Anticipating Cyberinsurance Wartime Exclusion Questions

By **Steven Stransky, David Finz and Rick Yocum** (March 8, 2022)

Steven Stransky

David Finz

Rick Yocum

In recent weeks, there have been clear warnings and threats that Russia and Moscow-sponsored groups may increase ransomware and similar malicious cyber operations as part of the Russia-Ukraine war.

In response, businesses have been enhancing their own cybersecurity posture to mitigate their risk in this area. A key part of any cyber risk mitigation plan is insurance.

However, underlying most cybersecurity insurance policies are the so-called war and hostilities exclusions that remove an insurance carrier's responsibility to provide coverage for damages and losses that arise in the context of a military conflict.

These exclusions are highly fact-specific and are based on the precise wording in a particular policy. Unfortunately, they have a sparse record of judicial interpretation in the context of wartime cyber operations.

There are several measures that businesses should be undertaking now to better prepare for potential incidents and claims, including analyzing how these exclusions apply to their specific policies and maintaining a comprehensive record of cyberattack warnings, threats and attributions made by government officials.

The Cyberthreat Landscape

As part of its war with Ukraine, the Russian government, as well as its agents and supporters, has undertaken comprehensive cyberattacks against Ukrainian infrastructure and have threatened to launch similar attacks against others who interfere with the international armed conflict.

For instance, in the months, weeks and hours leading to Russia's invasion of Ukraine, threat actors deployed, on multiple occasions, destructive malware against Ukrainian-based organizations to destroy their computer systems, networks and devices.[1]

In addition, there have been press reports describing digital attacks against Ukraine, including a cyberattack that disabled websites belonging to the Ukrainian Ministry of Foreign Affairs and the Ukrainian Embassy to the U.S.[2] The New York Post reported that "Russia appears to have officially declared cyberwar on the U.S., taking what's been described as preliminary steps at crippling its banking system and possibly other major industries."[3]

In addition, well-known ransomware groups have indicated that they will participate in the war — but on competing sides. The Conti ransomware group issued a public statement in support of Russia and noted that if any government, entity, or group "decide[s] to organize a cyberattack or any war activities against Russia, we are going to use our all [sic] possible resources to strike back at the critical infrastructures of an enemy."[4]

In response, members of the Anonymous hacktivist group announced that in order to

support Ukraine, the group would undertake its own cyber operations targeting Moscow.[5] In fact, shortly after its declaration of support for Russia, Conti and Trickbot, another hacking group with ties to Moscow, were themselves targets of separate cyber operations that resulted in the leaking of information on their internal operations.[6]

Russia's significant cyber operations against Ukraine are well known, as they have not just affected Ukraine's internal infrastructure but have also affected businesses and governments globally. For instance, in October 2020, six computer hackers within Russia's main intelligence directorate were indicted in federal court for engaging in systematic and continuous cyberattacks against Ukraine, including launching the NotPetya malware.[7]

Although the NotPetya malware attack targeted Ukrainian infrastructure, it spread beyond national borders and indiscriminately infected and crippled information networks, systems and devices around the world. It even shut down computer systems of hospitals and pharmaceutical companies, which is especially important to note given the devastating humanitarian impact such a cyberattack could have caused if perpetrated at the height of the COVID-19 pandemic.

According to the White House, the NotPetya attack "was part of the Kremlin's ongoing effort to destabilize Ukraine" but ultimately resulted in "billions of dollars in damage across Europe, Asia, and the Americas."[8]

Cyberinsurance, War Exclusion and the Merck Decision

The primary reason that insurance policies have war exclusion clauses is to address the catastrophic financial burden that insurers would incur in the event they had to cover damages and losses arising in the context of an armed conflict.

Because military conflicts are difficult to predict, especially in terms of their scope and scale, the insurance industry cannot confidently calculate risk and set premiums for their customers. Moreover, insurance companies routinely include such exclusions in policies that could potentially be invoked to redress damages caused by war, such as property, automobile, homeowners, renters, life insurance and cyber policies.

Although each insurance policy contains its own unique terms and conditions, a war exclusion clause often contains similar characteristics. Unfortunately, many of these clauses were drafted to align with traditional military operations and do not account for the nuances found in cyberwarfare.

The war exclusion clause in the insurance policy issued to Merck & Co. by Ace American Insurance Co. provides an interesting case study as the parties have been involved in litigation to determine whether the exclusion would prevent Merck from recovering millions of dollars of damages it suffered in 2017 as a result of the NotPetya attack.[9]

This particular war exclusion essentially rendered the policy inapplicable with respect to any loss, harm or damage incurred by Merck as a result of hostile or warlike actions during time of peace or war, including such actions that hinder, combat or defend against an actual, impending or expected attack by (1) a government or sovereign power — de jure or de facto — or by an authority that maintains or uses military, naval or air forces; (2) military, naval, or air forces themselves; or (3) an agent of any of the foregoing.[10]

In Merck v. Ace American Insurance, the New Jersey Superior Court assessed the applicability of this war exclusion in the context of the NotPetya attack and ultimately ruled

in favor of Merck in December that the exclusion did not apply.

Essentially, the court in analyzed a broad range of legal decisions that addressed similar war exclusion clauses and emphasized the U.S. Court of Appeals for the Second Circuit's 1922 holding in Queens Insurance Co. v. Globe & Rutgers Fire Insurance Co.:

> In order to impose liability under the war risk clause policy, all forms of hostilities or warlike operations of whatever kind must consist of some form or kind of hostility or warlike operations which have proximately caused the loss. Remote consequences of hostilities cannot become a recoverable loss.[11]

According to the New Jersey Superior Court, "no court has applied a war (or hostile acts) exclusion to anything remotely close" to the circumstances involving NotPetya and therefore Ace American could not invoke the war exclusion clause to avoid coverage.

It is important to note, however, that although the New Jersey court ruled in favor of Merck, this matter has been in litigation for almost four years and may still be appealed and further extend the time frame in which Merck may recover damages under its insurance policy.

Recent Proposals and Continued Ambiguity

The Merck decision highlights the challenges around how direct and indirect damages caused by a cyberattack during an armed conflict should be interpreted within the context of an insurance policy.

For instance, there are differing opinions and case law on whether war exclusions only apply when a war has been declared or acknowledged by the U.S. government in the constitutional sense or extend to encompass any significant military operations regardless of whether a declaration of war has been formally announced.

These issues are also complicated by the fact that victims and governments may not be able to reliably attribute a cyberattack to a particular country or organization, or determine whether the attack was actually part of the armed conflict or another, separate cyber operation.

In November 2021, Lloyd's of London published four new model war exclusion clauses for cyberinsurance policies that were designed, at least in part, to address these types of issues and to modernize these exclusions for the cyber context.[12] The four clauses generally focus on whether an insurance company can invoke the war exclusion based on harm arising from a cyber operation or war.

The term "cyber operation" is essentially defined as the use of a computer system by or on behalf of one state to negatively impact data in a computer system of, or in, another state. The term "war" means either (1) the use of physical force by one state against another, or as part of a civil war, rebellion, revolution, or insurrection or (2) the military takeover, confiscation, or damage to property by a government or public authority.

Importantly, under this definition, the war exclusion would broadly apply to situations involving hostilities regardless of whether a war has been formally declared. In some instances, the clauses remove an insurance company's obligation to cover losses when the damage occurs with respect to a war or cyber operation committed by certain specified states, which are defined to mean China, France, Germany, Japan, Russia, the U.K. and the U.S.

The first model exclusion removes broadly an insurer's obligations to cover losses arising from a war or cyber operation.

The second model exclusion focuses on denying coverage for losses that result from a: (1) war or a cyber operation that is facilitated during a war; (2) retaliatory cyber operations between any of those specified states; and (3) a cyber operation that has a major detrimental influence on the functioning of a state due to its impact on a state's ability to provide essential services or security.

It also provides the insured is only covered for other cyber operations to a specific limit, either per event or in the aggregate during the term of the coverage.

The third model exclusion is essentially the same as the second but omits the coverage for other cyber operations.

The fourth model exclusion, while similar in scope to the others, also bars recovery for losses that are caused by war or a cyber operation that is facilitated in the course of war and by a cyber operation that has a major detrimental impact on the functioning of a state due to its impact on a government's ability to provide essential services or security.

However, unlike the others, the fourth model excludes recovery of damages resulting from "retaliatory cyber operations between any specified states leading to two or more specified states becoming impacted states." In turn, the phrase "impacted state" essentially means any state where a cyber operation has had a major detrimental impact on the functioning of a state due to its impact on a state's ability to provide essential services or security.

These exclusions do not apply to either the direct or indirect effect that a cyber operation has on a "bystanding cyber asset," which is defined as a "computer system used by the insured or its third-party service providers that is not physically located in an impacted state but is affected by a cyber operation."

If adopted across the entire industry, these model war exclusions can bring a degree of clarity and uniformity to a difficult area of coverage. However, Lloyd's model clauses still present challenges of interpretation, which are highlighted by the Russia-Ukraine war, which could result in coverage disputes between policyholders and their providers.

For instance, under all the model clauses, the primary mechanism in determining attribution of a cyber operation is whether the government of the jurisdiction in which the cyber operation occurred attributes the event to another state or its agents.

However, pending such attribution, the insurance provider may rely upon other information and inferences to unilaterally determine the source of the attack, and during this period, it is not required to pay for any claims submitted by a policyholder.

This approach is difficult because of circumstances in which a government remains silent on attribution in order to protect intelligence sources or methods, for diplomatic reasons, or because of other political motivations. Even when a government does attribute a cyberattack to a foreign government or group, it could take months to do so, such as when the U.S. did not formally attribute the NotPetya attack to Russia until almost eight months after it originally occurred.

The Lloyd's proposal also does not account for situations wherein one branch of a

government seeks to attribute a cyber operation to a state, but another branch of the same government does not. As an example, it is entirely foreseeable that individual members of Congress or a particular legislative committee may attribute a cyber operation to Russia, while the president or others in the executive branch remain silent.

Best Practices

There is still a concern that the Russia-Ukraine war can escalate into a broader conflict, including one in which cyber operations, either intentionally or unintentionally, affect organizations well beyond the direct zone of conflict, such as in the U.S.

In light of this, there are actions businesses can undertake now to better protect themselves against cyberthreats and to better equip themselves in the event they need to submit a claim for losses or damages resulting from a ransomware attack or similar malicious cyberactivity that may be linked to the Russia-Ukraine conflict.

First and foremost, businesses should be analyzing their security controls to identify whether they provide adequate security in light of threats emanating from Russia and its agents.

Recently, the U.S. government identified several technical security measures that organizations should implement to mitigate risk in this area, including multifactor authentication; employing antivirus and anti-malware scanning; enabling strong spam filters; updating software; and filtering network traffic.[13]

In addition, organizations should review the White House's 2021 open letter on protecting against ransomware, as it summarizes the most fundamental and critical security controls that the private sector should be implementing and maintaining.[14]

Organizations should consider aligning their information security programs to industry-recognized frameworks, such as the National Institute of Standards and Technology's cybersecurity framework or the Center for Internet Security's critical security controls. In fact, it is common for insurance companies to require proof of compliance with these security measures and standards as a prerequisite for cyberinsurance coverage.

It is important that organizations test their security controls to ensure their adequacy in light of evolving threats, and they should be undertaking tabletop exercises to better ensure that business leaders are prepared to address the difficult issues that are presented in the context of a cybersecurity event.

Next, organizations must understand the scope of their insurance coverage, including whether their policies offer assistance with respect to implementing the above-mentioned security requirements. Given the current threat environment, it is especially important that organizations fully comprehend how war exclusions and similar types of exclusions, e.g., terrorism, apply to their policies, including whether these exclusions rely upon archaic formulations not well suited for cyberwarfare.

Accordingly, policyholders should identify whether their insurer has previously interpreted war exclusion clauses in the cyber context or issued a formal position on this matter, which can aid in establishing standards and expectations with respect to coverage. In the event such insurance is not adequate, organizations should immediately seek to identify whether they can procure supplemental or replacement coverage to minimize the risk.

However, it should be noted that cyberinsurance premiums are likely to increase as a result of the Russia-Ukraine war, which actually reflects a trend in the industry over the last several years to account for more sophisticated and damaging cyberattacks.

If organizations are unable to obtain sufficient coverage due to high costs, risk transference limitations or similar issues, they may need to consider alternate, or additional, risk mitigations, such as self-insurance funds and enhanced resources being devoted to internal security capabilities.

In addition, it is important for companies to retain comprehensive records of all malicious cyberactivity arising from the Russia-Ukraine war to assist in determining the viability of cyberinsurance claims and applicability of war exclusion clauses.

Accordingly, organizations should consider retaining records of any cyberattack warnings, threats and attributions adopted by the U.S. government, foreign governments or multinational organizations, e.g., the United Nations and the North Atlantic Treaty Organization.[15]

Companies should also consider memorializing any statements made by cybergroups, such as the public declarations made by the Conti group and Anonymous. To assist in this area, and to bolster their information security program more generally, businesses should consider joining a private-public cyberinformation center and obtaining data on current and foreseeable cyberthreats.

In the event an organization is subject to a ransomware attack or similar incident, it should be undertaking measures to identify the threat actor to determine whether it is connected to the Russia-Ukraine war, or otherwise for general export control compliance purposes.

This often involves assessing whether the cryptocurrency and virtual wallet or the cybertactics have been associated with a particular group, and whether the malware at issue can be reverse-engineered to determine whether the underlying code can be linked to a sanctioned state or group.

In this regard, insurers are instrumental in connecting their policyholders with preapproved consultants who specialize in this area, and this assessment is often a prerequisite to identify whether a ransom payment can lawfully be made and is recoverable under an insurance policy.

It is critical that organizations understand how they will preserve evidence in connection with a cyberattack, especially with respect to ensuring any digital forensic post-incident efforts do not inadvertently destroy logs, files or records that could be used for insurance recovery or litigation purposes.

Lastly, it is important to identify whether the U.S. government escalates its involvement in the Russia-Ukraine war, including the nature, scope and duration of any military or intelligence activity occurring in and around Ukraine.

Consequently, businesses should maintain records of any legislation or proclamations made by Congress or the president, e.g., foreign aid and military assistance, that may evince a collective understanding on the state and nature of the conflict. Such information can potentially be used to support or oppose arguments that a cyber operation occurred during a war, however so defined in an insurance policy, and therefore clarify whether a war exclusion applies.

Steven G. Stransky is a partner and co-chair of the privacy and cybersecurity practice group at Thompson Hine LLP. He is also an adjunct law professor at the Frederick K. Cox International Law Center at Case Western Reserve University School of Law.

David Finz is vice president for cyber risk at Alliant Financial Institutions.

Rick Yocum is the managing director of advisory services at TrustedSec LLC, where he leads the maturity, compliance, innovations and solutions teams.

[1] The Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, Joint Bulletin, AA22-057A, "Destructive Malware Targeting Organizations in Ukraine" (March 1 2022) ("Cybersecurity Bulletin"); Welivesecurity.com, "IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine" (March 1, 2022).

[2] Raphael Satter, "Ukrainian government sites taken down after cyber attacks," Reuters (Feb. 28, 2022).

[3] Charles Gasparino, "Russian cyber attacks against US banks increasing," NY Post (March 1, 2022).

[4] Jonathan Greig, "Anonymous hacktivists, ransomware groups get involved in Ukraine-Russia conflict," ZDNet (Feb. 25, 2022). After its public announcement, Conti issued a separate statement indicating that it was not affiliated with any government.

[5] Id.

[6] Corin Faife, "The Conti ransomware gang sided with Putin and had its chat logs leaked soon afterward," The Verge (Feb 28, 2022); Raphael Satter, "Details of another big ransomware group 'Trickbot' leak online, experts say," Reuters (March 4, 2022).

[7] U.S. Department of Justice, Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" (Oct. 19, 2020).

[8] The White House, Statement from the Press Secretary (Feb. 15, 2018), available at https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

[9] Merck & Co., Inc. et al. v. Ace American Ins. Co. et al., Case No. UNN-L-2682-18 (N.J. Sup. Ct., Dec. 6, 2021).

[10] Id.

[11] Id. (quoting British Steamship v. The King (1921) 1 A.C. 99, 107, 131.

[12] Lloyd's Market Association, Bulletin LMA21-042-PD, "Cyber War and Cyber Operation

Exclusion Clauses," (Nov. 25, 2021).

[13] Cybersecurity Bulletin, supra 1.

[14] Letter from Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, to Corporate Executives and Business Leaders, "What We Urge You To Do To Protect Against The Threat of Ransomware" (June 2, 2021).

[15] Steven G. Stransky, "Intel Chiefs Testify on Global Threats, Cybersecurity and Elections," Lawfare (Jan. 30, 2019) (example demonstrating how U.S. intelligence officials may formally attribute cyber operations to a foreign government or group).