source of a cyber attack remains. Insurers bear the burden of proving whether an attack was state-sponsored, which is often time-consuming, costly, impractical and carries the potential risk of political interference. At times it can be borderline impossible, depending on the jurisdictions involved and sophistication of the attack.

> "Brokers and insureds have been keen to suggest that insurers remove war exclusions from cyber policies, or at least limit their use to circumstances where there has been an official declaration of war."

Despite these reservations, most cyber insurance policies now expressly cover cyber terrorism. In a further welcome clarification, US companies are more likely to get some relief for terror attacks related to cyber following the decision last year to expand the scope of TRIA (the Terrorism Risk Insurance Act), which provides a federal 'backstop' for claims related to acts of terrorism.

Pool Re has just announced it has received backing from the UK government in principle to remove cyber terrorism exclusions on property damage, and that from April 2018 it hopes to be able to include war and terror-related cyber-attack coverage for major property damage claims created by such an attack. However, it should be noted that neither TRIA nor Pool Re have been tested in relation to cyber incidents.

Brokers and insureds have been keen to suggest that insurers remove war exclusions from cyber policies, or at least limit their use to circumstances where there has been an official declaration of war. While this might seem like a simple resolution to the problem, the issue remains that many events which are widely considered to be war by society at large are not classified as such by the governments involved. US troops are regularly in combat round the world, yet there have only ever been 11 congressional declarations of war in the history of the US. So, it would have to be an exceptional incident to compel a government to make a declaration of war.

The bottom line is that clients are looking for cyber war and terrorism coverage to be included to avoid the risk of loss from contingent physical or financial damage caused by an act of war, a terrorist act, or a cyber attack on their country or its critical national infrastructure.

Insurers therefore need to decide what level of risk they can accept, and then draft war exclusions accordingly. For example, they may wish to expressly address the status of various data and networks. One area for consideration might be medical data and medical computer networks, as damage to medical information and data systems in critical national infrastructure could be considered an armed attack.

## Clarity through evolution?

The reality is that cyber attacks are not going away. This crime continues to escalate year-on-year so there are no grounds to hold out hope for a turning of the tide in 2018. The issue of whether an attack constitutes a declaration of war will not be solved overnight.

Ultimately, in much the same way as legal actions generate new case law, so repeated cyber attacks should lead to a greater degree of clarity. As more organisations find themselves the subject of online assaults, so the boundaries of cover and the strength of the various exclusions will be tested. In some cases, our traditional methods of dealing with definitions of war may be found wanting; then we will need to regroup and invest time in reviewing our modes of operation. At LSM, we consider it prudent at this point in time to side with a well-considered war exclusion clause.

The war against the cyber villains remains in its infancy. However the battle for clarity and to ensure our clients retain their faith in the insurance industry's protection needs to be won.

> "Cyber crime continues to escalate year-on-year so there are no grounds to hold out hope for a turning of the tide in 2018."

**GET IN TOUCH**
**Tel: + 44 (0)20 3758 0368**
**Email:matthew.hogg@libertyglobalgroup.com**
**libertyspecialtymarkets.com**