COHEN
ZIFFER
FRENCHMAN
& MCKENNA

NEW YORK LAW JOURNAL

Call to Action: Modernizing the 'War Exclusion' for the 21st Century

By Jillian Raines and Amber N. Morris

May 20, 2022

Over the past decade, global cybercrimes have skyrocketed, fueled by the increased use of computer-based technology. There is little dispute that the techniques and technology employed by bad actors are ever-evolving, with estimates that by 2025 cybercrime will cost the world $10.5 trillion annually. Very recently, the United States and other governmental authorities have warned of an increased likelihood of cyberattacks in light of recent Russian militarism in Ukraine. See James Doubek, *The U.S. warns companies to stay on guard for possible Russian cyberattacks*, NPR (March 21, 2022); Joe Tidy, *The three Russian cyber-attacks the West most fears*, BBC (March 22, 2022).

In response to these increased cyber threats, governments, businesses, and consumers alike are ramping up their cyber security measures. Many prudent businesses are also revisiting their insurance portfolio, seeking confirmation that their coverage will adequately protect them if they are victimized by increasingly sophisticated cyberattacks, including those connected to the acute conflict in Ukraine.

This exercise has put an oft-overlooked exclusion found in many types of insurance policies—the War Exclusion—directly in the spotlight. And while there have been various calls to action to address outdated War Exclusions in the last few years, to which the market has begun to respond, the results do not go far enough in modernizing the War Exclusion for our increasingly digital age or to provide the certainty policyholders' premiums should guarantee in light of the present Russia-Ukraine war.

LEGACY WAR EXCLUSIONS

A staple exclusion in most types of insurance policies, the War Exclusion was introduced well before the advent of the internet and stand-alone cyber liability coverage. Its purpose: to avoid covering damage and losses posed by traditional, kinetic warfare, which is highly unpredictable, potentially catastrophic, and presents significant underwriting challenges. Consider two real examples of exclusions still used today:

1. This policy does not cover … Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:

    a. by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces;

b. or by military, naval or air forces;
c. or by an agent of such government, power, authority or forces[.]

2. The Insurer shall not be liable to make any payment for Loss … arising out of, based upon or attributable to any war, invasion, military action (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events.

This language is broad, and various terms (such as "hostile or warlike action") are left undefined, leaving insureds to ponder precise nuances between, for example, a "mutiny" and an "insurrection." Obviously designed with boots-on-the-ground warfare in mind, these legacy Exclusions do not contemplate or address cyberattacks.

Take, for example, the well-reported NotPetya malware attack. In 2017, Merck & Co. suffered losses in the billions after more than 40,000 of its computers across the globe were infected with malware. Merck tendered this loss to its property insurers, who denied coverage based on the policy's War Exclusion, claiming that the cyberattack was sanctioned by the Russian government. Merck eventually prevailed on summary judgment, with the New Jersey Superior Court holding that the subject property policy's war exclusion was ambiguous and could not reasonably be interpreted to apply to its NotPetya-related cyberattack losses. But Merck was forced to bring a lawsuit to achieve this result, an unfortunate consequence of an outdated exclusion. And Merck is not the only company that has faced pushback from insurers related to legacy war exclusions and NotPetya—Mondelez International was also forced to resort to litigation after its insurer similarly denied coverage.

While courts may be reluctant to apply these exclusions designed for conventional armed conflicts to cyberattacks in the property insurance context, iterations of these exclusions appear in virtually all types of policies, including stand-alone cyber liability policies in use today. Policyholders often secure carve-backs to coverage for "cyber terrorism" (frequently defined as acts targeting computer systems for the purpose of furthering social, ideological, religious, or political objectives), but precedent is lacking regarding the scope of these carve-backs as applied to current events.

MARKET REACTION TO CURRENT EVENTS

Until very recently, insurers have been slow to amend these outdated exclusions. For instance, it was not until November 2021, in the wake of the *Merck* case, that the Lloyd's Market Association (LMA) drafted four amended War Exclusions for its syndicates to be used in stand-alone cyber insurance policies.

These newer LMA exclusions take various forms, but each purports to exclude coverage for loss "directly or indirectly occasioned by" either "war" or a "cyber operation"—terms newly defined, albeit in ways that do not address the fundamental uncertainty in legacy exclusions.

For example, the definition of "war" used in these amended exclusions still refers to undefined "rebellion," "insurrection," or "revolution." A domestic hacker could arguably "rebel" against the United States by attempting to spread ransomware to government, corporate, and consumer computers. Yet, whether a single individual's actions could ever constitute "rebellion" is not clear. Moreover, these refined exclusions require that a cyberattack be "indirectly occasioned by" a war or cyber operation, which, particularly where the exclusion provides that war need not be officially declared, risks the exclusion swallowing coverage entirely. And whether such operation is performed "on behalf of a state" as these exclusions contemplate, is typically unclear at point of initial claim, as was the case in the NotPetya attacks and subsequent litigation.

Many other market players have recently introduced amendments aimed at modernizing the War Exclusion, too, in ways that are more affirmatively designed to clarify whether certain activities or actions constitute war and to "avoid surprises." See, e.g., Carolyn Cohn and Noor Zainab, Munich Re tightens up cyber insurance policies to exclude war, Reuters (April 8, 2022).

Yet, many of these revamped and untested War Exclusions circulating today (1) still refer to undefined terms such as "rebellion, revolution or insurrection," (2) introduce complexity around the chain of events that will trigger the exclusion, (3) indicate that the exclusion will apply to circumstances resulting in economic sanctions, (4) neglect to expressly reiterate coverage for cyber terrorism, or (5) include language tying the exclusion "in whole or in part" to not just cyber or hostile acts,

but to any "similar" or "related" acts taken "by or on behalf of" a sovereign state actor or state-sponsored actor. In short, recent amendments are more prescribed but do not go far enough.

A FURTHER CALL TO ACTION

But pointing out these uncertainties does not help policyholders who face current events without certain assurances on their bargained-for protections. Nor does it help carriers who have acted in response to calls for modernization. And waiting for lengthy and costly litigation on both sides could take years to reconcile. Instead, focusing collective efforts to further clarify War Exclusions is a reasoned next step.

To begin that discussion, exclusions should be further narrowed to make clear they apply only to kinetic warfare declared through resolution or other formal action taken by a sovereign state. Removing undefined and overly broad language such as "indirectly occasioned by," "whether war be declared or not," "on behalf of," or language that refers to related conduct or acts, will also help avoid confusion and arguments for an unintended expansion of this deliberate exclusion. And expressly reinforcing in cyber liability policies that coverage for cyber terrorism remains would also be beneficial.

Carriers are not the only ones with the capacity to achieve results on this front. Insurance regulators working to protect consumers, regulate premiums, and approve policy language, or the National Association of Insurance Commissioners (NAIC), could solicit and draft model language to guide the market. Indeed, NAIC has drafted model statutes regarding other exclusions—e.g., the Atomic Energy Exclusion (MO-700) in property and casualty policies.

Given the pervasive use of cyber technology in modern society and the crisis in Ukraine, clarity on the scope and import of the War Exclusion is essential to protect consumers and businesses. Policyholders paying significant premiums should not have to "wait and see" as cyberattacks and conflicts evolve. Earnest discussions among market players have much potential to benefit insurers and policyholders alike, and, accordingly, should be promptly undertaken.

Jillian Raines is a partner and Amber N. Morris is an associate at insurance recovery law firm Cohen Ziffer Frenchman & McKenna in New York. They represent a broad range of corporate policyholders in high-stakes insurance coverage disputes.

Reprinted with permission from the May 20, 2022 edition of the New York Law Journal © 2022 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or reprints@alm.com.