**Public Interest Law Reporter**

Volume 20
Issue 1 *Fall 2014*

Article 5

2014

# The Cold War of Cyber Espionage

Elizabeth Hanford

Loyola Public Interest Law Reporter

# The Cold War of Cyber Espionage

Elizabeth Hanford

During the Cold War, governments raced against each other to create the strongest and most effective nuclear weapons in the world.[1] Today, governments race against each other to obtain sensitive information through cyber espionage.[2] However, in cyber espionage "there is no MAD in the Cold War sense. . . You can't be 'assured' of attribution."[3]

Criminals are difficult to find in cyberspace, because "there is no equivalent of a DNA sample or fingerprint to identify the perpetrator of a specific cyber crime."[4] Perpetrators use proxy servers, virtual private networks, or peer-to-peer software to hide their identities within the vast world of cyberspace.[5] Although attribution proves difficult, researchers can analyze data such as the "time zone, location of the physical servers used in the attack, nation-specific tools and techniques, and language indicators."[6]

One example of this problem is Turla malware. The cyber espionage operation closely monitors diplomatic embassies in the former Eastern Bloc.[7] Researchers suggest state sponsorship, as there is "a steep cost to conduct such surveillance, yet no apparent economic motive."[8] However, the exact source of the operation remains unclear.[9] Another example includes Dragonfly, a cyber espionage operation capable of shutting down entire power grids in multiple

---

1 Robert Crowley and Geoffrey Parker, *The Reader's Companion to Military History,* HISTORY, 2009. *Available at* http://www.history.com/topics/cold-war/arms-race.

2 Rick Wilking, *Expert: US in cyberwar arms race with China, Russia*, NBC NEWS, Feb. 20, 2013. *Available at* http://investigations.nbcnews.com/_news/2013/02/20/17022378-expert-us-in-cyberwar-arms-race-with-china-russia.

3 *Id*.

4 DJ Summers, *Fighting in the cyber trenches*, FORTUNE, Oct. 13, 2014. *Available at* http://fortune.com/2014/10/13/cold-war-on-business-cyber-warfare/.

5 *Proxy and VPN Detection*, THREATMETRIX, http://www.threatmetrix.com/technology/proxy-and-vpn-detection/; Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, CONG. RESEARCH SERV. R43848, 7 (2015). *Available at* http://www.fas.org/sgp/crs/natsec/R43848.pdf

6 *Supra* note 4.

7 *Turla: Spying tool targets governments and diplomats*, SYMANTEC, Aug. 7, 2014. *Available at* http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats.

8 *Supra* note 4.

9 *Supra* note 7.

countries.[10] The large scale of the operation and "high degree of technical capability" suggests the operation is also state sponsored.[11]

Fortunately, Turla malware and Dragonfly abstain from harming civilians or causing physical damage at this point in time. However, every security breach is a serious threat that impairs national security and defense operations. When states become victim to cyber espionage, scholars turn to existing laws of armed conflict to determine permissible remedies.[12]

## SELF DEFENSE

According to the laws of armed conflict, the victim state may resort to self-defense in the wake of an armed attack.[13] The principles of necessity and proportionality govern whether an attack rises to the level of an armed attack.[14] In the context of cyber operations, scholars analyze a cyber attack in two steps.[15] If the activity satisfies both steps, the activity is referred to as "cyber warfare."[16]

First, the cyber activity must constitute a "cyber attack."[17] One definition of a cyber attack is an attack that can "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer [network] itself."[18] Other scholars define a cyber attack as "any action taken to undermine the functions of a computer network for a political or national security purpose."[19] In order to constitute a cyber attack, the cyber operation must do more than steal information or "passively observe a computer network."[20]

---

10 *Dragonfly: Western Energy Companies Under Sabotage Threat*, SYMANTEC, June 30, 2014. *Available at* http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

11 *Id*.

12 Oona A. Hathaway and Rebecca Crootof, *The Law of Cyber-Attack*, 100 CLR 820-21 (2012).

13 U.N. Charter art. 51. *Available at* http://www.un.org/en/documents/charter/chapter7.shtml.

14 *Supra* note 12 at 849.

15 *Id*. at 836-37.

16 *Id*. at 837.

17 *Id*. at 836.

18 James E. Cartwright, *Memorandum for Chiefs of the Military Services*, U.S. DEP'T OF DEF. Available at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

19 *Supra* note 12 at 826.

20 *Id*. at 830.

Second, the cyber attack's "effects must be equivalent to an 'armed attack,' or [the] activity must occur in the context of armed conflict".[21] Professor John C. Dehn explains, "the operation's attacks must be directed toward a military objective, which creates a direct military advantage."[22] In *Nicaragua v. U.S.*, the International Court of Justice analyzed the United States' operation's "scale and effects" in Nicaragua to determine whether the acts of an operation rose to the level of an armed attack.[23] The larger the "scale and effects" of the operation, the more likely a court will find the threshold has been met.[24]

Scholars argue that cyber espionage fails to constitute a cyber attack, because the operation fails to disrupt or destroy a computer network.[25] Additionally, states fail to claim that cyber espionage constitutes a prohibited use of force.[26] Therefore, states should not launch a military offensive attack to deter or retaliate against cyber espionage. One way for states to deter cyber espionage may be to prosecute offenders under domestic law.

## DOMESTIC PROSECUTION

On May 19, 2014, the United States brought the first ever charges against a state actor for cyber espionage.[27] The indictment alleged five Officers of the Chinese People's Liberation Army gained access to six United States utility companies and stole trade secrets from 2006-2014.[28] According to U.S. officials, the purpose of the indictment is to expose China's spying and reduce the targeting of American companies.[29]

---

21 *Id.* at 833.

22 Interview with John C. Dehn, Assistant Professor, Loyola University Chicago School of Law (Oct. 24, 2014).

23 *Nicar. v. U.S.*, 1986 I.C.J. 14, 195 (June 27).

24 *Id*.

25 *Supra* note 12.

26 David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, Am. Soc'y of Int'l L., Mar. 20, 2013. *Available at* http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving#_edn10

27 *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, Dep't of Def., May 19, 2014. *Available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

28 *Id*.

29 Shane Harris, *Exclusive: Inside the FBI's Fight Against Chinese Cyber-Espionage*, Foreign Pol'y, May 27, 2014. *Available at* http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/.

China points to Edward Snowden's WikiLeaks, which revealed United States involvement in the hacking of Chinese companies, and accuses the United States of hypocrisy.[30] In response, the head of the United States' Justice Department's National Security Division John Carlin argues, "[United States] spying on foreign companies is qualitatively different than what the Chinese are doing, because the United States doesn't share the fruits of its espionage directly with companies, the way China does."[31]

Even with the indictment of the Chinese Officers, it is unlikely governments will stop stealing sensitive information. Government espionage is already exposed. This exposure fails to reduce the amount of espionage.[32] Additionally, the United States admits incarceration of the Chinese Officers is unlikely.[33] The offenders' diplomatic status raises the protection of diplomatic immunity.[34] Furthermore, attribution is difficult to obtain in the cyber world.[35] Cyberspace creates a criminal playground where the risks are low and the gains are high.[36] To win the cold war of cyber espionage, states should "protect data at its core" and focus on creating the most effective cyber defense arsenals in the world.[37]

---

30 Jonathan Kaiman, *China reacts furiously to US cyber-espionage charges*, THE GUARDIAN, May 20, 2014. *Available at* http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

31 *Supra* note 29.

32 CSIS AND MCAFEE, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 2 (2014).

33 *Supra* note 29.

34 *Supra* note 26.

35 *Supra* note 4.

36 *Supra* note 32.

37 *Did Obama's Cybersecurity Proposals Go Far Enough?*, WALL ST. J., (Jan. 21, 2015). *Available at* http://www.wsj.com/video/did-obama-cybersecurity-proposals-go-far-enough/7B14948F-6713-4159-BBA5-4CA41067B66E.html.