Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

'Act Of War' Questions In Cyberattack Insurance Case

By **Daniel Garrie and Peter Rosen** (April 23, 2019, 3:21 PM EDT)

Daniel Garrie

Peter Rosen

Recently, Mondelez International Inc. sued Zurich American Insurance Co. for denying coverage, under its all-risk property policy's war exclusion, for Mondelez's alleged over $100 million in losses caused by the NotPetya ransomware attack in 2017. This case has the potential to make a significant impact on the cyber insurance market as it is the first time the war exclusion has been litigated in the cyber insurance context and highlights some key issues in applying traditional policy language to cyberattacks.

Does the war exclusion apply to cyberattacks? If so, can Zurich prove NotPetya came from a state actor given the challenge of attributing cyberattacks?

Mondelez was one of dozens of companies to suffer damages during the global NotPetya ransomware attack in 2017. The attack caused $10 billion in damage, according to the U.S. Department of Homeland Security.

Mondelez submitted a claim under its property policy with Zurich that covers "physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the malicious introduction of machine code or instruction." The policy also covered nonphysical losses and expenses caused by the failure of "electronic data processing equipment or media to operate" due to malicious cyber damage.

Eleven months after the claim was filed, and after negotiations, Zurich denied the entire claim on the grounds that the ransomware attack was a "hostile or warlike action" by a "sovereign government or power, military force or their agents" and as such was excluded from coverage under the policy's "act of war" exclusion.

Mondelez then sued Zurich in October 2018 for breach of contract in Illinois state court, in Chicago. Mondelez alleged that courts, insurers and companies have previously applied the "act of war" exclusion only to conventional, physical armed conflict and cyberattacks, such as NotPetya, are not specifically addressed in the policy. Mondelez further alleged that it is Zurich's burden to show that the exclusion extends to cyberattacks and that NotPetya is considered an act of war under its policy.

The relevant portion of the "act of war" exclusion of the policy reads as follows:

> B. This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
>
> […]
>
> 2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any: (i) government or sovereign power (de jure or de facto); (ii) military, naval, or air force; or (iii) agent or authority of any party specified in i or ii above.

It should be noted that this language covers a broad range of activity that would fall below the threshold for an "armed attack" under the international law of armed conflict. If the court finds that this exclusion applies to cyberattacks, the nature of the attack would almost certainly fall within the exclusion as it would be difficult to argue that NotPetya was not "hostile."

The real question then is whether the action was taken by a state actor. Traditionally, this was an easier question to answer than it is now because most hostile or warlike actions by state actors were physical actions, and thus easier to attribute. However, cyberattacks are almost impossible to attribute with complete certainty.

While it has yet to answer Mondelez's complaint, Zurich will likely attempt to support its denial of coverage by pointing to the fact that in February 2018, the United States, the United Kingdom, Canada and Australia all officially blamed Russia for NotPetya, with the White House referring to it as "part of Russia's effort to destabilize Ukraine." However, it could be difficult for Zurich to put forward technical evidence conclusively attributing the attack to Russia.

According to some cyber warfare commentators, "[o]ur legal and policy frameworks for responding to cyberattacks cannot work unless we have adequate attribution; these frameworks remain incomplete because we lack the basis [sufficient attribution] to actually use them."[1] The Mondelez case highlights the applicability of this concept to the still nascent cyber insurance market. Traditional "act of war" exclusion frameworks are extremely difficult to apply to cyberattacks due to this attribution issue. Further complicating the issue, oftentimes cyberattacks executed for the benefit of a state are actually put into action by citizens, making it even more challenging to determine the state actor's role in the attack.

The outcome in the Mondelez case, especially with respect to how the court interprets and the trier of fact applies the "act of war" exclusion to the NotPetya ransomware attack, could have significant impacts on the cyber insurance market.

Even if the court finds that the exclusion is applicable to cyberattacks as a matter of law, it is possible that the exclusion would not, from a practical perspective, apply to cyberattacks due to the near impossibility of exact attribution. This would force insurers to rethink their approach to war exclusions in property and cyberrisk policies and could set off a massive rewriting of policy language. The outcome of Mondelez could also affect premiums, deductibles and limits as insurers reassess exposure considering the applicability, or inapplicability, of the war exclusion.

Daniel B. Garrie is a neutral at JAMS. He is managing partner at Law & Forensics LLC and a partner at Zeichner Ellman & Krause LLP.

Peter Rosen is a neutral at JAMS. He teaches insurance law at USC Gould School of Law and Pepperdine University School of Law.

[1] Shane McGee, Randy V. Sabett, & Anand Shah, Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense, 8 J. Bus. & Tech. L. 1, 28-29 (2013) (quoting Jeffrey Hunker et al., Institute for Info. Infrastructure Protection, Role And Challenges For Sufficient Cyber-Attack Attribution 5 (2008)).