Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity Insurance

Insurance policies contain a host of exclusions, including war exclusions, but it is uncertain how the war exclusion applies to cybersecurity insurance, so companies need to carefully review the war exclusion when purchasing a cybersecurity policy, the authors write.

Untested in Battle—The Cybersecurity Insurance Policy War Exclusion

BY J. WYLIE DONALD AND JENNIFER BLACK STRUTT

It has not been a good week. A foreign enemy—an unnamed sovereign state, terrorists or a rebel faction—first pilfered $10 million through an unauthorized wire transfer, and then unleashed Aurora, Stuxnet, or some yet-to-be named cyber-pestilence on your ''supervisory control and data acquisition'' (SCADA) systems. When the dust cleared, you had $8 million in physical damage to your plant. But your risk manager is not concerned. ''This is exactly why we purchased that cybersecurity insurance policy and put the cyber endorsement on our property policy,'' she tells you. You relax. Proper prior planning prevents poor performance.

Or did it? Your policies contain a ''war exclusion'' excluding loss caused by ''foreign enemies.''[1] Is all that planning to be negated?

Before we get to that, a little background in cybersecurity insurance is in order. Everyone is familiar with the need for property and liability insurance. We have such coverage on our car and our house. Trees falling, fires, careless driving, trips-and-falls; we protect ourselves from identified risks. Ideally we would protect ourselves from unidentified risks as well. The well-known ''All Risk'' property policy suggests that might be attainable. But it is not because all insurance policies contain exclusions.

At first, risks caused by hacking, malicious software, distributed denial of service (DDOS) attacks, phishing, and the whole host of cybersecurity plagues with which we are now familiar, were not expressly considered by property and liability policies. Policyholders and their insurers were left to argue, among other things, about whether bad code constituted property damage and whether a DDOS attack was a covered ''occurrence.''

That has since changed. Now, various forms of cybersecurity risk are regularly excluded from property and liability policies. For example, the Insurance Services Office has published an ''Access or Disclosure of Confidential or Personal Information and Data-Related Liability'' exclusion. It is broadly written and seeks to exclude coverage for damages arising out of:

(1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing meth-

J. Wylie Donald is a partner in the Insurance Recovery Practice Group at McCarter & English LLP, Washington.

Jennifer Black Strutt an associate in the Insurance Recovery Practice Group at McCarter & English LLP, Stamford, CT.

The views expressed in this article are those of the authors and not necessarily those of the firm or its clients.

[1] We assume all other requirements for coverage are met. This may not be a safe assumption. Cybersecurity insurance policies vary widely in what they cover.

 ISSN 1538-3423

ods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or

(2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.[2]

Today, if a business wants to be certain it has coverage for cybersecurity risks, it must specifically seek the coverage. That can come in the form of an endorsement on the liability or property policy, or in the form of a stand-alone cybersecurity policy. The market is growing like Topsy with double digit increases in those acquiring the coverage in recent years.

But just like the property and liability policies that went before, cybersecurity policies and cybersecurity endorsements also are subject to exclusions. One of interest here is the so-called ''war exclusion.''

Here is a sample of the language:

> This CyberRisk Policy will not apply to any Claim or Single First Party Insured Event based upon or arising out of war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, confiscation, nationalization, requisition, or destruction of, or damage to, property by or under the order of any government, public or local authority; provided that this exclusion will not apply to any ''act of terrorism'' as defined in the Terrorism Risk Insurance Act, as amended.[3]

Returning to our initial scenario, it seems pretty clear that we do not have a ''war'' (i.e., there is no Pearl Harbor, bombardment of Fort Sumter, or crossing of the Rubicon). Or do we (and by ''we,'' we mean the U.S.)? We have ''boots on the ground'' in Syria engaging with the so-called Islamic State.[4] With the lack of a peace treaty, we are technically still at war with North Korea.[5] We have been fighting the ''War on Terror'' for almost 15 years.[6] And now ''Cyber War'' is a normal state of affairs.[7]

And even if there is no ''war,'' what about ''acts of foreign enemies,'' ''hostilities (whether war is declared or not),'' ''insurrection'' or ''military or usurped power.'' What do such terms mean? More importantly, what do such terms mean in a cybersecurity insurance policy?

Militaries around the globe have reconfigured as a result of technological advancements,[8] and the term ''war'' (among others) may have connotations today that differ from those of the past. However, the war exclusion's text is comprised of terms of art. When there is a coverage dispute concerning the meaning of the exclusion, courts will be guided by past judicial interpretation, even if such case law is from another (pre-cyber) era.

The touchstone for understanding the war exclusion is the Second Circuit Court of Appeals 1974 decision in *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.*, which examined the exclusion in a case involving unfolding chaos in the Middle East in 1970.[9] The court succinctly laid out the incident leading to the insurance claim by Pan Am:

> On Sept. 6, 1970 Pan American Flight 083, while on a regularly scheduled flight from Brussels to New York, was hijacked in the sky over London about 45 minutes after it had taken off from an intermediate stop in Amsterdam. Two men, Diop and Gueye, acting for the Popular Front for the Liberation of Palestine (the PFLP), forced the crew of the aircraft to fly to Beirut, where a demolitions expert and explosives were put on board. The aircraft, a Boeing 747, was then flown to Egypt still under PFLP control. In Cairo, after the passengers were evacuated, the aircraft was totally destroyed.[10]

At issue was whether Pan Am's all risk insurers or war risk insurers would pay the claim. The all risk insurers asserted a war exclusion:

> C. This policy does not cover anything herein to the contrary notwithstanding loss or damage due to or resulting from:
>
> 1. capture, seizure, arrest, restraint or detention or the consequences thereof or of any attempt thereat, or any taking of the property insured or damage to or destruction thereof by any Government or governmental authority or agent (whether secret or otherwise) or by any military, naval or usurped power, whether any of the foregoing be done by way of requisition or otherwise and whether in time of peace or war and whether lawful or unlawful (this subdivision 1. shall not apply, however, to any such action by a foreign government or foreign governmental authority follow-the forceful diversion to a foreign country by any person not in lawful possession or custody of such insured aircraft and who is not an agent or representative, secret or otherwise, of any foreign government or governmental authority) . . .;
>
> 2. war, invasion, civil war, revolution, rebellion, insurrection or warlike operations, whether there be a declaration of war or not . . .;
>
> 3. strikes, riots, civil commotion . . . .[11]

The all risk insurers singled out various components of the exclusion as relevant: ''military . . . or usurped power,'' ''insurrection,'' ''civil war,'' ''war,'' ''warlike operations'' and ''civil commotion.''[12]

Following a six week bench trial, the trial court found the all-risk insurers had ''failed to meet their burden of proving that the cause of the loss was fairly within the intended scope of any of the exclusions.''[13] Further, it

---

[2] Ins. Serv. Office, CG 21 07 05 14.

[3] Travelers Insurance Company, Cyberrisk® Policy ¶ III.A.2.

[4] Kathy Gilsinan, *Cliché of the Moment: ''Boots on the Ground''*, The Atlantic (Nov. 5, 2015).

[5] *The Korean War Armistice*, BBC (Mar. 5, 2015).

[6] Paul Reynolds, *Declining use of ''war on terror''*, BBC (Apr. 17, 2007).

[7] Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat To National Security And What To Do About It (2010).

[8] Damian Paletta, Danny Yadron & Jennifer Valention-Devries, *Cyberwar Ignites a New Arms Race*, Wall Street Journal (Oct. 11, 2015).

[9] *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.*, 505 F.2d 989 (2d Cir. 1974).

[10] *Id.* at 993.

[11] *Id.* at 994.

[12] *Id.* at 996.

[13] *Id.* at 997.

  PVLR ISSN 1538-3423

found that ''the ancient marine insurance terms selected by the all risk insurers simply do not describe a violent and senseless intercontinental hijacking carried out by an isolated band of political terrorists.''[14] The all risk insurers appealed.

A key element in the Court of Appeals for the Second Circuit's analysis was the doctrine of contra proferentem, loosely translated as ''against the offeror.'' In other words, because the insurers were the authors of the language of the insurance contract, it would be construed against them. As the court noted: ''Contra proferentem has special relevance as a rule of construction when an insurer fails to use apt words to exclude a known risk.''[15] Further, ''[w]hen the all risk insurers failed to exclude political risks in words descriptive of today's world events, they acted at their own peril.''[16] ''[T]he maxim defines the scope of coverage as much as if it were a clause in the all risk policies. It is part of the understanding of the parties.''[17]

A second key element was the rule of proximate causation. ''The all risk policies exclude 'loss or damage due to or resulting from' the various enumerated perils, a phrase that clearly refers to the proximate cause of the loss. Remote causes of causes are not relevant to the characterization of an insurance loss.''[18] As Justice Holmes stated:

> The common understanding is that in construing these policies we are not to take broad views but generally are to stop our inquiries with the cause nearest to the loss. This is a settled rule of construction, and if it is understood, does not deserve much criticism, since theoretically at least the parties can shape their contract as they like.[19]

The Second Circuit recognized that there was an attenuated ''cause of causes'' to be found in the violent circumstances of the Middle East, ''[b]ut for insurance purposes, the mechanical cause of the present loss was two men, who by force of arms, diverted Flight 093 from its intended destination.''[20]

With those precepts, the court turned to the various terms at issue. The analysis was lengthy and we will not go into it in depth. What we will do is capture the specific rulings on the terms of interest:

> *Military or usurped power* - ''in order to constitute a military or usurped power the power must be at least that of a de facto government . . . by giving laws and punishing for not obeying those laws.''[21] ''The clause . . . secures the all risk insurers from losses caused by the military activities of a usurping power.''[22]
>
> *War* - ''English and American cases dealing with the insurance meaning of 'war' have defined it in accordance with the ancient international law definition: war refers to and includes only hostilities carried on by entities that constitute governments at least de facto in character.''[23] ''[A]n undeclared de facto war may exist between sovereign states.''[24]
>
> *Warlike operations* - ''There is no warrant in the general understanding of English, in history, or in precedent for reading the phrase 'warlike operations' to encompass (1) the infliction of intentional violence by political groups (neither employed by nor representing governments) (2) upon civilian citizens of non-belligerent powers and their property (3) at places far removed from the locale or the subject of any warfare. (4) This conclusion is merely reinforced when the evident and avowed purpose of the destructive action is not coercion or conquest in any sense, but the striking of spectacular blows for propaganda effects.''[25]
>
> *Insurrection* - ''[I]nsurrection means '(1) a violent uprising by a group or movement (2) acting for the specific purpose of overthrowing the constituted government and seizing its powers.' ''[26]

In reaching its decision to affirm holding the all risk insurers liable for the loss, the court could not escape the essential violence of the act: the kidnapping and holding hostage of the crew and passengers, and the ultimate destruction by explosives of the airplane. Nevertheless, by focusing on the ''ancient marine insurance terms'' and the specific details of the criminal actors, the court concluded that ''[t]erms like 'military . . . or usurped power,' 'war,' 'insurrection' and the other terms found in [the exclusion] simply do not describe a hijacking committed by two men far from the site of any larger scale violence.''[27]

The Court's task is to give the words at issue their insurance meaning; and to place the burden of proof in accordance with law.

There have been other cases since *Pan Am*. For example, in *Holiday Inns, Inc. v. Aetna Ins. Co.*,[28] a hotel operator sought to recover for the property damage to its hotel caused by repeated battles between armed factions in Beirut in 1975 and 1976. Following a bench trial where the insurer had the burden to prove the application of the war exclusion, the court ruled for the policyholder:

> Aetna, as an all risk insurer, had the burden of proving that the damage to the Holiday Inn was caused by a peril whose consequences were excluded by the policy. It undertook to show that the damage resulted from ''insurrection,'' ''civil war,'' or ''war,'' as those terms are used in insurance policies. Having

[14] *Id.* at 998.
[15] *Id.* at 1000.
[16] *Id.* at 1001 (internal quotations omitted).
[17] *Id.* at 1003.
[18] *Id.* at 1006.
[19] *Id.* at 1006 (*quoting Queen Ins. Co. v. Globe & Rutgers Fire Ins. Co.*, 263 U.S. 487, 492 (1924)).
[20] *Id.* at 1007.
[21] *Id.* at 1009-10.
[22] *Id.* at 1009 n.11.
[23] *Id.* at 1012.
[24] *Id.* at 1013.
[25] *Id.* at 1015-16 (*quoting Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.*, 368 F. Supp. 1098, 1130 (S.D.N.Y. 1973)).
[26] *Id.* at 1017 (*quoting Pan Am.*, 368 F. Supp. at 1124).
[27] *Id.* at 1022.
[28] *Holiday Inns, Inc. v. Aetna Ins. Co.*, 571 F. Supp. 1460 (S.D.N.Y. 1983).

failed to sustain that burden, Aetna is liable under the policy.[29]

The court adhered closely to the Second Circuit's conclusion that insurance terms need to be construed for their insurance meaning. It eschewed the loose language of journalists and politicians:

> Journalists and politicians invariably referred to these events in Lebanon as a ''civil war.'' They do so today. The Court's task, however, is to give the words at issue their insurance meaning; and to place the burden of proof in accordance with law. At the end of that exercise, I find for [the policyholder] on the question of coverage.[30]

But no case has yet addressed an incident where a foreign enemy unleashed a cyberattack. How would such an event fare under *Pan Am* and its progeny?

As evidenced in *Pan Am*, the details of the cyberattack matter critically. The Second Circuit looked at the specific circumstances of the radical group at issue—its actual status in the world of sovereign states, its statements as inflated propaganda or actual reality—as well as the relative locations of the hijacking and the conflict. Thus, while cyberattacks by Anonymous,[31] the Russian mafia,[32] and even al Qaeda,[33] would not measure up to the sovereign or de facto sovereign status needed to trigger the exclusion, were a cybersecurity event able to be traced back to North Korea or the so-called Islamic State, an essential feature of the exclusion may very well be satisfied. In that case, to avoid the exclusion, one would need to demonstrate that the actions were not of the sort as could be characterized as war or warlike operations. The North Korean hack of Sony would appear to lack the violence needed be characterized as war, notwithstanding North Korea's bellicosity and the lack of a peace treaty.

Application

Turning to the scenarios presented at the opening of this article—a $10 million theft and the destruction of property, both by cyber means—how might a ''war exclusion'' fare were cybersecurity coverage sought? The $10 million theft, by itself, should not invoke the exclusion because of the lack of violence. But when it is coupled to the $8 million in property damage, we then need to look to the actors and their intentions. If the attacker did not possess the attributes of sovereignty or de facto sovereignty, then we do not have ''war'' or ''war-like operations'' or ''military or usurped power.'' But if the attack were carried out by Islamic State, have the scales tipped?

A different argument could be that, notwithstanding all the rhetoric, cyberattacks are not war; they are no more than criminal acts, even when perpetrated by sovereigns or de facto sovereigns. Without case law or statutes to guide us, however, one can only speculate. The introduction of the Stuxnet virus into Iranian uranium centrifuges (attributed to Israeli and/or U.S. actors)[34] caused substantial property damage but no war was noted, notwithstanding the hostile relations among Israel, the U.S. and Iran. Was it a war-like operation? Certainly not in the traditional sense, and if ''ancient marine insurance terms'' control, then it was not in the modern sense either.

But what about terms not addressed in *Pan Am*, specifically: ''acts of foreign enemies?'' *Pan Am* did not construe the phrase. We can repeat the analysis above and require a traditional interpretation, or the acts of sovereigns, etc. Or we can go one better and eliminate it from the exclusion. ''War exclusions'' are not uniform; here is one contained in another cybersecurity policy:

> ''[This policy does not insure] any riot or civil commotion, outside the United States of America or Canada, or any military, naval or usurped power, war or insurrection.''[35]

Notwithstanding the crisp analysis that we have written, one thing is certain: there is uncertainty. The sovereign state, terrorists and rebel faction in our scenario are foreign and an enemy as evidenced by the havoc they have wrought. But are they a ''foreign enemy'' within the meaning of a cybersecurity policy? While lawyers may relish the thought of making the arguments for and against, policyholders do not. To the extent it is obtainable, policyholders want certainty. To achieve that goal, at the very least, the war exclusion needs to be carefully reviewed when purchasing a cybersecurity policy.

While it is probably a certainty that the exclusion cannot be removed, it might be tweaked, such as, for example, by removing vague phrases like ''foreign enemies'' or by specifying that the exclusion is not meant to apply except in conjunction with an attack with conventional means of war. One might even consider engaging a different insurer with narrower war exclusion language (assuming other terms and conditions were satisfactory). Proper prior planning prevents poor performance. Where the application of the war exclusion is untested and questions concerning its interpretation may be imagined, the proper procurement of cybersecurity insurance is imperative.

---

[29] *Id.* at 1503.

[30] *Id.See also Sherwin-Williams Co. v. Ins Co. of State of Pa.*, 863 F. Supp. 542 (N.D. Ohio 1994) (finding war exclusion applied but endorsement bought back coverage); *Younis Bros. & Co. v. CIGNA Worldwide Ins. Co.*, 899 F. Supp. 1385 (E.D. Pa. 1995) (applying war risk exclusion to ''insurrection'').

[31] David Kushner, *The Masked Avengers: How Anonymous Incited Online Vigilantism from Tunisia to Ferguson*, New Yorker (Sept. 8, 2014).

[32] Nicole Perlroth & David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, N.Y. Times (Aug. 5, 2014).

[33] Damian Paletta, *FBI Director Sees Increasing Terrorist Interest in Cyberattacks Against U.S.*, Wall Street Journal (July 22, 2015).

[34] Ellen Nakashima & Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say*, Washington Post (June 2, 2012).

[35] Chubb Insurance Company, Cybersecurity by Chubb Specimen Policy ¶ III.4.d.

  PVLR ISSN 1538-3423