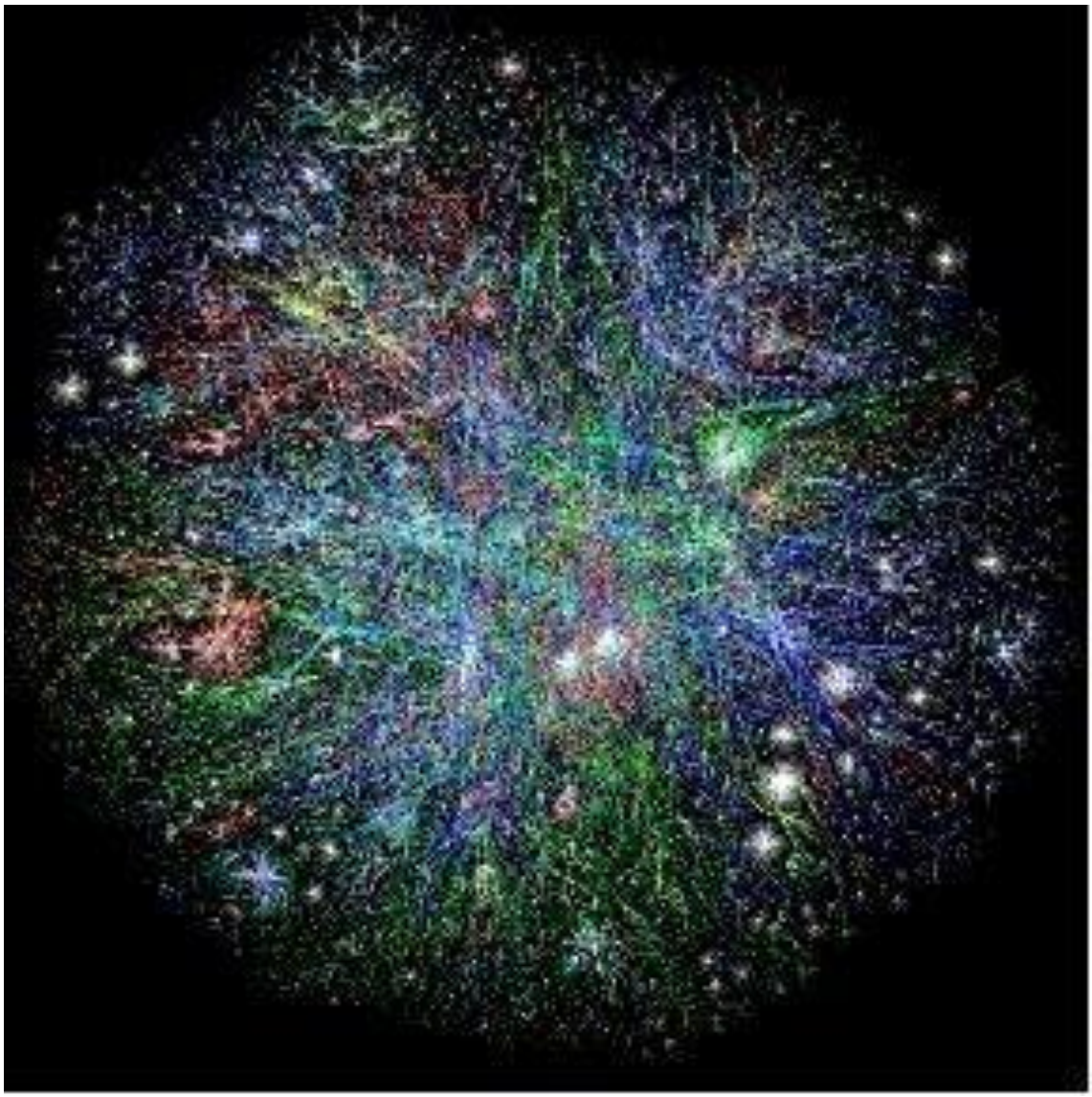
SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

WAR, TERRORISM, AND HACKTIVISM UNDER CYBER INSURANCE POLICIES

VINCENT J. VITKOWSKY



New York Connecticut New Jersey

WAR, TERRORISM, AND HACKTIVISM UNDER CYBER INSURANCE POLICIES

VINCENT J. VITKOWSKY

Cyberspace is the world's most dynamic domain, and cyber insurance is the industry's most dynamic product. So far, insurance has focused on losses from data breaches and network disruption. But as hackers move from information technology to operational technology, some insurers are starting to provide coverage for losses from cyber exploits resulting in bodily injury and property damage. All of these exposures can arise through activities by the full range of actors – from lone wolf teenage joyriders through highly organized national military units.

Most cyber insurance policies contain broad war exclusions. Some are silent on terrorism, others contain terrorism exclusions, and only a few affirmatively grant terrorism coverage. Most often, hacktivism is not addressed directly.

The application of war and terrorism exclusions and grants will depend on several factors. The first is the policy language, which will be construed in part by reference to existing case law. The second is the nature and effect of the exploit. Is it an act of war, terrorism, hacktivism, or something else? The third is the nature of the actor. Is it a nation state, an organized non-state entity, a loose collective, or an individual? What is its relationship with a nation state? What is its purpose and intent? Blurred lines will create challenging issues.

Policy Language

Cyber insurance policies do not have uniform wordings. Some policies use standard exclusions developed for traditional lines of business. Others are bespoke.

Some of the terms appearing in war exclusions include the following:

- war
- hostilities or warlike operations (whether declared or not)
- military operations
- military uprising [sometimes, rising]
- military or usurped power
- damage to property by or under the order of any government
- acts of foreign enemies
- political disturbance
- popular uprising
- insurrection
- rebellion
- revolution
- any action taken to hinder or defend against these events, [or alternatively]
- action in hindering or defending against an actual or expected attack by any government, sovereign or other authority using military personnel or other agents.

Terrorism exclusions are often structured along the following lines:

- an act of any person or group of persons
- whether acting alone or on behalf of or in connection with any organization or government
- committed for political, religious, ideological or similar purpose
- including the intention to influence any government
- or to put the public, or any section of the public, in fear.

The Case Law

The interpretation of policy language is a matter of state insurance contract law. This means there is no single answer to any question. Different facts, analytical approaches, and judges produce different results.

Even so, the starting point will be the existing cases construing war exclusions. They make distinctions among the types of actors who might fall within them. Distilled to their essence, the existing cases provide a few potentially useful principles, not all of which are consistent.

The leading case is *Pan American World Airways Inc. v Aetna Casualty and Surety Co.* It involved the hijacking and destruction of a jet airplane by the terrorist organization known as the Popular Front for the Liberation of Palestine, a PLO affiliate. The case arose in the influential Second Circuit, and the Court applied New York law. Among its key holdings is that to qualify as "war," or as the exercise of "military or usurped power," an act must be performed by a sovereign or an organization having sufficient indicia of sovereignty to be at least a de facto government.[1]

Another leading case held that both sides involved in a conflict must be sovereigns.[2]

However, another court applied Delaware law to apply a war exclusion clause to acts of looters who were "enabled by the military hostilities between Panama and the U.S." It found the looters were agents of the Panamanian government, but in *dicta* suggested that this agency was not essential to triggering the exclusion.[3]

Mere financial support from a government to a terrorist organization does not bestow sovereign or quasi-sovereign status on the terrorists.[4]

However, the *Pan American* court noted that the PFLP had never acted on behalf of a recognized government. This suggests that if it had such an agency relationship, there might have been sufficient indicia of quasi-sovereignty to trigger the war exclusion.

---

[1] 505 F. 2d 989, 1006 (2nd Cir. 1974).
[2] *Holiday Inns Inc. v Aetna Insurance Co.*, 571 F. Supp 1460, (S.D.N.Y. 1983) (involving fighting among three factions in Lebanon).
[3] *TTR/FTC Communications Inc. v Insurance Company of the State of Pennsylvania*, 847 F. Supp 289 (D.Del 1993).
[4] *Pan American*, 505 F.2d at 1014.

A single individual may engage in an "act of war" if performed "under orders of a commanding officer and sanctioned by a recognized government."[5]

"Insurrection" requires that a group engage in hostilities with the intent to overthrow a government. *Pan American*, 505 F. 2d at 1017-18.

"Hostilities" are 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.[6]

The Nature and Effect of the Exploit

War

Under international law, "war" typically entails a use of armed force that would warrant the use of armed force in response. This is analyzed under a conceptual framework known variously as "The Law of Armed Conflict" ("LOAC"), "International Humanitarian Law", or colloquially, "War Law". This law is only partially codified. The United Nations Charter (which is in essence a treaty among nations) provides some guidance. Article 2(4) generally prohibits the "threat or use of force against the territorial integrity or political independence of any state." But Article 51 preserves the "inherent right of individual or collective self-defense if an armed attack occurs". This "inherent right" includes the rules of "customary international law," which consists of generally accepted law as demonstrated by the actual conduct of nations, and the statements they make.[7]

The United States Government ("USG") has expressed its views in so-called "canonical law" through speeches by senior officials in the Obama Administration. On September 18, 2012, Harold Koh, Legal Advisor to the US State Department, gave a speech entitled *International Law in Cyberspace*. He said, in essence, that the USG position is that the principles of the LOAC apply in cyberspace. Specifically, cyber exploits may sometimes constitute the use of force within the meaning of Article 2(4) of the UN Charter 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." ("Kinetic weapons" means, in essence, bullets, bombs, and other traditional implements of war.) He went on to say that "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force." The Article 51 right of self-defense "may be triggered by computer network activities that amount to an armed attack or imminent threat thereof".[8]

---

[5] *Thomas v. Metro. Life Ins. Co.*, 131 A.2d 600, 606 (Pa. 1957).
[6] *Int'l Dairy Eng'g Co. v. Am. Home Assurance Co.,* 352 F. Supp 827, 829, aff'd 474 F.2d 1242 (9th Cir, 1973).
[7] More detail on the application of this conceptual framework can be found in Vincent J. Vitkowsky, *Remarks on Customary International Law and the Use of Force Against Terrorists and Rogue State Collaborators*, ILSA Journal of International & Comparative Law, Vol. 13.2 (2007): p. 371.
[8] The entire speech can be found at http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace.

A few weeks after Koh's speech, Secretary of Defense Leon Panetta also addressed cyber doctrine in an October 11, 2012 speech. He warned that aggressor nations or extremist groups could use cyber tools to create a "Cyber-Pearl Harbor" that would cause physical destruction and the loss of life. He said that the US has the capacity to detect an imminent threat of attack, and the "capability to conduct effective operations to counter threats." That is, the US has the capacity to take preemptive action against a threat. This concept is known as "active defense."[9]

Under this framework, the Pentagon has been developing rules of engagement for military operations in cyberspace. NATO also has undertaken a similar process, through a group of international law practitioners and scholars who have a produced document called *The Tallin Manual on International Law Applicable to Cyber Warfare*. That Manual concludes that Stuxnet, which is understood to be a joint U.S.-Israeli cyber exploit that successfully sabotaged Iranian nuclear reactors, constituted an "act of force" and was likely illegal under international law.[10]

However, as noted, international law develops through the conduct and responses of nations. As a result, like everything else involving cyberspace, the application of cyberwar concepts and doctrines will be subject to considerable evolution and refinement over time.

Moreover, there is a credible counter-argument against the basic premise that the LOAC should apply to cyber exploits. Some scholars argue that the very essence of the LOAC is that nations should use proportionality and distinction in responding to an armed attack or an imminent threat. That is, force should be met by proportional measures of force, and care should be taken to avoid unnecessary collateral damage to civilians. Yet given the nature of cyber exploits, it is currently impossible to apply these principles. Once a cyber exploit is launched, there is no way to keep it from going "into the wild," *i.e.,* from moving beyond the intended targets to other networks, including civilian networks. Under this analysis, an entirely new framework would need to be developed.[11]

Nonetheless, under current USG doctrine, a cyberattack resulting in extensive bodily injury or physical damage, if launched by a nation-state, could be deemed an act of war. It seems clear that straightforward cyberespionage would not. Similarly, a denial of service attack would not likely be seen as an act of war. Nor would the destruction of data in networks. Questions could be raised about attacks that disable computers.

The conceptual flaw in this doctrine, of course, is that huge financial losses could occur even in the absence of direct physical effects. Recall that one false tweet from an AP account caused a $90 billion loss in the U.S. stock market.[12] Imagine the chaos coming from a computer bug

---

[9] The entire speech can be found at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[10] Shaun Waterman, *U.S.-Israeli cyberattack was an 'act of force,' NATO study found*, The Washington Times, March 24, 2013. This conclusion highlights an important aspect of international law. There is often a gap between what scholars believe and what political leaders do.

[11] Stephen L. Carter, *The World's Most Dangerous Software,* http://www.bloombergview.com/articles/2014-02-13/the-world-s-most-dangerous-software.

[12] htpps://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-white-house-wipes-billions-off-US-markets.html

that corrupted the records of a major stock exchange. The systemic shocks to the financial sector could be uniquely destructive.

Terrorism

There are various definitions of terrorism, but for insurance purposes, a key definition is contained in the Terrorism Risk Insurance Act ("TRIA") and its successor statutes, currently the Terrorism Risk Insurance Program Reauthorization Act ("TRIPRA"). That definition has two components. The first focuses on the effect of the act. It defines "act of terrorism" as an act that is dangerous to human life, property or infrastructure and results in damage within the US (or on a US flag vessel, aircraft or mission). The second component is intent. The act must be "committed by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the [USG] by coercion".[13] These are consistent with the essential terms used in many terrorism exclusions.[14]

Also, statutes such as the Anti-Terrorism Act define international terrorism to include providing material support or resources, including money, to terrorists.[15] They are of potential interest because cyber activities have been used to finance terrorist attacks. The Congressional Research Service has cited to press reports that the 2002 terrorist bombings in Bali were partially financed through online credit card fraud.[16] Similarly, it is believed that the Mumbai terrorist attacks were funded by an unidentified hacking group in Saudi Arabia.[17]

Hacktivism

Hacktivism is a recent development. It is generally understood to be hacking to promote social and political causes -- that is, hacking as a tool of activism. A favorite cause for hacktivists is "free speech," although as one commentator has observed, "the irony of shutting down websites you don't agree with in the name of free speech and transparency seems to be lost on many of them." [18]

Most often, hacktivists use non-violent techniques such as website defacement and denial of service attacks. But some hacktivist exploits have involved acquiring personal information, or other forms of cybercrime.

Sometimes hacktivists try to insert themselves into armed conflict. For example, members of Anonymous stated an intention to launch cyberattacks at nations they assert fund or arm the

[13] 31 CFR 50.5(b).
[14] It is unclear whether the insurance backstop provisions of TRIPRA would apply to a catastrophic cyber attack by terrorists. In theory they could, if the attack were to be certified by the requisite Cabinet officials. There have been calls to clarify this in any 2014 legislative renewal of TRIPRA, although they have not been heeded as of the date of this paper.
[15] 18 USC 2339A.
[16] Catherine A. Theohary and John Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace,* CRS Report for Congress, March 8, 2011.
[17] Matthew J. Schwartz, *AT&T Hackers Have Terrorism Ties, Police Say,* Information Week, November 28, 2011.
[18] Nate Anderson, *Who Was That Masked Man?,* Foreign Policy, January 31, 2012.

radical Islamic terror group known as the Islamic State in Iraq and Syria ("ISIS"), including Turkey, Saudi Arabia and Qatar.[19]

In terms of ends if not means, hacktivism is similar to terrorism, because its purpose is to attempt to influence public policy. This is likely to lead to some thorny interpretive issues.

The Nature of the Actor

The nature of the acts and their treatment under policy language will often depend on the identity, character, and intentions of the actor.

One of the historical challenges in cybersecurity has been "attribution," which means accurately identifying the source of a cyber exploit. Within the last few years, this challenge, though still substantial, has become less formidable. Given sufficient time and resources, proper attribution can be made. Secretary Panetta was clear about this in his October 11, 2012 address.[20]

Once the actor is identified, the analysis can become especially interesting. A review of some current actors shows why.

The Ajax Security Team. According the cybersecurity firm FireEye, this is the principal Iranian hacking group. Its exploits show a level of sophistication suggesting the involvement of a nation, but its precise links to the Iranian government are not in the public record. In addition to conducting espionage and infecting US computers with malware, it is believed to have been involved in online credit card fraud.[21]

Cyber Fighters of Izz ad-Din al-Qassam. This group claimed credit for the concentrated attacks on American banks in late 2012 and early 2013, purporting to be acting in protest of anti-Islam videos. Although there is some suggestion it is associated with Hamas, American intelligence officials believe it was actually a cover for the Iranian government, acting in retaliation for economic sanctions and cyberattacks by the US.[22]

The Syrian Electronic Army. This self-proclaimed virtual army purports to act on behalf of Syria, but its exact relationship to the Syrian government is not in the public record. So far has limited its activities to attacks on websites.

Nightmare. This group of pro-Palestinian cyberattackers has ties to a hacker named oxOmar, who posted the details of more than 20,000 Israeli credit cards.[23]

---

[19] Jasper Hamill, *Anonymous Hacktivists Prepare For Strike Against ISIS 'Supporters'*, http://www.forbes.com/sites/jasperhamill/2014/06/27/anonymous-hacktivists-prepare-for-strike-against-isis-supporters/.

[20] See fn. 9, *supra*.

[21] http://www.fireeye.com/resources/pdfs/fireeye-operation-saffron-rose.pdf.

[22] Nicole Perlroth and Quentin Hardy, *Bank Hacking Was the Work* of *Iranians, Officials Say*, The New York Times, January 8, 2013.

[23] Isabel Kershner, *2 Israeli Web Sites Crippled as Cyberwar Escalates*, The New York Times, January 16, 2012.

People's Liberation Army Unit 61398. This is the official branch of the Chinese Army linked to extensive industrial cyberespionage directed at US companies.[24]

UglyGorilla. This is a hacker based in China who is believed to be a member of PLA Unit 61398, conducting freelance cyber surveillance on US utilities in his off-duty hours.[25]

Freelancers/moonlighters. It is believed that hackers within the Russian and Chinese military also engage in traditional data breach cybercrimes, and will provide their services to others for a price.

Miscellaneous Hacktivist Groups. These include groups like Anonymous, LulzSec, Cult of the Dead Cow, and countless others. Their means and motivations vary. Certainly at least some members of some groups support the overthrow of the established order, including governments, and view their activities as insurrection.

General Observations

For the immediate future, only a few states have or could likely obtain the capacity to launch an attack that would have the necessary physical effects to be considered an armed attack under current USG doctrine. Israel, the United Kingdom and France are allies, and China has too much of a stake in the US economy to intentionally wreak havoc on it. Over the long course of the Cold War, the Soviet Union was a consummately rational actor, and Russia shares the same essential ethos. The only other states with the capacity, or likely to obtain the capacity in the near term, are Iran and Syria. They seem likely to act covertly and indirectly, through sponsorship of terrorist groups or hacker collectives.

Terrorist organizations acting on their own do not seem to have the current capacity to launch a cyber exploit with direct physical effects, but certainly the desire to do so exists. And in fact, there is a general understanding within the national security community that within a few years, terrorists may be able to conduct a high-impact attack with either physical or financial consequences.[26]

Lesser attacks, such as the theft of personal information or supply chain disruption, are already possible. Many cyber tools, and considerable cyber talent, are available for purchase in the so-called "Dark Market". As just a single example, one group of 6 to 10 hackers, known as Icefog, has been reported to specialize in selling tailor made attacks on supply chains.[27]

---

[24] This was revealed by the cybersecurity firm Mandiant, in its report: http://intelreport.mandiant.com.
[25] Michael Riley and Jordan Robertson, *UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat,* http://www.Bloomberg.com/news/print/2014-06-13/uglygorilla-hack-of-u-s-utility-exposes-cyberwar-threat.html
[26] *See, e.g.,* Combating Terrorism Center at West Point, Christopher Heffelfinger, *The Risks Posed by Jihadist Hackers,* July 23, 2013, http://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers.
[27] Thomas M. Chen, *Cyberterrorism After Stuxnet,* U.S. Army War College Strategic Studies Institute, June 2014.

How Will the Language Apply?

As this discussion makes clear, it will be difficult to determine definitively whether a given cyber exploit fits into various terms in war and terrorism provisions, such as "military or usurped power," "acts of foreign enemies," "insurrection," "political disturbance," and "ideological or similar purpose," just to name a few.

Similarly, if a nation-state engages in active defense (*i.e.,* a preemptive attack) in anticipation of an attack, will that constitute "an act taken to hinder or defend" against an attack? What will be the effect on the losses of innocent victims suffering collateral damage?

As a not-entirely-hypothetical thought exercise, it is interesting to consider the following scenarios.

Personal information of two million customers of a large retailer is revealed online. A hacktivist collective claims credit and says that it has customer information from five more retailers. Unless the USG allows Edward Snowden back into the US with a promise not to prosecute, it will reveal the rest. The USG does not comply, and the data is made available.

Same scenario, except the act is to disable medical devices in hospitals throughout the country, resulting in deaths.

The USG learns that the Syrian Electronic Army is planning to try to shut down the New York Stock Exchange. It preempts the attack by inserting a malicious code into the hostile computers. The malicious code inadvertently spreads to private commercial computers of Western banks in Dubai, rendering them permanently inoperable.

Cyber Fighters of Izz ad-Din al-Qassam effectuates a series of fraudulent wire transfers from US banks to protest US assistance in developing and maintaining Israel's Iron Dome technology.

Nightmare engages in data breaches, sells the information and gives the proceeds to ISIS. In response, a hacktivist group steals and releases data from the US branches of banks in Turkey and Quatar, countries they assert are funding Nightmare.

A cyberattack on a communication network or emergency system greatly exacerbates the death and destruction from a traditional physical terrorist attack.[28]

[28] This possibility is suggested by Chen, *supra*, at 25.

Conclusion

The application of war and terrorism exclusions is not an exercise involving certainty derived from immutable facts. Rather the determination is a *decision,* based on an evaluation of often incomplete facts, made by people – claims executives, their legal advisors, and ultimately judges.

In a process like this, it is not useful to state abstract conclusions. Instead, it is useful to remember that four US courts faced the question of whether the attack on Pearl Harbor fell within war exclusions. Those courts split two-to-two.[29]

September 2014

Vince Vitkowsky is a partner in Seiger Gfeller Laurie LLP, resident in New York. He represents insurance and reinsurance companies in complex claims matters, and advises on cybersecurity and cyber insurance issues. He has served as an Adjunct Fellow at the Center for Law and Counterterrorism, and is a member of the Executive Committee of the American Branch of the International Law Association. He can be reached at vvitkowsky@sgllawgroup.com.

[29] *Compare New York Life Insurance v. Bennion*, 158 F.2d 260 (10th Cir, 1946) and *Stankus v. New York Life Insurance Co.*, 44 N.E.2d 687 (Mass. 1942) (finding that the exclusion applied) with *Gladys Ching Pang v. Sun Life Assurance Co. of Canada*, 37 Haw 288 (1945) and *Rosenau v. Idaho Mutual Benefit Association*, 145 P.2d 277 (Idaho 1944) (finding the exclusion did not apply).