CYBERWARFARE IN THE STUXNET AGE

CAN CANNONBALL LAW KEEP PACE WITH THE DIGITAL BATTLEFIELD?

BY DAVID Z. BODENHEIMER

A nuclear processing facility shuts down. Government websites crash. A city goes dark. Is it an accident—or cyber blitzkrieg? After the cyberattacks on Estonia and Georgia in 2007 and 2008 and the Stuxnet penetration of Iran's Bushehr nuclear power facility in 2010, cyberwar has moved from theory to reality. We know that cyberwarfare has gone mainstream when dozens of countries are mobilizing forces for battle in cyberspace, the Secretary of Defense himself warns of a "digital Pearl Harbor," and the popular press churns out stories on the emerging battlefront.

With the fog of cyberwar comes a torrent of legal issues regarding authentication, intelligence gathering, counterstrike authority, and liability under domestic and international laws. Rather than tackling the broader policy issues applicable to nation-states,[1] this article focuses upon what cyberwar may mean for the private sector, including government contractors, caught in the cross fire of cyberbattles and the ensuing legal fallout.

Cyberwar Comes of Age

Quite simply, cyberwar is reality. Although some have downplayed cyberwar as mere science fiction, the technology has already been proven, and the risks scare those who know.

Why Cyberwar Has Become a Top Security Concern

President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."[2] The Secretary of Defense put it more starkly:

> We could face a cyber attack that could be the equivalent of Pearl Harbor. [Such an attack could] take down our power grid, take down our financial systems in this country, take down our government systems, take down our banking systems. They could virtually paralyze this country.[3]

The former Director of National Intelligence, Vice Admiral Michael McConnell (Ret.), summed up the risk bluntly: "If we were in a cyberwar today, the United States would lose."[4]

Congressional members—Democrats, Republicans, and Independents—share these concerns about "catastrophic" risks from cyberattacks:

> *Senator Lieberman:* "Catastrophic cyber attack is no longer fantasy or fiction. It is a clear and present danger."[5]
> *Senator Collins:* "It's important to realize that the threat of a catastrophic cyber attack is not theoretical. It's very real. It is not a matter of 'if' such an attack is going to occur, but when."[6]
> *Senator Carper:* "[U]nfortunately our enemies have identified cyberspace as an ideal 21st century battlefield."[7]

A few examples highlight the nature and magnitude of the threat. According to intelligence sources, foreign spies have already penetrated the electrical grid in the United States.[8] The Energy Department's Idaho National Laboratory and others used simulated attacks to show how skilled hackers could cause serious damage to the power grid, even with rudimentary tools.[9] And even industry executives acknowledge that the threat is growing.[10] Given the long lead time for rebuilding or replacing complex electrical systems in the power grid, the economic impact alone could mount to more than $700 billion for an extended shutdown.[11]

The banking industry represents another high-stakes target for our cyberenemies. On a daily basis, US banks move the wealth of the world. Compared with America's Gross Domestic Product (GDP) of $14 trillion, "two banks in New York move *over $7T per day* in transactions."[12] A crippling cyberattack on New York banks would devastate both the US and world economies:

According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a United States bank, the economic consequences would have been "an order of magnitude greater" than those caused by the physical attack on the World Trade Center.[13]

How Cyberwar Has Moved From Risk to Reality

The rise of cyberweapons has long been predicted. More than a decade ago, senior Chinese military officers identified "computer viruses" as an unconventional means for attacking financial systems and networks.[14] Cyberattacks on critical infrastructure are no longer theoretical. History has already shown the damage that cyberwarriors can inflict upon their adversaries.

Pipeline Attack: "A previous historic example includes a reported case of stolen code that impacted a pipeline. In this case, code was secretly 'Trojanized' to function properly and only some time after installation it instructed the host system to increase the pipeline's pressure beyond its capacity. This resulted in a three kiloton explosion, about one-fifth the size of the Hiroshima bomb."[15]

Power Grid Shutdown: "[I]n other countries cyber attacks have plunged entire cities into darkness."[16]

Crippled Internet: "And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, cyberattacks crippled Georgian government websites."[17]

The Stuxnet attack on the Iranian nuclear power facilities provides the strongest proof yet that cyberweapons have become a mainstream part of the global arsenal.

Stuxnet was programmed specifically to infiltrate certain Industrial Control Systems (ICS), allowing the worm potentially to overwrite commands and to sabotage the infected systems. It was discovered in July at the Bushehr power plant, Iran's controversial nuclear power facility. It was also found in systems in China, Indonesia, India, the United States, and elsewhere. More than 100,000 computers have been infected.[18]

Stuxnet represents the most technologically advanced cyberweapon yet discovered. It has been described as "the world's first publicly verified military-grade cyber weapon capable of destroying machinery"[19] and "a landmark activity that opens the battlefield for global cyber warfare."[20] The Stuxnet worm reflected a level of sophistication and complexity beyond the technical capabilities of all but a few nations:

- *10,000 Programming Hours:* "Experts estimate that 10,000 man-hours of programming time went into writing Stuxnet. . . ."[21]
- *"Zero-Day" Vulnerabilities:* "Stuxnet invades its target computers using four different Microsoft Windows security vulnerabilities that had been unknown until Stuxnet was set loose. These security flaws, known as 'zero-day vulnerabilities,' are difficult to discover and are valuable commodities on the black market. Using four of them in one piece of malware is unprecedented."[22]
- *Stolen Digital Certificates:* Digital certificates stolen from Realtek Semiconductor and JMicron Technology cloaked Stuxnet as not being malicious: "This theft alone is an operation that requires either a physical burglary at the headquarters of both companies, or the kind of hacker attack that very few programmers worldwide are capable of performing, because these certificates are additionally secured and encoded."[23]
- *Multiyear Project:* "An analysis by a European intelligence agency . . . states that it would have taken a programmer at least three years to develop Stuxnet, at a cost in the double-digit millions."[24]

Now that cyberweapons have been field-tested, virtually no one expects Stuxnet to be the last attack. As Dr. Lewis testified, "[c]yber attack will be like the airplane—within a few years, no self respecting military will be without this capability."[25] Major US adversaries are developing the capacity for cyberattacks on critical infrastructure:

> One is the threat of cyber attack. Many nation states, like Russia, China, North Korea, and Iran, have offensive cyber attack capabilities, while terrorist groups like Hezbolla and al Qaeda continue to work to develop capabilities to attack and destroy critical infrastructure like the electric grid through cyber attacks.[26]

Indeed, some US officials have predicted that major cyberattacks are "nearly a certainty," given "the promised retaliation against the U.S. for the Stuxnet work that destroyed Iranian nuclear centrifuges."[27] The distributed denial of service (DDOS) attacks on Estonia and Georgia during disputes with Russia and the coordinated hacking attacks on Google to access accounts of Chinese dissidents provide real-world examples that the age of cyberwar has already arrived. Given this new reality, the private sector needs to gear up for the risks that come with a cyberwar world.

Cybertechnology Outpaces Legal Answers for the Private Sector

With more than 85 percent of US critical infrastructure in private hands, cyberwar will inevitably strike the private sector. Aside from the economic waste and business disruption of an attack, war in cyberspace will engage the private sector in other ways. The military will depend

David Z. Bodenheimer is a partner in the law firm of Crowell & Moring LLP (www.crowell.com) in the Washington, DC, office, where he heads the Homeland Security Practice and specializes in government contracts, litigation, and cybersecurity. He currently co-chairs the ABA Section of Science & Technology Law Homeland Security Committee, as well as the PCL Cybersecurity, Privacy, and Data Protection Committee.

upon government contractors to forge cyberswords and shields, raising legal questions about liability exposure for weapons gone awry or defenses that fail. Even private bystanders may be pulled into the fray if their systems are shut down due to botnet infections or security gaps, thus raising legal questions about who bears the risk for such losses.

When Contractors Support Offensive Cyberoperations

The private industrial base has traditionally hammered out the tools of war. With the exponential surge in the complexity of military technology, the private sector will inevitably have a critical role in building offensive cyberweapons and authenticating the identity of attackers. With this role will come litigation and liability that hinge upon law that never contemplated the complexity and murkiness of cyberwar.

Cyberweapons and Liability Risks

For many years, the government contractor defense often shielded military contractors from third-party liability when a defect in an aircraft, vehicle, or other product caused an injury. However, this Supreme Court doctrine generally required the contractor to conform to "reasonably precise specifications" created or approved by the military department.[28] With the shift away from detailed government-approved specifications to more general performance-based requirements, the government contractor defense has eroded, leaving more contractors exposed to third-party liability for accidents resulting from products sold to the US government.

Cyberweapons will more likely fall into the latter category, thus leaving open questions about the contractor's liability when such items accidently take down friendly infrastructure or injure third parties. Without the protection of the government contractor defense, cybercontractors could face potentially catastrophic losses much like those that hit certain manufacturers of products like Agent Orange.[29] Given the uncertainty of the law in this area, cybercontractors will face the tough choices outlined by the Supreme Court: raise prices to the US government or get out of the business.[30]

Authentication Versus Surveillance

In a kinetic war, the foe is usually obvious, as satellites and electronic signatures unmask the country that launched the missile or fired the shot. With cyberwar, the opposite is true. Cyberweapons may bounce from botnet to botnet across multiple international borders, leaving questions about whether terrorists, organized crime, or unfriendly countries launched the assault.

The US intelligence agencies will seek to pin down the attacker, but may need the help of the private sector for such information gathering. For example, the National Security Agency (NSA) has turned to the telecommunications industry for information to identify potential terrorist activities. This private sector cooperation then triggered massive lawsuits, such as the $50 billion class action against Verizon.[31] Congress ultimately stepped in with legislation to indemnify the telecom companies against such lawsuits.

The NSA/telecom litigation serves as a cautionary tale for private industry (whether in the Internet, telecom, or forensics business) that assists the US government in tracking down culprits in cyberattacks that may cross several international borders. Whether such forensics or assistance would violate US electronic surveillance laws and European computer crime sanctions (or more) remains an open legal question to be examined in a future trial—perhaps in a foreign courtroom.

When Contractors Assist With Cyberdefense

The US government has already made substantial investments in hardening defenses against cyberattacks, including the award of significant contracts for such security.[32] Congress anticipates expanding such efforts by "cultivating commercial industry to produce advanced cybersecurity technologies and capabilities."[33] However, if security technology or safeguards fail, the sellers may face crippling losses or lawsuits that may discourage the most innovative cyber technologies from coming to the market. For example, a security breach allowed hackers to counterfeit the digital website certificates issued by DigiNotar, driving the Dutch company into bankruptcy.[34]

For antiterrorism technology, Congress passed the SAFETY Act to spur development and innovation by shielding sellers from huge lawsuits flowing from terrorist attacks.[35] However, this liability protection only extends to acts of terrorism (as determined by the Secretary for Homeland Security), not acts of war. If the Department of Defense declines to extend indemnification for "ultrahazardous risks" to cybersecurity contractors under Public Law No. 85-804, such contractors will be left to fend for themselves when security measures fail and private lawsuits ignite. Given these legal uncertainties, the military and intelligence agencies may not be able to obtain breakthrough cyberdefenses if sellers remain on the sidelines due to fears about crippling lawsuits and bet-the-company losses.

When Private Bystanders Get Caught in the Cybercrossfire

In a cyberwar, some private bystanders may become collateral damage. For example, cyberattacks may be fought by proxy, enlisting armies of botnets from unwitting individuals and companies to wreak havoc on the target. In such cases, the military may seek to disable or shut down these botnet-infected networks, resulting in businesses being brought to a standstill.[36] Such actions would trigger a host of questions about whether the US government could be sued under various tort theories or even under the Constitution for a Fifth Amendment taking.[37] Similarly, such companies would be pitted against their insurers (if any) over whether coverage extended to "acts of war" and "sovereign acts."

Even more difficult questions would arise over false positives—that is, when the US government acts to disable private networks due to a perceived threat that turned out to be nothing. Many companies could not stand even a week without an information network, yet the courts do not appear to have faced due process issues or injunctive relief actions based on an improper governmental act of pulling the plug on a private network for a nonexistent security threat. Whether the courts will find due process protections against such governmental acts remains an open question for now.

Who Bears the Risks?

About cyberwar, we know certain things: the risks are gargantuan, top officials are scared, and the opening salvo has already been fired, as exemplified by the Stuxnet attack. We also know that the private sector (including government contractors) will be caught in the cybercrossfire. What we do not know is the legal outcome because, once again, technology has outpaced the law. Just as new cybertechnology has opened new battlefronts, the legal fallout will create new legal frontiers as Congress and the courts will be forced to sort out who must bear what risks when the digital Pearl Harbor attack happens. ◆

Endnotes

1. Several sources have explored the broader issues of applying international treaties (*e.g.*, the Geneva Convention) and domestic law to nations engaged in cyberwar. *See, e.g.*, National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*; Cyberlaw Edition, 64 A.F.L. Rev. 1–257 (2009).

2. Whitehouse Fact Sheet, *Cybersecurity Legislative Proposal* (May 12, 2011).

3. Margery Beck, *Panetta Compares Cyber Threat to Pearl Harbor*, Army Times.com (Aug. 6, 2011).

4. *Cybersecurity: Next Steps to Protect Our Critical Infrastructure: Hearings Before Senate Comm. on Commerce, Science, & Transportation* (Feb. 23, 2010) (statement by Adm. McConnell) (http://commerce.senate.gov/public/?a=Files.Serve&File_id=52507485-dfbe-4873-8089-82dd24f7beaa) (hereinafter 2010 Senate Commerce Critical Infrastructure Hearings).

5. Sen. Comm. on Homeland Security and Governmental Affairs, *Committee Adopts Comprehensive Cybersecurity Legislation*, June 24, 2010 (remarks by Sen. Lieberman) (http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=6be6b903-5056-8059-76ef-7e691cc176fd).

6. *Id.* (remarks by Sen. Collins).

7. *Id.* (remarks by Sen. Carper).

8. Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies,* Wall St. J. (Apr. 8, 2009) ("Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials").

9. Justin Blum, *Hackers Target U.S. Power Grid*, Wash. Post at E1 (Mar. 11, 2005); David Z. Bodenheimer, "Pulling the Plug on the Power Grid: Cyberthreats and Homeland Security Challenges," *The SciTech Lawyer*, at 4 (Spring 2006).

10. McAfee and Center for Strategic and International Studies (CSIS), *In the Dark: Crucial Industries Confront Cyberattacks,* at 1 (2011).

11. Letter from Representatives Thompson and King to Representative Dingell, May 29, 2009, (http://chsdemocrats.house.gov/SiteDocuments/20080530130810-85574.pdf).

12. 2010 Senate Commerce Critical Infrastructure Hearings (statement by Vice Adm. McConnell) (emphasis in original).

13. The Cybersecurity Act of 2010, S.773, 111th Cong., § 2(8) (2010) (www.gpo.gov/fdsys/pkg/BILLS-111s773rs/pdf/BILLS-111s773rs.pdf).

14. Liao Liang and Wang Xiangsui, *Unrestricted Warfare* at 117 (PLA Literature) (1999).

15. *Securing Critical Infrastructure in the Age of Stuxnet: Hearings before Sen. Comm. on Homeland Security and Governmental Affairs,* 111th Cong. (Nov. 17, 2010) (statement by Dean Turner, Symantec) (http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=954c3149-042e-4028-ae23-754868902c44) (hereinafter 2010 Senate Stuxnet Hearings).

16. The White House Office of the Press Secretary, *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, May 29, 2009 (www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure).

17. *Id.* For a detailed discussion of the cyberattacks against Georgia, *see* Cooperative Cyber Defence Centre of Excellence, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Nov. 2008).

18. 2010 Senate Stuxnet Hearings (statement by Sen. Collins).

19. Mark Clayton, *Cyberwar Timeline*, Christian Sci. Monitor, Mar. 7, 2011.

20. *Stuxnet Sparks Debate at Paris Expert Forum*, Financial Times, Mar. 14, 2011 (quoting Nimrod Kozlovski, head of Altal Information Security).

21. 2010 Senate Stuxnet Hearings (statement by Sen. Lieberman).

22. *Id.*

23. Holger Stark, *Stuxnet Virus Opens New Era of Cyber War*, Spiegel Online, Aug. 8, 2011.

24. *Id.*

25. *Cybersecurity: Assessing the Immediate Threat to the United States: Hearings Before House Subcomm. on National Security, Homeland Defense and Foreign Operation of the Comm. on Oversight and Government Reform,* May 25, 2011 (statement of Dr. James Lewis).

26. *Securing the Modern Electric Grid from Physical and Cyber Attacks: Hearings Before House Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology of the Homeland Security Comm.,* 111th Cong., July 21, 2009 (statement by Rep. Clarke) (http://chsdemocrats.house.gov/SiteDocuments/20090721141443-38588.pdf); *see also* Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies,* Wall St. J. (Apr. 8, 2009).

27. *Big Utility Cyberattack Sure Thing Within Five Years, Federal Experts Say*, Washington Internet Daily, June 3, 2011; *see also* Peter Beaumont, *Stuxnet Worm Heralds New Era of Global Cyberwar*, The Guardian, Sept. 30, 2010 (General Keith Alexander "has recently said that it is only a matter of time before America is attacked by something like the Stuxnet worm").

28. *Boyle v. United Technologies Corp.,* 487 U.S. 500, 512 (1988).

29. *See, e.g., Hercules, Inc. v. United States,* 516 U.S. 417, 420–22 (affirming decision placing risk of loss for "Agent Orange" injuries on chemical manufacturers rather than US government).

30. *See Boyle,* 487 U.S. at 507.

31. *Court Will Decide State Secrets Issues First in NSA Phone Surveillance Class Action Suit*, BNA Privacy Law Watch, June 9, 2006.

32. *See, e.g., Contractors Vie for Plum Work, Hacking for U.S.*, N.Y. Times, May 31, 2009 (major contractors "have major cyber contracts with military and intelligence agencies").

33. S. Rep. No. 112-26 at 166 (2011).

34. Eric Chabrow, *The Worst Security Hack Ever*, GovInfo Security, Sept. 22, 2011 (http://blogs.govinfosecurity.com/posts.php?postID=1068&rf=2011-10-01-eg&elq=7e0c009d13434acf9fc2269201e22ee4&elqCampaignId=489).

35. 6 U.S.C. § 441-44.

36. For botnets in the United States, the military departments would face tough questions about their authority to operate domestically under the "posse comitatus" doctrine.

37. *See, e.g., Ruckelshaus v. Monsanto,* 467 U.S. 986 (1984) (allowing eminent domain "takings" claim where agency compromised corporate trade secrets).