Professional Perspective

Cyber Risk & ‘War Exclusions’

Jasmeet K. Ahuja and Jack Shaked, Hogan Lovells US LLP

Bloomberg
Law

Read Professional Perspectives | Become a Contributor

Cyber Risk & 'War Exclusions'

Contributed by Jasmeet K. Ahuja & Jack Shaked, Hogan Lovells US LLP

May 2022

On March 21, 2022, President Joe Biden warned that Russia may conduct malicious cyberattacks on U.S. entities in retaliation for U.S. sanctions and support for Ukraine, and called on U.S. companies to "harden your cyber defenses immediately." Indeed, on April 8, 2022, the Finnish government was victim to a series of botnet attacks from Russia based on its support of Ukraine.

Cyberattacks have already caused significant collateral damage. On Feb. 24, for instance, Russia successfully conducted a cyberattack against U.S. satellite company Viasat, which the Ukrainian military relies on for communications. The attack on Viastat's modem quickly spread all over the world. The resulting internet outages impacted at least 27,000 users, from planes' in-flight WiFi to a German wind farm of 5,800 wind turbines. The U.S., UK, and EU all attribute the Viasat cyberattack to Russia. Corporations across industries should continue to prepare for both direct and indirect cyberattacks.

Damage and losses from cyber warfare are inevitable. The question is who will pay for the costs of liability and lost revenue. Insurance coverage for those losses will depend on specific policy language, which may include "war exclusions" that exclude losses caused by "war," "warlike activities," "hostilities," and other specified activities.

A review of decisions examining the scope of "war exclusions" highlights several issues that could shape whether losses arising from the current war are excluded or covered. These include: whether "war exclusions" exclude coverage for cyberattacks launched by state operatives during a time of war; what is required to attribute a cyberattack to a state actor; and what causal relationship between war or warlike activities and loss is needed for an exclusion to apply.

State-Sponsored Cyberattacks

Case law addressing such exclusions is limited. In a recent case examining the scope of the "war exclusion," the New Jersey Superior Court in December 2021 held that a "War and Hostile Acts" exclusion in an all risks policy did not apply to loss caused by the NotPetya ransomware attack. See *Merck & Co. Inc. v. Ace Am. Ins Co.*, No. UNN-L-002682-18, (N.J. Super. Ct. Dec. 6, 2021). The court so found despite the U.S. government expressly attributing the attack to hackers who were officers of the Russian Main Intelligence Directorate (GRU) and indicting them. The case was being appealed as of publication.

The exclusion at issue in the *Merck* case read:

1) 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;

This policy does not insure against loss or damage caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

The insurer argued that the exclusion applied on the ground that, among other things, the malware was "an instrument of the Russian Federation as part of its ongoing hostilities against the nation of Ukraine." The court, however, found the scope of the exclusion ambiguous and thus interpreted it to conform with what it found to be Merck's reasonable expectation that it excluded only loss caused by the use of conventional armed forces.

A second case relating to coverage for loss stemming from the NotPetya attack was pending before the Illinois Circuit court as of publication. See *Mondelēz Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-011008 (Ill. Cir. Ct. Oct. 10, 2018). According to the complaint in that case, the implicated 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.

In March 2022, in a summary order without an accompanying memorandum opinion, the court denied partial summary judgment on this exclusion for both parties. Further developments in this case are important to monitor.

After NotPetya, many insurers incorporated new exclusions into standalone cyber-insurance policies to exclude loss, damage, or liability (together "loss") stemming from state-sponsored cyberattacks. For example, in November 2021, the Lloyd's Market Association of London (LMA) issued **four models** of such exclusions.

One states the insurance does not cover loss "directly or indirectly occasioned by, happening through or in consequence of war or a cyber operation." The three others use similar language but impose the restrictions on the circumstances under which a "cyber operation" triggers the exclusion:

1.1. war or a cyber operation that is carried out in the course of war; and/or

1.2. retaliatory cyber operations between any specified states; and/or

1.3. a cyber operation that has a major detrimental impact on:

1.3.1. the functioning of a state due to the direct or indirect effect of the cyber operation on the availability, integrity or delivery of an essential service in that state; and/or

1.3.2. the security or defence of a state.

The LMA model exclusions define "cyber operation" as "the use of a computer system by or on behalf of a state to disrupt, deny, degrade, manipulate or destroy information in a computer system of or in another state."

The exclusions also state what is sufficient to determine attribution of a cyber operation:

4. Pending attribution by the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located, the insurer may rely upon an inference which is objectively reasonable as to attribution of the cyber operation to another state or those acting on its behalf. It is agreed that during this period no loss shall be paid.

5. In the event that the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located either:

5.1. takes an unreasonable length of time to, or

5.2. does not, or

5.3. declares it is unable to attribute the cyber operation to another state or those acting on its behalf, it shall be for the insurer to prove attribution by reference to such other evidence as is available.

Impact of Biden's Statements on Attribution

Historically, countries, including the U.S., have been reluctant to attribute cyberattacks to other specific countries. This is for many reasons, including that cyberattacks are hard to trace, and countries fear exposing their methods or sources of intelligence. In the event of a country's reluctance to attribute, the LMA policies allow for the insurer to "rely upon an inference which is objectively reasonable" to attribute the attack. This may permit reliance on, for example, public attributions made by private cybersecurity firms and technology companies.

The LMA models each provide that they only apply if the "cyber operation" is attributed to another country "or those acting on its behalf." They also all indicate that the primary factor in determining whether a cyber operation has been attributed to a hostile state actor shall be whether the state "in which the computer system affected … is physically located attributes the cyber operation to another state or those acting on its behalf."

Attribution of cyberattacks is a key issue when it comes to the application of insurance exclusions. Given Biden's public statements warning the private sector to prepare for cyberattacks and the U.S. government's decision to name Russia in the NotPetya attack and the Viasat attack—a departure from past U.S. policy—determinations of insurance coverage could be made on whether Biden's statements show there is an "inference which is objectively reasonable" to support attributing a cyberattack to Russia. If a war exclusion applies only if the state in which the affected computer system sits attributes the attack to a state actor, certain states' inability or unwillingness to make such attributions could also become a factor.

Causation Analysis & War Exclusions

The level of causation required for a loss to be considered a result of warlike or hostile action has been an important issue for the applicability of war exclusions. Cyberattacks can make the question of causation challenging, and the majority of claims likely will not be from companies that were direct targets, but instead from companies who were mere collateral damage. In examining the question of causation, considerations may include the temporal and geographic proximity of the damage to the cyber "shot" that was fired.

In a case that did not involve a cyberattack, but rather insurance coverage for moving a TV production out of Jerusalem following rocket attacks launched by Hamas, the U.S. Court of Appeals for the Ninth Circuit found a district court erred by failing to recognize that "war" and "warlike action by a military force" require hostilities between either de jure or de facto sovereigns, and that Hamas was neither.

The insurer argued that the exclusion applied in any situation where the loss is caused, whether directly or indirectly, by a war or warlike action of "a" military force. Because of that, Israel's military engagement with Hamas was enough to trigger the exclusion. In rejecting this argument on proximate causation grounds, the Ninth Circuit held that "the fact that an excluded risk contributed to the loss would not preclude coverage if such a risk was a remote cause of the loss." See *Universal Cable Prods., LLC v. Alt. Specialty Ins. Co.*, 929 F.3d 1143, 1161 (9th Cir. 2019) (quoting *Julian v. Hartford Underwriters Ins. Co.* , 110 P.3d 903, 907 (Cal. 2005)).

In a case from decades earlier, the U.S. Court of Appeals for the Second Circuit had examined proximate cause as it relates to coverage for the loss of a 747 plane that was destroyed by hijackers claiming to represent The Popular Front for the Liberation of *Palestine. See Pan American World Airways, Inc. v. Aetna Cas. & Sur. Co.,* 505 F.2d 989 (2d Cir. 1974). In *Pan American*, the court held that remote causes are not relevant to the characterization of insurance loss and the words "due to or resulting from" limit the inquiry to the facts immediately surrounding the loss."

In support of this conclusion, the court cited cases finding that a loss remotely caused by a war was not excluded by a war exclusion. These included a World War I-era British case involving the loss of a ship that went aground and was lost because it took a more northerly route to avoid German submarines. Similarly, when a ship collided with a minesweeper, the loss was interpreted to have been caused by the collision rather than the war-related minesweeper's presence in the harbor. See *Standard Oil v. United States, 340 U.S. 54, 71 S. Ct 135, 95 L.Ed. 68 (1950)*. And, when an insured aircraft was lost over Vietnam in a collision with a military aircraft, the loss was due to an aviation peril, notwithstanding that the two aircraft were flying over Vietnam only because there was a war. *Airlift International, Inc. v. United States* , 335 F. Supp. 442, 449 (S.D. Fla.1971), aff'd, 460 F.2d 1065 (5th Cir. 1972) (mem.).

These cases may be distinguishable, however, from one seeking loss from a wartime cyberattack. Because military leaders recognize cyberattacks as a type of weapon, such loss may be more akin to the loss of vehicles that were destroyed by mortar fire in a clash between Israelis and Arabs in 1948. See *Hamdi & Ibrahim Mango Co. v. Reliance Ins. Co.*, 291 F.2d 437 (2d Cir. 1961) (finding this loss was due to "warlike operations"); but see *Int'l Dairy Eng'g Co. of Asia v. Am. Home Assur. Co.*, 352 F. Supp. 827, 828 (N.D. Cal. 1970), aff'd, 474 F.2d 1242 (9th Cir. 1973) (insured's loss in a fire set by a U.S. parachute flare during the Vietnam War was attributable to a "warlike operation").

The specific facts surrounding a state-sponsored cyberattack will likely shape the proximate cause analysis and this analysis could be impacted by whether the damage at issue, although indirect in time and space, was directly caused by the cyberattack's malware. The new LMA exclusions exclude loss that is “directly or indirectly occasioned by, happening through or in consequence of war or a cyber operation.”

As in most contract disputes, the language of the exclusion itself will be most important. One LMA model exclusion, for example, has a partial carve back for “direct or indirect effect of a cyber operation on a bystanding cyber asset,” 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.” It remains to be seen how causation language regarding cyberattacks will be applied by the courts.

Although not included in the LMA exclusions, many insurance policies’ war exclusions also contain a carve back for “cyber-terrorism,” allowing attacks defined as such to be covered by the policy. Some definitions of the term focus on the non-state nature of the perpetrators, others on their motivations—if they're political/ideological vs. economic—and others on the effects of the attack itself.

A common definition of cyber terrorism used in insurance policies is a “use or threatened use of disruptive activities against the insured's computer system committed with the intent to further stated social, ideological, religious, economic, or political objectives.” In general, definitions focused on the effects of the attack may be broader, while definitions focused on the type of perpetrator and their motivations may be narrower, but this would of course depend on the actual language used.

What's Next

The cybersecurity risk and stakes are higher than ever and policy language may further be changing as a result. Whether an exclusion is found to apply will depend not just on the facts of the attack, but on the type of the policy, and the specific language of the exclusion. For example, does the exclusion require attribution from the impacted state before it applies? For companies that experienced collateral damage, will it be considered the result of “war” or “warlike” action even if they weren't the primary target of the attack?

Moving forward, both insurers and insureds should therefore consider what type of exclusion they are comfortable with and pay special attention to the exclusion's standards regarding attribution and causation. The four LMA model exclusions, for example, contain varying language on these points. The importance of that language cannot be overstated in evaluating the scope of cyber coverage for a policyholder's own systems and—in the case of software developers, IT consultants, web hosting services, and other companies offering similar services—their clients’ systems.

As cyberattacks related to Russia's invasion of Ukraine increase in severity, strong presidential statements and the increasing willingness of the U.S. to accuse Russia of cyberattacks may make it more likely that a war exclusion's attribution requirement will be satisfied. If courts determine, as in *Mondelez*, that issues of fact impact coverage, resolution of these issues may become more costly and time-consuming.