CYBER ATTACK NOT WITHIN WAR EXCLUSION

Appellate Division of the Superior Court of New Jersey decides the 2017 NotPetya malware attack did not fall with the 'hostile or warlike' acts exclusion in 'All Risks' property insurance cover

One purpose of war exclusions is to protect the solvency of insurers and, in turn, their ability to pay claims. Risks of that nature can impact a wide range of insured sectors or types of insurance policies at the same time and therefore aggregate very large claims.

In our May 2022 article It's War - But Not As We Know It, we considered the development of war and hostilities exclusion clause wordings and the decision in *Merck v ACE & others*.

The Appellate Division of the Superior Court of New Jersey ("the Appellate Division") published its decision in May 2023. We consider here its reasoning and the need for a clear exclusion that caters for the rapidly developing nature of risks presenting in the current world order.

Background

The pharmaceuticals company, Merck, was one of a large number of companies affected globally by the malware known as NotPetya. In 2017, it damaged over 40,000 of Merck's computers via accounting software originating in Ukraine and was widely alleged to have been orchestrated by actors for or on behalf of the Russian government. Indeed, in October 2020, a federal grand jury in Pittsburgh indicted six Russian Federation nationals, all officers in the Russian main Intelligence Directorate.

NotPetya spread to over 60 countries, including Russia. Within the first 5 minutes of its infection, about 20,000 of Merck's computers were impacted, which gives some sense of the scale and gravity of the attack.

Merck claimed under its 'All Risks' property insurance and the insurers declined cover, relying on the 'hostile or warlike' acts exclusion.

At first instance, Merck argued successfully that the malware attack did not come within the 'hostile or warlike' acts exclusion. The Court found that *"cyber attacks of various forms, sometimes from private sources and sometimes from nation-states … have become more common. Despite this, Insurers did nothing to change the language of the exemption to reasonably put this insured on notice that it intended to exclude cyberattacks"* and the insurers having *"failed to change the policy language, Merck had every right to anticipate that the exclusion applied only to* ***traditional*** *forms of warfare"* [our emphasis].

Merck argued successfully that the nature of the attack upon them did not comprise a traditional form of warfare, despite the wording of the exclusion not including the word 'traditional' (the terms of the exclusion can be found here). The insurers appealed.

Insurers' Appeal

By the time the appeal was heard, the claim value in issue was just under US $700 Million, and involved eight insurers. Additional interested parties also made representations given the potential ramifications of the case and the absence of cyber attack findings on which the decision could rely.

In pursuing the Appeal, insurers asserted that 'hostile' should be *"read In the broadest possible sense, as meaning "adverse," "showing ill will or a desire to harm," "antagonistic," or "unfriendly." According to the Insurers, any action that "reflects ill will or a desire to harm by the actor" falls within the hostile/warlike action exclusion, as long as the actor was a government or sovereign power, in this case the Russian Federation."*

The Appellate Division did not regard the plain language of the exclusion as supporting this argument, and ultimately favoured the insured.

The Appellate Division concluded *"the exclusion of damages caused by hostile or warlike action by a government or sovereign power in times of war or peace requires the involvement of military action."* It was not willing to stretch the meaning of "hostile" in an attempt to apply it to a *"cyberattack on a non-combatant firm that provided accounting software updates to various non-combatant customers, all wholly outside the context of any armed conflict or military objective".*

The Judgment usefully considered the history behind the war exclusion, noting that property policies always contain an exclusion similar to the hostile/warlike action exclusion that had first appeared in the 1950s. It noted that previous cases on war exclusions "*demonstrate a long and common understanding that terms similar to "hostile or warlike action" by a sovereign power are intended to relate to actions clearly connected to war or, at least, to a military action or objective."*

CPB Comment

The US approach (similar to that in England) is that exclusion clauses in insurance policies should be interpreted narrowly.

Although it was strongly suspected that the NotPetya malware attack was attributed to Russia, whether or not Russia was responsible or accountable was not key to the outcome. Instead, existing principles of construction of the insurance contract, the context in which it was written and the history of the development of exclusion clauses were central in the Court's approach.

Having decided that the exclusion clause could not fairly be applied to the NotPetya malware attack, the Appellate Court decided that the insurers' request to *"delineate the exact scope of what cyberattacks might be encompassed under the hostile/warlike exclusion"* was beyond the scope of its role.

This Judgment sets down a marker that a state-sponsored cyber attack targeting another state would not be sufficient, in itself, to fall within a traditional war exclusion. Clear wording would be needed if that were the intention of the parties to the insurance contract.

The potential effects of a cyber attack could be widespread and include property damage, bodily injury or death. In the case of the NotPetya attack, the Appellate Division noted there was no evidence that it caused bodily injury or death. However, when updating policy exclusions and/or devising standalone cyber insurance products, the potential range of ramifications needs to be carefully thought through.

Interest in this decision is, perhaps, more widespread than usual because the global insurance industry has been working hard to develop cyber policy wordings and war exclusions to address the growing prevalence of cyber attacks and to improve clarity in insurance wordings. In the UK, the Prudential Regulation Authority (PRA) wrote to all insurers in January 2019 to reinforce its' expectation that all insurers should have action plans to reduce the unintended exposure that can be caused by non-affirmative cyber cover (sometimes referred to as 'silent cyber'). 'Silent cyber' was initially used to describe cyber-related losses stemming from insurance policies that were not specifically designed to cover cyber risk, leading therefore to insurers paying claims for cyber losses arising under a policy not designed for that purpose.

Lloyd's, too, responded. On 4 July 2019, Lloyd's Market Bulletin Y5258, announced that the market should adopt best practice. For first-party property damage policies incepting on or after 1 January 2020, Lloyd's underwriters were required to ensure that all policies affirm or exclude cyber cover, and in relation to liability and treaty reinsurance it was proposed that there should be a 'phased-basis' implementation, following further consultation.

On 16 August 2022, Lloyd's Market Bulletin Y5381 set out new requirements for Lloyd's syndicates with standalone cyber attack policies for cyber liability (risk code CY) and cyber property damage (risk code CZ). First, unless agreed by Lloyd's, from 31 March 2023 these cyber attack policies need to exclude liability for losses arising from any state-sponsored cyber attack (in accordance with specific listed requirements - it is not an absolute exclusion regardless of the scale) and, secondly, there must be a war exclusion (either within that clause or separately). Y5381 sets out the minimum requirements, in further detail, such as having a robust method for how the parties agree on attribution to one or more states. Attribution is often a thorny issue in practice.

More recently, on 20 January 2023, the LMA Cyber War working group published replacement clauses to the four model exclusion clauses published in November 2021, mentioned in our May 2022 article. The 20 January 2023 clauses contain 'A' and 'B' versions. The 'A' versions meet the requirements of Lloyd's Market Bulletin Y5381 in relation to standalone cyber attack policies under risk codes CY and CZ. The 'B' versions differ as they do not address attribution and consequently are non-compliant without prior agreement from Lloyd's.

Even more recently, on 8 June 2023, Lloyd's stated that it would require syndicates to increase capital for cyber war coverage that falls outside the wordings deemed in line with the Y5381 requirements.

There has certainly been pressure from brokers for insurers to include state-sponsored cyber attacks within cyber terrorism carve-backs, in order to respond to the concerns about the increasing risks in

the modern world. However, clarifying what would be covered as a state-sponsored cyber attack and what would amount to uninsurable 'cyber war' is complex where the cyber landscape is continually evolving. In a similar vein, what amounts to terrorism and the point at which it would be regarded as war also gives rise to prospective coverage difficulties for insurers and policyholders alike.

June 2023

Any questions

If you have any questions regarding the insurance-related issues highlighted in this article, please get in touch with Helen or Lisbeth.

The challenge of cyber risks was one of several topics that were debated during the Insuralex global network annual seminar on 15 June 2023 by CPB's partner, Bernadette Bailey, and her fellow panel members. Please follow Carter Perry Bailey LLP and Insuralex on LinkedIn in order to receive information about invitations for future events and to receive future Insuralex reports.

Helen Tilley
Partner

T: 0203 697 1910
M: 0750 182 5588
helen.tilley@cpblaw.com
LinkedIn

Lisbeth Poulsen
Solicitor / European Qualified Lawyer
T: 0203 697 1905
M: 0782 346 7563
lisbeth.poulsen@cpblaw.com
LinkedIn

You can review a range of articles on similar insurance and reinsurance related topics in the Publications section of our website.

If you did not receive this article by email directly from us and would like to appear on our mailing list please email tracy.bailey@cpblaw.com