The Russia-Ukraine conflict and insurance for state-sponsored cyberattacks

By Jeffrey J. Meagher, Esq., Lucas J. Tanglen, Esq., and Reymond E. Yammine, Esq., K&L Gates LLP

MARCH 25, 2022

Now that Russia has invaded Ukraine and the United States and its allies have responded by imposing economic sanctions on Russia, cyberattacks against U.S. businesses may soon follow. In recognition of this threat, President Joe Biden, in a statement (https://bit.ly/3IFJlWi) on March 21, 2022, cited "evolving intelligence" that "the Russian Government is exploring options for potential cyberattacks" and urged private sector businesses to "harden your cyber defenses immediately." Statement by President Biden on our Nation's Cybersecurity, The White House, March 21, 2022.

President Biden's remarks follow earlier warnings by the nation's top cyber defense agency recommending that "all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets" (Shields Up, (https://bit.ly/3JIGvXp) U.S. Cybersecurity & Infrastructure Security Agency).

The threat is a serious one, as evidenced by the 2017 NotPetya cyberattack, which also arose out of the Russia-Ukraine conflict. That attack, which caused billions of dollars in damage, led some insurers to assert that the war exclusion found in many types of insurance policies barred coverage for state-sponsored cyberattacks.

This article discusses that potential coverage defense, including several recent developments that may impact whether policyholders have insurance coverage for cyberattacks that arise out of the ongoing Russia-Ukraine conflict.

The NotPetya cyberattack and a recent pro-policyholder court decision

In June 2017, the NotPetya cyberattack quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. According to a White House statement issued a few months later, it was "the most destructive and costly cyber-attack in history." Statement from the Press Secretary, White House (Feb. 15, 2018). In a departure from past policy, the U.S. government expressly blamed Russia for the attack, calling it "part of the Kremlin's ongoing effort to destabilize Ukraine … ."

Even though Ukraine was believed to be the primary target of the attack, many U.S. companies suffered collateral damage, including Merck & Co., Inc. (Merck), which submitted a claim for more than US$1.4 billion in losses under several "all risk" property insurance policies. Merck's insurers denied coverage, citing several almost identical war exclusions that barred coverage for loss or damage caused by "hostile or warlike action" by "any government or sovereign power."

To date, no courts have construed war exclusions so broadly as to preclude coverage for cyberattacks — which may originate and have their impacts far away from any battlefield — based on a purported nexus to traditional warfare.

The New Jersey Superior Court recently rejected the insurers' argument that the war exclusion applied to the NotPetya cyberattack in *Merck & Co., Inc. v. ACE American Insurance Co.* (No. UNN-L-2682-18, N.J. Super. Ct. Dec. 6, 2021). According to the court, both parties were aware that cyberattacks, including cyberattacks sponsored by nation-states, had become more common in recent years, but the insurers did nothing to change the relevant policy language, which predated the existence of such attacks. As a result, the court held that the exclusion applied only to traditional forms of warfare and did not apply to cyberattacks.

The *Merck* decision is the first reported decision to consider the application of the war exclusion to a cyberattack, which could discourage other insurers from taking a similar position. At the very least, it gives policyholders favorable authority to cite in any coverage dispute involving the application of the war exclusion to a cyberattack. That said, Merck's insurers have filed a motion for interlocutory appeal, which the Appellate Division recently granted, so the Superior Court's decision is unlikely to be the last word on this issue.

Cyber-insurance implications

Like the property insurance policies at issue in the *Merck* case, most stand-alone cyber insurance policies also have a war exclusion. The specific language varies from policy ¬to policy, but cyber policies often exclude coverage for loss or damage arising out of "war," "warlike action," "action by a military force," or "invasion."

Many cyber policies, however, now also include a "cyberterrorism" exception to the war exclusion, which restores coverage if the exception applies. Once again, the specific language varies from policy to policy, but cyber policies sometimes define cyberterrorism quite broadly to include any attack against a computer system with the "intent to cause harm" in furtherance of "social, ideological, religious, economic or political objectives."

Policyholders should also be aware that, going forward, some insurers are revising their cyber insurance policies in an attempt to exclude coverage for state-sponsored cyberattacks.

Given this structure, the application of a war exclusion to a cyberattack arising out of the Russia-Ukraine conflict may require a two-part analysis: (a) Does the core exclusion bar coverage, and (b) if so, does the cyberterrorism exception restore coverage?

The insurer would likely bear the burden of proving that the core exclusion applies (which may be difficult if the origin of the attack is unclear), while the policyholder (depending on the applicable law) may bear the burden of proving that the exception applies. The *Merck* case is relevant to the first part of the analysis. Accordingly, a policyholder can point to that case and argue that the war exclusion applies only to loss or damage that arises out of traditional forms of warfare.

Now that Russia has invaded Ukraine, however, insurers may argue that the exclusion applies to loss or damage caused by cyberattacks that arise out of the Russia-Ukraine conflict because that conflict now looks more like a conventional war than it did when the *Merck* case was decided. That said, to date, no courts have construed war exclusions so broadly as to preclude coverage for cyberattacks — which may originate and have their impacts far away from any battlefield — based on a purported nexus to traditional warfare.

In addition, policyholders that reside in countries that are not involved in ongoing hostilities with the state sponsor of a cyberattack may be able to argue that the war exclusion does not apply to cyberattacks that cause collateral damage in non-combatant countries.

Even if the war exclusion applies to a specific cyberattack, the cyberterrorism exception may restore coverage.

As noted above, many cyberterrorism exceptions apply to any attack against a computer system with the "intent to cause harm" in furtherance of "social, ideological, religious, economic or political objectives." Any cyberattack that arises out of the Russia-Ukraine conflict seems likely to have been executed with the intent to cause harm and in furtherance of social, ideological, economic or political objectives.

An insurer might argue that a policyholder must prove that Russia (or those acting on behalf of Russia) specifically intended to harm the policyholder (as opposed to Ukraine or the United States more generally), but the plain language of most cyberterrorism exceptions does not support such a reading.

Policyholders should also be aware that, going forward, some insurers are revising their cyber insurance policies in an attempt to exclude coverage for state-sponsored cyberattacks. Lloyd's of London recently issued four model exclusions that exclude coverage for loss or damage that arises out of "cyber operations" by or on behalf of a state to "deny, degrade, manipulate or destroy information in a computer system of or in another state." (Bulletin LMA21-042-PD, Nov. 25, 2021).

These model exclusions differ in language, but each exclusion contains a provision stating that the "primary" factor in determining attribution of a cyber operation "shall be whether the government of the state ... in which the computer system affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on its behalf."

It remains to be seen whether insurers outside of the London insurance market will introduce similar exclusions, but policyholders should pay very close attention to any proposed endorsements or other policy language changes that implicate the war exclusion or otherwise attempt to restrict coverage for state-sponsored cyberattacks.

Conclusion

If past is prologue, insurers may rely on the war exclusion in property and cyber insurance policies to deny coverage for cyberattacks arising out of the Russia-Ukraine conflict. Policyholders should review their insurance policies in light of recent developments and carefully consider any proposed changes to the war exclusion at renewal.

About the authors



Jeffrey J. Meagher (L) is a partner in **K&L Gates**' Pittsburgh office, where he concentrates his practice on insurance coverage and complex commercial litigation. In the insurance coverage area, he represents corporate policyholders seeking coverage under different types of insurance policies. He also counsels clients regarding their cyber insurance programs and cyber incident response plans outside of litigation. He can be reached at: Jeffrey.Meagher@klgates.com. **Lucas J. Tanglen** (C), a Pittsburgh partner at the firm, represents businesses seeking to maximize the value of their insurance assets and has experience representing policyholders in complex insurance matters. In his cyber insurance practice, he counsels policyholders regarding the placement and renewal of cyber policies, including negotiation of key terms of coverage. He can be reached at: Lucas.Tanglen@klgates.com. **Reymond E. Yammine** (R) is an associate in the firm's Newark office, where he focuses his practice on general commercial litigation matters with a particular focus on energy, construction, and infrastructure. In addition, he focuses his practice on government enforcement matters with emphasis on compliance with the Foreign Corrupt Practices Act (FCPA) and matters in the field of cyber insurance. He can be reached at: Reymond.Yammine@klgates.com.

This article was first published on Reuters Legal News and Westlaw Today on March 25, 2022.