SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

WAR EXCLUSIONS AND CYBER THREATS FROM STATES AND STATE-SPONSORED HACKERS

VINCENT J. VITKOWSKY

New York Connecticut New Jersey

War Exclusions and Cyber Threats from States and State-Sponsored Hackers

Vincent J. Vitkowsky

Introduction

States and groups supported or sponsored by States have become important sources of cyber attacks affecting private business.

Senior security officials in the U.S. and Europe confirm that States have provided sophisticated cyber malware to criminal and activist groups, who then conduct cyber operations on behalf of the States. That is, cyberattacks are outsourced to "cyber privateers".[1] A recent regulatory decision, several federal criminal indictments, and state of the art cyber forensics have made it substantially clear that States are indeed responsible for many cyber operations directed at private business. Many of these have financial consequences that are within the initial coverage of cyber and other insurance policies, such as breach notification, network disruption, and business interruption. These cyber operations may or may not fall within the scope of War Exclusions in cyber and other insurance policies.

Attacks with Links to States

China

One of the largest data breaches in history involved Anthem Blue Cross Life and Health Insurance Company. It compromised the protected medical information of almost 80 million people.

The California Department of Insurance was one of the seven U.S. insurance departments leading the national investigation of the breach. It engaged a forensic examination team that included the cybersecurity firm Crowdstrike, which specializes in attribution to States, and Alvarez and Marshall Insurance and Risk Advisory Services LLC. In its Press Release announcing the overall Regulatory Settlement Agreement, the California Department quoted its Commissioner as saying that "our examination team has concluded with a significant degree of confidence that the cyber attacker was acting on behalf of a foreign government. Insurers and regulators alone cannot stop foreign government assisted cyber attacks." Elsewhere the Press Release stated that "[T]he [examination] team determined with a high degree of confidence the identity of

[1] Sam Jones, *Cyber Crime: States Use Hackers to Do Digital Dirty Work*, **Financial Times**, September 4, 2015.

the attacker and concluded with a medium degree of confidence that the attacker was acting on behalf of a foreign government. There is some potential inconsistency in these statements, notably with respect to how an examination determining something with a "medium degree of confidence" can support a conclusion with a "significant degree of confidence." But the overall message was clear.[2]

In April 2017, PwC issued a report in collaboration with BAE Systems, working closely with the UK's National Cyber Security Centre. The report is entitled *Operation Cloud Hopper,* and stated that the Chinese-based group known as APT 10 has been conducting a widespread cyber operation against companies in 15 countries, including the U.S., the U.K., and France.[3] It noted that in addition to Anthem, several other healthcare firms were targeted by organizations with links to China. These included Premera, Blue Cross and CareFirst.[4]

Russia

Russian groups have been leaders in cybercrime from the beginning.

Russian State involvement has recently been brought into sharp focus. In a criminal indictment released on March 15, 2017, U.S prosecutors described in detail Russia's involvement in the hack of Yahoo, which affected 500 million emails accounts and targeted, among others, business executives, for financial gain. The indictment provides significant insight into Russian State-sponsored hacking.[5]

The indictment alleged that the Russian Federal Security Service (FSB), which is the successor to the KGB, recruited leading cybercriminals. The indictment alleges that the FSB recruited the Latvian Alexsey Belan, who in 2012 and 2013 breached American e-commerce businesses, stealing user databases for the purpose of selling them. The U.S. issued warrants for Belan's arrest, and he was arrested in Greece. Before he could be extradited, he escaped to Russia. Instead of arresting him, Russia recruited him to its Centre for Information Security and provided him with sophisticated hacking tools. By the end of 2014, he had completed the Yahoo hack. The empowered Belan was working on private projects as well. It is alleged that in November 2014, he modified the code for Yahoo's search engine so that users searching for erectile dysfunction drugs were directed to a specific online pharmacy, for which he was paid a commission.

---

[2] *Investigation of major Anthem cyber breach reveals foreign nation behind breach*, California Department of Insurance Press Release, Jan. 6, 2017, available at http://www.insurance.ca.gov/0400-news/0100-press-releases/2017/release001-17.cfm.

[3] *Operation Cloud Hopper* at 10, available at https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html.

[4] *Id.* at 14.

[5] https://www.justice.gov/opa/press-release/file/948201/download.

The indictment also named FSB intelligence officers Dmitry Dokuchaev and Igor Sushchin. It is noteworthy that the FSB unit involved is the FBI's point of contact in Russia for law enforcement cooperation related to computer crimes.[6]

North Korea

There are strong indications that North Korea is engaged in a far-ranging effort to steal money from banks and casinos. There is speculation that the proceeds are being used to fund its nuclear program.

Kapersky Lab has reported that a North Korean group known as Bluenoroff, a subgroup within the Lazarus group, is solely engaged in cybercrime and has targeted banks, casinos, and crypto-currency firms in over a dozen countries. On April 3, 2017, at its security conference, a Kapersky researcher said that North Korea may have been responsible for the theft of $81 million from the Bangladesh Central Bank in February 2016.[7] Kapersky obtained digital records showing that a European server used in the theft had exchanged data with a computer that had an Internet address belonging to North Korea's State-owned Internet service provider. The researcher said that apart from the State-owned company, North Korea has "very little presence on the Internet, and the chances that this is just a random connection are extremely small."[8]

In February 2017, another leading cybersecurity firm, Symantec, found a suspected link between the group and a Polish bank, and reported that North Korea has targeted more than 100 organizations in 31 different countries. In addition, BAE issued a less definitive report that linked Lazarus malware to attacks on 15 U.S. banks, 7 U.K. banks, 19 Polish banks, and 9 Mexican banks.[9]

Previously, North Korea was famously linked to the attack on Sony Pictures in 2014, which reverberated throughout the movie industry and included cyber sabotage like hard drive disk wiping. It has been reported that in March 2017, Richard Ledgett, a deputy director at the National Security Agency, said that research linked the Sony Pictures attack and the Bangladesh theft. He also affirmed that he believed states were now robbing banks.[10]

---

[6] Charley Snyder and Michael Sulmeyer, *The Department of Justice Makes the Next Move in the U.S.-Russia Espionage Drama*, **Lawfare**, March 16, 2017, available at www.lawfareblog.com.

[7] *Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies*, April 3, 2017, available at www.kapersky.com.

[8] Robert McMillan, *Cyberattack on Bangladesh tied to North Korea*, **Dow Jones News Service**, April 4, 2017. Jason Murdock, *North Korean worldwide hacking rampage steals millions from casinos and banks*, **IB Times**, April 4, 2017.

[10] Paul Mozur, *North Korea's rising ambition seen in bid to breach global banks*, **New York Times Online**, March 26, 2017.

It is also significant that the malware used in both the Sony and Bangladesh exploits used codes and codebases that were not being shared on underground forums. That is, they are closely guarded, which further suggests that a State is involved.[11]

Iran

On March 24, 2016, the U.S. Government announced an indictment accusing seven Iranian hackers of coordinating cyber attacks on dozens of U.S. banks from 2011 to 2013, using distributed denial of service attacks to cause millions of dollars in lost business. The hackers were also accused of accessing the control system of a dam in Rye Brook, New York, which they tried to shut down. The hackers were believed to have been working on behalf of the Iranian government and the Islamic Revolutionary Guard.[12]

Iran is also believed t have attacked numerous government agencies and vital facilities in Saudi Arabia in mid- to late 2016, destroying numerous computers by wiping the master boot records used to start up.[13] The hackers appeared to use an updated version of the "Shamoon" virus that was used in 2012 to attack the oil company Saudi Aramco. It rendered computers permanently inoperable.

Syria

On March 22, 2016, the U.S. Government released two criminal indictments against three alleged members of the Syrian Electronic Army, a group that publicly proclaims that its hacks are conducted in support of President Bashar al-Assad. The indictment alleges that one member of the group hacked at least 14 private companies in the U.S. from which he extorted money.[14]

Framework for Analysis

At least some of these attacks, and undoubtedly other attacks in the future, may be subject to War Exclusions.

The interpretation and application of War Exclusions is an exercise undertaken initially by claims executives, and ultimately by the courts.

The most important factor in the exercise, of course, is the language of the particular War Exclusion at issue. Next is the application of relevant case law, but that is sparse,

---

[11] Andrea Peterson and Ellen Nakashima, *The hackers that took down Sony Pictures are still on the attack, researchers say*, **The Washington Post,** February 24, 2016.
[12] https://www.justice.gov/usao-sdny/file/835061/download.
[13] Jim Finkle and Jeremy Wagstaff, *Shamoon virus returns in new Gulf cyber attacks after four-year hiatus*, **Reuters Technology News**, Dec. 1, 2016; Julianne Geiger, *Saudi Arabia Blames Iran for Serious Cyber Attacks*, **Oilprice.com**, Dec. 2, 2016.
[14] https://www.justice.gov/opa/file/834271/download; https://www.justice.gov/opa/file/834276/download.

and insurance coverage law is subject to differing interpretations and applications across U.S. jurisdictions.

There are two other important factors. One is the extent to which a particular cyberattack can be characterized as an "Act of War" as a matter of U.S. Government policy and the international law of armed conflict. The second is the extent to which an accurate attribution can be made, establishing a link to the foreign government.

Policy Language

War Exclusions typically cover more than large scale, fully-declared wars between States. They often exclude acts such as the following: hostilities or warlike operations (whether declared or not); military operations; damage to property by or under order of any government; acts of foreign enemies; any action taken to hinder or defend [against these events]; or actions in hindering or defending against actual or expected attack by any government, sovereign, or other authority using military personnel or other agents.

U.S. Case Law

There are only a few cases with potential application to State-sponsored hackers. Under the case law, "hostilities" have been construed more broadly than "war." They include operations that are "either offensive, defensive, or protective," and the weapon used need not be in itself capable of inflicting harm.[15] There is authority for the proposition that a single individual may engage in an "Act of War" if performed "under order of a commanding officer and sanctioned by a recognized government."[16] Also, a War Exclusion has been applied to acts of looters who were agents of the Panamanian government (the case arose in the context of ongoing military hostilities).[17]

International Law of Armed Conflict

The commonly used phrase "Act of War" is a term with political and colloquial meaning, but not legal meaning in international law. It is generally used by political leaders to characterize an act of significant hostility and magnitude which warrants the most serious response. But under international law, the operative standard is whether an action constitutes an "armed attack" under United Nations Charter. If it does, a State may respond with armed force in self-defense. [18]

---

[15] *Int'l Dairy Eng'g Co. v. Am. Home Assurance Co.,* 352 F. Supp. 827, 829, *aff'd* 474 F. 2d 1242 (9th Cir. 1072).
[16] *Thomas v. Metro. Life. Ins. Co.,* 131 A.2d 600, 606 (Pa. 1957).
[17] *TTR/FTC Communications, Inc. v. Ins. Co. of the State of Pennsylvania,* 847 F. Supp. 289 (D. Del. 1993).
[18] If an attack does not amount to an armed attack, it may still violate international law principles, or a State's domestic law. In those cases, States can respond with "countermeasures," which are acts that are designed to bring the attacker into compliance with international law, but that in other circumstances would themselves violate international law. And acts that do not violate international law but may be perceived as hostile, such as espionage, can be met with "retorsion", which are unfriendly but legal acts, such as expelling diplomats or imposing sanctions. See Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rule 20 (countermeasures) and Rule 20, Note 4 (retorsion).

As the domestic case law demonstrates, under the language of a particular War Exclusion, attacks far short of a large scale military assault may trigger the Exclusion. Nonetheless, the closer the attack comes to constituting an armed attack under international law, the stronger the case for applying a War Exclusion.

The U.S Government's view of what kind of cyber attacks would constitute an armed attack has evolved in the last few years. The U.S. first addressed this issue in 2012, in a speech given by then-State Department Legal Advisor Harold Koh, in which he said that a cyber attack may constitute an armed attack if "the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons".[19] "Kinetic weapons" means, in essence, bullets, bombs, and other traditional implements of war.

The U.S. Government has refined this positon in subsequent statements. For example, in 2016, in a response to questions posed in connection with testimony before the House Armed Services Committee, Thomas Akin, acting assistant secretary of Defense for homeland defense and global security, elaborated as follows:

> When determining whether a cyber incident constitutes an armed attack, the U.S. Government considers a number of factors including the nature and extent of injury or death to persons and the destruction of, or damage to property … Besides effects, other factors may also be relevant to a determination, including the context of the event, the identity of the actor perpetrating the action, the target and its location, and the intent of the actor, among other factors."[20]

These standards leave some key matters open for interpretation. Notably, they do not provide a definitive statement on how to treat cyber incidents that do not have itangible kinetic effects, but still cause grave real-world harm. These might include, for example, an attack causing widespread and extended disruption of banking and financial services. Or a ransomware attack threatening the destruction or public disclosure of medical data on a widespread scale, such as the records of every major hospital in the Northeast. Such attacks might be considered armed attacks of the type that constitute an armed attack.

One of the leading sources of the understanding of how international law applies to cyber conflict is the *Tallinn Manual*. This Manual is the product of consultations by leading international law professors, meeting in Tallinn, Estonia, under the aegis of the NATO Cooperative Cyber Defense Center for Excellence. The Manual was first

---

[19] Harold Hohgju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOMM Inter-Agency Legal Conference (Sept. 18, 2012.) This position has also been stated in the Department of Defense Law of War Manual (Dec. 2016 edition) and Paper submitted by the United States to the 2014-15 UN Group of Governmental experts (Oct. 2014).

[20] U.S. Government Publishing Office, Hearing on *Military Cyber Operations*, House of Representatives Committee on Armed Services, held June 22, 2016.

released in 2013, and was then called *Tallinn Manual on the International Law Applicable to Cyber Warfare.* In 2017, the Second Edition was released, and it is called *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* It expanded the scope of the first Manual to encompass international law pertaining to cyber activities during peacetime. The Manual sets forth a series of Rules that represent the consensus among the experts on the current standards under customary international law (international law as reflected by State practice and a sense of legal obligation), as applied to cyber operations. The Rules are elaborated on by a series of Notes.

Tallinn Manual 2.0 does not state the official policy of NATO or any other entity. Instead, it reflects the perspectives of a group of experts and is intended as a guide to assist state legal advisors in analyzing issues. In fact, the Tallinn process itself revealed gray issues on which the answers are not clear, and on which the drafters themselves were unable to reach consensus. One of those areas concerns the destruction of civilian data. There are indications that an attack on data, and specifically medical data, would be an armed attack, or at least a violation of international law.

Rule 92 defines "cyber attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." Such an operation would constitute an armed attack. Note 6 to the Rule states that the reference to individuals or physical objects "should not be understood as excluding" cyber operations against data from qualifying as an attack. If an attack on data "foreseeably results" in injury, death, damage or destruction, the operation qualifies as an armed attack. And "an operation against data on which the functionality of physical objects relies can sometimes constitute an attack."

Rule 99 prohibits attacking "civilian objects" during an armed conflict. Rule 100 provides that "Cyber infrastructure may qualify as a military objective," and thus be a legitimate subject for targeting. But consensus could not be reached as to the status of data. Note 6 to Rule 100 says that the majority of experts take the view that because data is intangible, the notion of "object" does not include data, so an operation directed toward data *per se* does not qualify as an prohibited armed attack, unless the operation fits into one of the categories in Rule 92, Note 6 (see above). However, Note 7 states that a minority of experts hold the view that the deletion of "essential civilian datasets such as social security data, tax records, and bank accounts" should be regarded as an attack on protected civilian objects. For them, the "key factor … is the severity of the operation's consequences, not the nature of the harm." The position of the U.S. Government broadly aligns with the minority.

Thus, whether or to what extent international law applies to operations targeting data *per se* is currently unclear, and open to differing conclusions. It is certainly arguable that an attack affecting the integrity of key financial records is a "cyber armed attack," *i.e.*, colloquially, an Act of War.

Another frequent target of criminal hackers is medical information. Ransomware exploits sometimes threaten to make protected medical information public, or even delete medical information. As this paper is being written, such a scenario is playing out in the spread of the WannaCry virus, with suggestions of possible State involvement.[21] In the context of an ongoing cyber armed conflict between States, Rule 132 prohibits attacks on "computers, computer networks, and data that form an integral part of the operations or administration of medical units and transports." It applies to both military and civilian "medical units." Note 3 explains that the "data" referred to is essential data, and gives the examples of "data necessary for the proper use of medical equipment and tracking the inventory of medical supplies." It states that "[P]ersonal medical data required for the treatment of patients is likewise protected from alteration, deletion, or any other act by cyber means that would negatively affect their care, regardless of whether the act amounts to a cyber attack."

It bears repetition that an act need not be an armed attack, or "Act of War'", to qualify as an act that is within the scope of a given War Exclusion. But it certainly supports such a conclusion.

Attribution Issues

One of the challenging technical issues has been accurately identifying the source of a cyber attack. This is called "Attribution." While challenging, it is not impossible. The California Insurance Department was sufficiently satisfied to make decisions to reduce the severity of fines against Anthem because it recognized that effective preventive measures against a State-grade attack are limited. And through its indictments, the U.S. Department of Justice has made it clear that it expects to be able to establish attribution beyond a reasonable doubt. Former government officials have stated that it is clearly possible for states and private companies to attribute hacks. They have said that "[T]he real question is not if states can attribute cyber attacks, but if they will publicly do so."[22] Where attribution is not made, the reasons are often political considerations or concerns about revealing sources and methods.

Many of the same resources used by the Government to make attributions are equally available to private companies. An example is the cyber forensic firm Crowdstrike, and others of similar caliber.

The attribution need not be made to a level of metaphysical certitude. Like everything else involving courts, it is a matter of proof. Insurers have the burden of proving the application of an exclusion. In some jurisdictions, the formulation of the standard can seem daunting. Yet in the real world, insurers routinely succeed in enforcing

[21] Ellen Nakashima, Craig Timberg and Paul Schemm, *Clues point to possible North Korean involvement in massive cyberattack*, **The Washington Post**, May 15, 2017.
[22] Michael Sulmayer and Amy Chang, *Three Observations on China's Approach to State Action in Cyberspace*, **Lawfare**, January 22, 2017, available at www.lawfareblog.org.

exclusions, often after a contested proceeding on the facts. So this, too, is challenging but not impossible.

To Cover or Not to Cover?

There has been pressure from insureds and brokers to remove the War Exclusion in cyber policies, or to limit its application to instances in which there is an official declaration of war. This limitation would virtually eviscerate the War Exclusion. Although U.S. troops have gone to war many times, there have only been 11 congressional declarations of war in U.S. history. Today, it would require extraordinary circumstances to compel Congress to make such a declaration. There is virtually no chance it would do so in response to a cyber operation affecting data or networks, but not resulting in enormous damage and economic loss.

The rationale for continuing the War Exclusion is that it is extremely difficult, if not impossible, to protect against State grade-attacks, so corporations cannot take, or be encouraged to take, effective defensive measures by regulators or cyber insurers. It is impossible to underwrite against a State-sponsored attacks. Also, the potential scope of a state-sponsored attack could be enormous, and potentially destabilize the cyber insurance market. Again, consider the example of the scope of loss resulting from a data dump or destruction of records of every major hospital in the East Coast of the U.S.

Ultimately, insurers and their reinsurers need to decide what types and scale of risk they are willing to accept, and draft their War exclusions accordingly. When drafting, they may wish to expressly address the status of all data, and medical computer networks and data in particular.

May 16, 2017

Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He represents insurers and reinsurers in coverage matters across many lines of business, including cyber, CGL, and professional liability. He also defends insureds in complex claims. Vince Chairs the International & National Security Law Practice Group of the Federalist Society and has been an Adjunct Fellow at the Center for Law and Counterterrorism. His email address is vvitkowsky@sgllawgroup.com, and he can be found on Twitter @vince_vitkowsky.