ARE CYBER WAR & CYBER TERRORISM INSURABLE?

Privacy, Data Breach & Cybersecurity Alert
February 10, 2015

The frequency of cyber war and terrorism is no longer the risk. The magnitude of the potential damages is the real threat.

It's conceivable that an enemy of the U.S. government could hack a U.S. energy, water, or fuel distribution system causing loss of life, severe physical damage to property, or insurmountable financial damage to a non-government business. In 2007, the Department of Homeland Security conducted the "Aurora Generator Test" involving the turbine of an electricity generator that burst into smoke in the Idaho National Laboratory, ultimately causing failure of the device. Engineers determined that by simply changing the operating cycle of a power generator remotely via computer, the turbines could set fire, eventually destroying the machine. For a public or private company, the concern is whether a cyberattack on the U.S. government causing ancillary damage is insurable under a cyber liability insurance policy. The answer is not black and white.

This article explores that concern. First we examine the U.S. government's definition and position on cyber war and terrorism. Second, we analyze the application of a war and terrorism exclusion under a cyber liability policy to the foregoing scenario.

The U.S. Government

Although the government's definitions of *cyber war* and *cyber terrorism* are limited in scope to attacks on the U.S. government, the government's definitions are a useful resource in analyzing whether a war and terrorism exclusion would apply to bar coverage to a public or private company under a cyber liability policy.

What Is the Government's Definition of Cyber Terrorism?

Cyber terrorism is damaging computer-based attacks or threats of attack by non-state actors against information systems, conducted to intimidate or coerce governments or societies in pursuit of political or social goals. The FBI defines cyber terror as "the use of computer network tools to shut down critical national infrastructures—energy, transportation, government operations—or to coerce or intimidate a government or civilian population."[1]

Practices & Industries

Cybersecurity & Privacy

At a 2012 cybersecurity insurance workshop hosted by the Department of Homeland Security's National Protection and Programs Directorate, the majority of attendees believed that "catastrophic" cyber risks that the federal government should be responsible for (e.g., war, terrorism, critical infrastructure failure, "in the wild" and state-sponsored computer viruses) are currently uninsurable. Before denying coverage under a terrorism and war exclusion, carriers must evaluate, among other things, whether: 1) it's clear that an act of terrorism or war has occurred, and 2) a more specific exclusion addressing cyber terrorism or war is included in the policy. Yes, the United States is able to pinpoint the origination of a cyberattack by a foreign enemy, but will cyber liability insurance cover the risk of loss?

What Is the Government's Position on Cyber War & Terrorism?

The threat of future terrorism will come in the form of a cyberattack that could cause massive destruction. Below, is a brief outline of the government's position on cyber war and terrorism.

- **Department of Defense.** Cyberattacks are "acts of war" because the attacks are military operations or warlike actions brought by or at the behest of foreign enemies. Terrorism is defined as "the unlawful use of—or threatened use of—force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious or ideological objectives."[2]

- **Department of Justice.** The FBI defines cyber terrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents."[3]

- **Department of Homeland Security**. The U.S. National Infrastructure Protection Center, formerly a part of DHS, defined cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies."[4]

With this scenario looming, a public or private company must evaluate whether the government's position on a cyberattack impacts the application of the war and terrorism exclusions in a cyber liability insurance policy.

Does a Cyber Liability Policy Cover a Cyber War or Terrorism?

The language in a cyber liability policy varies from policy to policy depending on the carrier. Cyber liability policies typically contain a "war exclusion." The ISO cyber policy form contains a war exclusion stating: "We will not be liable for "defense expenses" or "loss". . .based upon, attributable to or arising out of. . .[w]ar, including undeclared or civil war or civil unrest."

But, the courts have traditionally interpreted such "war" and "warlike actions" as events involving two sovereigns or quasi-sovereign governmental entities. Without direct involvement by a sovereign state, the war-risk exclusion would not generally bar coverage. For example, in *Pan American World Airways, Inc. v. Aetna Casualty & Surety Co.*,[5] the U.S. Court of Appeals for the Second Circuit held that war required the hostile engagement of a sovereign or quasi-sovereign nation. The court concluded that terrorist acts against civilians by operative of a political organization or guerilla group cannot be characterized as war or warlike operations. This narrow interpretation traditionally limited the scope of the war exclusion.

The Second Circuit in *In re September 11 Litigation*,[6] loosened the narrow reading of the exclusion. The court determined that the "act of war" exception to Comprehensive Environmental Response, Compensation and Liability Act liability (CERCLA) applied to claims stemming from 9/11. In construing the statute's act-of-war clause, the court distinguished the *Pan Am* decision and insurance-related precedent requiring a state actor to conduct war. The court reasoned that the elaborate and well-planned 9/11 attacks were carried out by an extra-national terrorist organization that had declared war on the United States and intended to bring down its leading commercial and political institutions. The court recognized that warfare is often waged by irregular forces who can cause extraordinary damage. As such, and because of the United States' response to 9/11, the court concluded that the 9/11 attacks were acts of war. The expansion of the war risk exclusion to encompass irregular forces or terrorists may limit insurers' cybersecurity losses.

As for terrorism, the ISO cyber policy form does not have exclusions automatically built in. Instead, each insurance company decides if it would like to add ISO's form exclusionary language to its cyber policies. Since the passage of the Terrorism Risk Insurance Act (TRIA), many terrorism risk exclusions bar recovery for injuries or damages arising, directly or indirectly, out of acts of terrorism as determined or "certified" by the secretary of the U.S. Treasury. The secretary of the Treasury has not certified a cyberattack as an act of terror. Not all terrorism risk exclusions, however, are tied to the secretary of the Treasury's certification process. Some exclusions preclude coverage for noncertified terrorist events. These exclusions are likely much more powerful in limiting exposure to cyber terrorist attacks.

TRIA-related rules contain certain definitions, requirements, and procedures for insurers filing claims with the Treasury for payment of the federal share of compensation for insured losses under the Terrorism Risk Insurance Program. The claims procedures rule specifically addresses requirements for federal payment, the submission of an initial notice of insured loss, loss certifications, the timing and process for payment, and associated recordkeeping requirements, as well as the department's audit and investigation authority. These procedures will apply to all insurers that wish to receive their payment of the federal share of compensation for insured losses under TRIA.

The current form does not, however, rule out coverage for hacking by a foreign enemy even if such hacking is deemed an act of terrorism or war. For example, the ISO form[7] "Exclusion of Terrorism" states that the exclusion applies only when one or more of certain circumstances are attributed to "terrorism" such as "[t]he total of insured damage to all types of property exceeds $25,000,000" or "[f]ifty or more persons sustain death or serious physical injury." Thus, only if the hacking met such conditions would the exclusion apply.

Conclusion

This issue has no simple conclusion given the increased frequency and severity of cyberattacks. Courts are faced with the challenge of interpreting whether a war and a terrorism exclusion limits coverage under a cyber liability policy when a foreign enemy attacks the U.S. government, causing damage to a public or private company. If a company has a cyber liability policy, the prudent course of action is to negotiate the inclusion of cyber war and terrorism coverage to avoid the risk of loss from the secondary physical or financial damage to a public or private company caused by a war or terrorist act on the U.S. government

[1] The FBI Law Enforcement Bulletin, an article entitled "Cyber Terror" by William L. Tafoya

[2] Hoffman, Bruce. "Inside Terrorism." Columbia University Press, 1998 . Web. .

[3] Singer, Peter W. "The Cyber Terror Bogeyman." Brookings.com, November 2012. Web. .

[4] Kostadinov, Dimitar. "Cyberterrorism Defined (as distinct from 'Cybercrime')." Infosec Institute, 21 December 2012. Web. .

[5] 505 F.2d 989 (2nd Cir. 1974).

[6] 931 F. Supp. 2d 496 (S.D.N.Y. 2013)

[7] Form No. EC 21 09 07 06