CyberPro

May 2010

Keeping Cyberspace Professionals Informed

When does electronic espionage or a cyber attack become an 'act of war'?

BY MAJ. DAVID L. WILLSON, U.S. ARMY

In a recent article entitled, "U.S. Would Lose Cyber War," retired Vice Admiral and former Director of National Intelligence Mike McConnell told the Senate Commerce Committee, "the United States [is] the 'most vulnerable' target for a massive, crippling cyber attack, primarily because the country is also 'the most connected' to the Web."[1] Lieutenant General Alexander, director of the National Security Agency (NSA) and nominee for commander, U.S. Cyber Command, echoed these concerns to the Senate in his confirmation hearings, stating that U.S. networks are a "strategic vulnerability."[2] These statements are eye-opening in light of numerous recent headlines. In the last couple of years, we have read that the first cyber war may have already occurred, i.e., "Russia accused of unleashing cyberwar to disable Estonia"[3]; "Georgia – Russo Conflict: First Cyberwar"[4]; and, "Has North Korea Started the First Cyberwar?"[5]

Cyber incidents that made the news and other not so well-known incidents could be characterized, at least for now, as either criminal activity or electronic espionage, but do they rise to the level of an "act of war"?

Before proceeding, it is important to clarify that the term "act of war" in this article refers to and will be used in place of the more accurate terms "act of aggression" or "armed attack," wherein one nation attacks another, thus authorizing the attacked nation to act in self-defense under Article 51 of the U.N. Charter; to act in anticipatory self-defense; or for the U.N. Security Council to authorize the use of force under Article 42 of the U.N. Charter.[6] For now, it is probably safe to say the line between electronic espionage or cyber crime and an "act of war" has not yet been crossed based on the lack of a defensive action in the form of a kinetic or cyber attack in self-defense by the nations attacked electronically.

Can the line between electronic espionage/cyber crime and cyberwar be clearly identified? Can a cyber incident actually be equivalent to an armed attack, or amount to an "act of war"? Consider this: if a hacker is able to gain access to a network and read or steal data, chances are depending on the network, they can do much worse, e.g. erase data, cause destruction, manipulate the system, place backdoors, etc. At the very least, the line between electronic espionage and cyber attack is very thin – possibly a matter of a keystroke or two.

---

[1] "U.S. Would Lose Cyber War: Warning From Former Intelligence Chief, John Michael McConnell," The Hill.Com, (February 24, 2010).
[2] Baldor, Lolita, "Military Asserts Right to Return Cyber Attacks," Associated Press (Apr. 14, 2010).
[3] Traynor, Ian, The Guardian (May 17, 2007).
[4] Handelman, Marc, InfoSecurity.US (Mar. 20, 2008).
[5] Schroeder, Stan, Mashable, The Social Media Guide (Jul. 8, 2009).
[6] "Act of War". Under Article 51, U.N. Charter a nation is authorized to act in self-defense when faced with an act of aggression by another nation. Equally, the U.N. Security Council can authorize armed attack in response to unlawful and aggressive action by one nation against another under Article 42. "Anticipatory self-defense", although not recognized in the U.N. Charter, is well recognized in international law and is based on the theory that a nation does not need to wait until the missile is in the air to defend itself. The most notable but also most extreme example in history is the 1980's destruction of the Iraqi nuclear weapons factory by Israel before it was brought online and nuclear weapons generated.

Jaikumar Vijayan, writing about Operation Aurora – the name of the recent attack on Google and other technology companies – believes these cyber incidents have come close to the cyberwar line, but not crossed it.

"After Google-China dust-up, cyberwar emerges as a threat – The episode highlighted cyber threats facing the U.S., but it's not a war – yet!"[7] He stated, "If a full-fledged cyberwar were to break out, the nation's economy would be hit hard. Banks might not be able to function, electricity, water and other utilities could be shut off, air travel would almost certainly be disrupted, and communications would be spotty at best – in a word, chaos."[8]

Steve Chabinsky, a senior official with the FBI, stated many adversaries – given enough time – have the capability and funding to penetrate every computer system in the United States, a risk that could "challenge our country's very existence."[9]

U.S. Navy Admiral Robert Willard, commander of U.S. Pacific Command, warned Congress that U.S. military and government networks are being attacked by entities within China and they are "challenging . . . [our] ability to operate freely in the cyber commons."[10]

Certainly, if another nation seriously challenged our ability to launch missiles or interceptors, we would retaliate or at least take some sort of defensive action. Shouldn't the same be true if an adversary challenges our ability to operate in cyberspace, threatens to cripple our infrastructure or claims they have the ability and takes steps to prove it? Wouldn't these actions be grounds to retaliate in self-defense with a cyber or kinetic attack?

There is no question that the cyber attack, followed by the massing of troops on the border and invasion into Georgia by Russia, constituted an act of aggression, but was not considered a cyberwar – although labeled such by the media. What if a nation were stealing terabytes of sensitive data (sound familiar); jamming or cutting off a nation's communications; or placing backdoors in order to deny all communications, cut-off electricity or block or disrupt financial markets, etc.? Would any of these activities rise to the level of an act of aggression or the proverbial "act of war" permitting a response in anticipatory self-defense?"

To analyze this, let's first define "act of war" – or in this case, "act of aggression" – and "espionage." As stated above, the term "act of war" is not one used in international law, but is defined at Dictionary.com as, "an act of aggression by a country against another with which it is nominally at peace."[11] "Act of aggression" is defined as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the

[7] Vijayan, Jaikumar, "After Google-China dust-up, cyberwar emerges as threat," Computer World (April 7, 2010).
[8] *Id*.
[9] Thibodeau, Patrick, "Cyber attacks, an existential threat to U.S., FBI says," Computer World (Mar. 24, 2010).
[10] *See* Google-China dust-up *supra* note7.
[11] "Act of War," Dictionary.Com (March 14, 2010).

United Nations, as set out in this Definition."[12] Espionage is "the act or practice of spying; the use of spies by a government to discover the military and political secrets of other nations; the use of spies by a corporation or the like to acquire the plans, technical knowledge, etc., of a competitor: industrial espionage."[13] There is no official definition for "electronic espionage," but it could easily be defined as the use of electronic techniques, such as computers, phones, wiretaps, etc., to conduct spy activities. International law does not specifically define what acts constitute an act of aggression entitling a nation to retaliate in kind, so nations must use their best judgment.

Bottom line: A nation will have to decide how much pain they are willing to endure and where they believe the international community's tolerance lies – assuming they care – before retaliating against electronic attacks or invasions to their networks. Some very tough issues must be addressed and questions answered before making this decision. Attacked or invaded nations must ask, "Do we know who is attacking us; do we know the extent of their capabilities; what are the long-term ramifications of a cyberwar; do we have more to lose than the nation attacking us; what are their true intentions?"

Obviously, an outright cyber attack followed by some sort of kinetic strike would make the decision very black and white. But a pure cyber attack with no kinetic follow-up creates a very murky situation. James Lewis, director and senior fellow at the Center for Strategic and International Studies, hit the nail right on the head when he stated that the attacking nation would have to decide whether taking down the United States' or another nation's networks is more valuable than the intelligence they may be gathering.[14] Unless a nation is ready to go to war with the nation whose networks they disrupt, then this is not likely. The reverse is also true: Unless the victim nation is ready to go to war with the nation they retaliate against, they had better think through all possible scenarios and responses to their retaliation. Additionally, what if the potential retaliation will lead to an escalated cyberwar affecting more than just the two warring nations?

The most significant issue to address is the nation's level of assurance as to the identity of the attackers or invaders. It is obviously relatively easy to remain anonymous in cyberspace, and this fact is what

[12] United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression, Article 1 (Dec. 14, 1974). *See also*, Article 3, Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression:
(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof,
(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
(c) The blockade of the ports or coasts of a State by the armed forces of another State;
(d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein. Article 4, The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter.
[13] Merriam-Webster Online, "Espionage."
[14] *Id.*

plagues nations and law enforcement worldwide.[15] The attacker could be an adversary nation, but could also be terrorists, criminals or even "script kiddies." In fact, a victim nation may never know who was sitting at the keyboard when a cyber attack was launched.

Can you attack what you can't identify? Not according to international law. A victim nation does not have the right to strike out, blindly impacting neutral nations in hopes of striking their attacker.[16] Let's face it – regardless of the label, espionage or criminal, perpetrators no longer have to put their physical well-being at risk, but merely sit behind a computer with a cup of coffee, tap away and enjoy almost complete anonymity. Even if significant evidence appears to exist, the attacking nation-state could merely claim it was the victim of rogue dissidents or "hactivists" within their territory attempting to discredit the legitimate government.[17]

Consider Operation Aurora. "Google . . . claimed the cyber-attack originated in China. Since Google's announcement, researchers have sought to confirm the source of the attacks, but have largely come up wanting, [and] . . . [t]he Chinese government has repeatedly denied any involvement."[18] Also consider the cyber attacks on Estonia in 2007. The Estonian government stopped short of accusing the Russian government, but the implication was there. The evidence seemed to indicate the attacks came out of Russia, but the Russian government denied any involvement, despite the fact one of the IP addresses was linked to a Russian government official.[19]

Let's step away from this issue for a moment and address one that may be weighing heavily on some readers' minds. Why couldn't a nation who was either the victim of a cyber attack or continues to be a victim merely retaliate against the computer or server from which they believe the attack originates? In other words, strike back blindly, or block the attack at the last visible hop?

Despite the claims that cyberspace has no borders, this action would violate the law of neutrality under international law.[20] The invasion of another nation's territory can be considered an act of war since their territory is inviolable. So a blind retaliation is an attack on an innocent neutral nation that would thus give that nation the right to attack back in self-defense. An argument could be made that the neutral nation violated its neutral status by allowing its servers to be used to launch an attack. But, Hague V specifically states that a neutral is not required to forbid this use of its "telephone, telegraph cables, or wireless telegraphy apparatus . . .," which can be equated to modern day cyberspace.[21] Additionally, how can a neutral nation be held responsible for the acts of another if it is not aware of those acts? Finally, to hold the neutral nation responsible would fly in the face of the laws and policies the world presently lives by on the Internet. Internet service providers (ISPs) are not presently held liable for infringing copyright material or other illegal material on their servers unless they are aware of it, and for

[15] Carr, Jeffrey, "Projecting Borders Into Cyberspace," SecurityFocus.com (Apr. 2009).
[16] *See* United Nations *supra* note 12.
[17] *See*, "Projecting Borders Into Cyberspace," *supra* note 15.
[18] "Google Attacks Linked to Two Chinese Schools," Brian Prince, E.Week.com (Feb. 19, 2010). *See also*, "China Denies Link to Cyber-Attacks," Brian Prince, EWeek.com (Jan. 25, 2010).
[19] "Cyber Assaults on Estonia Typify a New Battle Tactic," Peter Finn, Washington Post (May 19, 2007).
[20] Hague V (1907), Article 1, "The territory of neutral powers is inviolable."
[21] *Id.* at Article 8.

the most part, they owe no duty to search for this material.[22] In light of some recent court rulings around the world, the winds of change may be coming.[23] But for now, the neutral nation – until made aware of the activity on the servers within its territory by the victim nation – cannot and should not be the victim of a retaliatory strike.

Will we really get to a point where a purely cyber attack is significant, intrusive or threatening enough that the victim nation would be willing to begin a cyberwar and/or retaliate? Based on past statements, some nations may have already set the stage. In the early 1990s, Russia declared they retain the right to retaliate with nuclear weapons if a nation attacks them using strategic information warfare weapons in light of the "possible catastrophic consequences" from a cyber attack.[24] There was never a clarification, but were they referring to an actual cyber attack that results in catastrophic consequences or an attack that merely has the potential but does not result in catastrophe?

So, where does this leave us? Will we ever get to the point where nations engage in a true cyberwar? We should certainly hope not. The ramifications could be catastrophic, equivalent to nuclear attacks, but instead creating mutually assured economic destruction. Any cyberwar would not be limited to the networks and financial markets of the warring nations, but would affect markets globally.

Whether we label it electronic espionage, cyber crime or cyber attack, the pain or frustration levels apparently have not risen to the point where a nation is ready to go to war. For now, it is probably safe to say if a nation's ability to defend itself is threatened by a cyber attack, it will not sit idly by, but seek some form of retaliation or defensive action – most likely kinetic – assuming the identity of the attacking nation can be verified. For my theory on how a nation can defend itself and/or block a cyber attack without knowing the identity of its attacker or violating the neutrality of an innocent nation, please see my article entitled, "A Global Problem: Cyberspace Threats Demand an International Approach."[25]

About the Author

Maj. David Willson has spent the last 20 years serving his country as an active duty attorney in the U.S. Army. He spent the first 10 years of his military career representing clients as a criminal defense attorney, in administrative hearings, and as a military prosecutor and a Special Assistant U.S. Attorney. During the last 10 years, Willson focused on technology and the law. He has provided legal advice and counsel to very high levels in the Department of Defense in the areas of space operations and the law, cyber or computer network operations and the law, and international law as it applies to military operations. He was a legal advisor at Army Space Command and the National Security Agency. Following his retirement later this year, Willson is looking to practice information security and compliance law and get involved in or start a business doing security consulting.

[22] *See* U.S. Copyright Act.
[23] *See*, Remondini, Chiari, "Google Executives Convicted of Privacy Violation in Italy Trial," Business Week (Feb. 24, 2010).
[24] Thomas, Timothy L., "Russian Views on Information-based Warfare," Airpower Journal (July 1996).
[25] Willson, David, "A Global Problem: Cyberspace Threats Demand an International Approach," Armed Forces Journal (July 2009), *see also*, The ISSA Journal (August 2009).