LexisNexis® Emerging Issues Analysis

Carey Lening, Kirsten Koepsel, and Ron Weikers on

The Effects and Means of Combating State-Sponsored Cyberthreats

2010 Emerging Issues 5326

Click here for more Emerging Issues Analyses related to this Area of Law.

State-sponsored cyberattacks have beleaguered information security specialists for quite some time, particularly those specialists managing attractive critical infrastructure targets such as government, transportation, energy, and banking networks.[1] Fifty-four percent of 600 IT and security professionals polled in a 2008 study reported that their organizations – all "critical infrastructure enterprises" – had experienced large attacks by "high-level adversaries" such as terrorists, organized crime rings, or nation-states.[2]

Unlike their predecessors, hackers today are no longer content to target large government systems. The hypertechnical criminals of today have become masterful at marketing their tools and services as "hired guns" to a multitude of actors – ranging from nation-states to organized crime rings and drug traffickers. Simultaneously, the method and means of attack have themselves become commodities, with sophisticated tools such as "botnets,"[3] distributed denials of service,[4] and Trojan attacks[5] widely bought and sold on

---

1. "Critical Infrastructures" include structures, computer systems, and networks whose destruction or other compromise would have a debilitating effect on security, the national economy, public health or safety, or any combination thereof. Department of Homeland Security, Critical Infrastructure and Key Resources, http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

2. McAfee In the Crossfire: Critical Infrastructure in the Age of Cyber War 4, available at http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf.

3. A "botnet" or "bot network" is made up of large numbers of remotely controlled machines that have been compromised in some way, usually through malicious code delivered as part of an infected e-mail or website. Once infected, a PC will establish a secret communications link to a remote "botmaster" in preparation to receive new commands. The malicious code may also send back personal data and other information collected on the machine to the botmaster.

   Attackers favor botnets because whole networks of compromised machines (or the tools to make them) can be readily purchased on the black market, require little or no technical expertise, and provide relatively unsophisticated attackers with an easy means to disrupt or block Internet traffic to victim computers through the power of distributed attack. Clay Wilson, Congressional Research Service Report for Congress RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 20 (Jan. 29, 2008), *available at* http://www.fas.org/sgp/crs/terror/RL32114.pdf.

4. A "denial of service attack" (DoS) is an attack that is designed to make a particular computer or resource unavailable to its intended users. A distributed DoS (DDoS) occurs when a group of computers flood a single target for the same purpose. National Cyber Alert System, Cyber Security Tip ST04-015, Understanding Denial-of-Service Attacks, *available at* http://www.us-cert.gov/cas/tips/ST04-015.html.

5. A Trojan horse attack consists of an "apparently useful program [that] contain[s] hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat." US CERT Advisory, CA-1999-02, Trojan Horses (Mar. 8, 1999), *available at* http://www.cert.org/advisories/CA-1999-02.html.

criminal trading platforms and in online chatrooms.[6] The damage inflicted from cyberattacks has become so widespread that the Federal Bureau of Investigation estimated the total cost to businesses and government systems at $559 million annually.[7]

A specific type of computer-based attack may qualify as either an act of state-sponsored "cyberwarfare" or a "cybercrime" depending on the relevant players.[8] This has led some to assert that we should do away with overly complex definitions and frameworks, and should instead assume that all attacks bear some form of state sponsorship.

Methods, Motivations, and Forms of Attack

While numerous definitions of cyberwarfare exist, former Special Advisor to the President on Cybersecurity Richard A. Clarke offers a useful place to start. He defines cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[9] Ascertaining whether any given attack qualifies as an instance of cyberwar versus the more garden-variety form of cyberattack, however, is fraught with difficulty, as the definition heavily depends upon knowledge of the attacker's intent, fellow conspirators, and identity.[10]

Although types of attacks vary, generally three classes of activity make up the bulk of state-sponsored cyberwarfare: (1) attacks that are designed to spread propaganda (e.g., website vandalism and political spam bombing); (2) attacks that sabotage or disrupt software or hardware (e.g., viruses, botnets, DDoS attacks); and (3) attacks that

---

6. For example, in March 2009, "Click," a BBC television show, acquired a botnet from an online chatroom and used it to demonstrate how botnets works. The program used the botnet to hijack almost 22,000 computers, and in turn launched a distributed denial of service attack against a backup computer network owned by security firm Prevx, which consented to the experiment. *Click: Is Your PC Doing a Hacker's Dirty Work,* BBC Networks (Mar. 12, 2009), *available at* http://news.bbc.co.uk/2/hi/programmes/click_online/7938503.stm.

7. Press Release, Federal Bureau of Investigation, IC3 2009 Annual Report on Internet Crime Released (Mar. 12, 2010), *available at* http://www.fbi.gov/pressrel/pressrel10/ic3report_031210.htm.

8. Nart Villeneuve, Blurring the Boundaries Between Cybercrime and Politically Motivated Attacks (Apr. 10, 2010), Internet Censorship Explorer, http://www.nartv.org/2010/04/10/blurring-the-boundaries-between-cybercrime-and-politicaly-motivated-attacks/. For example, Villeneuve chronicles how the Kneber botnet was used both by criminal gangs to steal financial information and by another group to obtain sensitive government information on .mil and .gov accounts.

9. Richard A. Clarke, Cyber War: The Next Threat to National Security and What to do About It (2010).

10. Serge Krasavin, Computer Crime Research Center, What is Cyberterrorism? (Apr. 23, 2004), http://www.crime-research.org/analytics/Krasavin/. Estimates on criminal apprehension rates are equally depressing: One source claimed that only five percent of cybercriminals are ever arrested or convicted. Wilson, *supra* note 3, at 29.

steal or corrupt data (e.g., cyber-espionage, identity theft). U.S. counterintelligence officials speculate that there are about 140 different foreign intelligence organizations that use these techniques or otherwise attempt to infiltrate U.S. government and business information networks on a regular basis.[11] A brief timeline of confirmed notable attacks would include the following:

- 2001: A European Union "Special Committee of Inquiry" accused the United States, United Kingdom, Canada, Australia, and New Zealand of operating a large industrial espionage network against several EU member states and businesses.[12] The network, known as Echelon, was reportedly capable of monitoring wireless, e-mail, and fax data from around the world. Although no direct accusations of cyber-espionage were ever conclusively proven, according to the committee, strong evidence supported claims that the U.S. government tapped the phone lines of European aircraft maker Airbus Industries, which was negotiating a $6 billion contract with the Saudi Arabian government and national airline.[13]

- 2004: Researchers at a major security firm detected a team of government-sponsored attackers in Guangdong Province, China, conducting cyber-espionage on networks owned by the U.S. Defense Information System Agency, the National Aeronautics and Space Administration, and the World Bank. The attacks – code-named "Titan Rain" – probed government websites hundreds of times each day and stole U.S. flight planning and other software.[14]

- April 2007: Estonian government computer networks were inundated by a sustained DDoS botnet-style attack traced to Russian hackers. The attacks, which were initially thought to have been state sponsored,[15] flooded dozens

---

11. Wilson, *supra* note 3, at 12.

12. Eur. Parl. Doc. (A5-0264) 103-06 (2001), *available at* http://www.fas.org/irp/program/process/rapport_echelon_en.pdf ; Martin Asser, *Echelon: Big brother without a cause?,* BBC News (July 6, 2000), *available at* http://news.bbc.co.uk/1/hi/world/europe/820758.stm.

13. Eur. Parl. Doc. (A5-0264) 21; Paul Meller, *European Parliament Adopts 'Echelon' Report*, CNN.com (Sept. 7, 2001), *available at* http://archives.cnn.com/2001/TECH/internet/09/07/echelon.report.idg/. The State Department has denied such allegations.

14. AFP, *Hacker attacks in US linked to Chinese military: researchers*, Breitbart (Dec. 12. 2005), at http://www.breitbart.com/article.php?id=051212224756.jwmkvntb&show_article=1.

of government servers, bogged networks down with bogus information requests, and blocked legitimate traffic, eventually leading the government to shut down a number of sites in order to handle the problem.[16]

- April 2009: Reports began to surface in early 2009 that cyberspies had successfully penetrated the U.S. electrical grid and left behind software programs that could be used to cause future disruption of the system, according to current and former national-security officials. According to the same officials, the attacks occurred over a lengthy period and were pervasively spread across the United States.[17]

Beyond the obvious damage and cost to systems and infrastructure, state-sponsored and other forms of organized cyberattack have the potential to affect a range of daily activities. For example, supervisory control and data acquisition (SCADA) systems, which monitor and regulate the operations of most critical infrastructure systems, such as power generation, water distribution, and traffic control, are often attractive targets.[18] SCADA systems automatically monitor and control physical processes based on data fed back. Most SCADA systems, however are routinely placed in remote, unsupervised locations, and are increasingly connected to local area networks or directly to the Internet.

Possible Solutions to Cyberthreats

John C. Gannon, Chairman of the National Intelligence Council, noted that over the next fifteen years, the U.S. dependence on data and the free flow of information will also

---

15. The Estonian attacks provide an excellent example of why the dividing line between state sponsorship and criminal act can be challenging. Although the attacks were thought initially to be a state-sponsored response to the Estonian government's decision to remove a Soviet-era war statue, later analysis revealed that there was no Russian government connection, and that the attacks were instead the product of a group of loosely associated attackers. Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War*, 9 Geo. J. Int'l Affairs 121-26 (2008), *available at* http://www.bligoo.com/media/users/1/50369/files/Ataque%20Estonia.pdf.

16. Carolyn Duffy Marsan, *Examining the Reality of Cyberwar in Wake of Estonian Attacks*, 24:33 Network World 24 (Aug. 27, 2007); Robert Vamosi, *Cyberattack in Estonia — What It Really Means*, CnetNews.com (May 29, 2007), http://news.com.com/Cyberattack+in+Estonia-what+it+really+means/2008-7349_3-6186751.html.

17. Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, Wall St. J. Apr. 8, 2009, at A1, *available at* http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html.

18. *See* Scott Nance, *Debunking Fears: Exercise Finds 'Digital Pearl Harbor' Risk Small*, Defense Week (Apr. 7, 2003); Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, Security Focus (Aug. 19, 2003), *available at* http://www.securityfocus.com/news/6767.

place the United States at an increased risk of foreign cyberthreats.[19] As such, a major challenge for the United States will be to find more effective means to boost awareness and responsiveness in order to reduce the threat of state-sponsored cyberattacks.

Awareness. Active vigilance is a starting point to keeping cyberattacks at bay. For example, both the government through the National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) and private companies such as Verizon have developed information "cyber crisis centers," designed to track, analyze, share information about, and respond to potential attacks.[20] In 2004, the NCSD also established the National Cyber Alert System (NCAS), a coordinated nationwide system managed by the U.S. Computer Emergency Readiness Team (US-CERT).[21]

While monitoring is necessary, there is only so much that can be done. For example, Verizon's security center in Virginia reports that the company witnesses over one billion security events every day. Little can be done to thwart such attacks, as nearly three-quarters of those attacks come from outside the country, where the U.S. government's law enforcement powers are inadequate to meet the task.[22]

Reduction. Another key is to work on reducing the likelihood that successful attacks can occur. To bolster networks in the United States, the government has been quietly cultivating some of its best security defenders from within major hacking groups. In 2009, for example, General Dynamics Information Technology put out a virtual "help wanted" sign on behalf of DHS, seeking individuals who could "think like the bad guy" and be able to un-

---

19. John C. Gannon, Remarks by John C. Gannon, Chairman, National Intelligence Council, to the Columbus Council on World Affairs (April 27, 2000), *available at* https://www.cia.gov/news-information/speeches-testimony/2000/gannon_speech_05022000.html.

20. The Verizon network in particular monitors activities coming in from over 150 countries around the world, across 700,000 miles of fiber optics. The NCSD oversees the Cyber Security Tracking, Analysis and Response Center, which conducts ongoing analysis of cyberspace threats and vulnerabilities, issues alerts and warnings for upcoming cyberthreats, and responds to major cybersecurity incidents. Terry McCarthy, *Cyber Attacks Jeopardize Superpower Status,* CBS Reports/USA Today (Apr. 22, 2010), *available at* http://www.cbsnews.com/stories/2010/04/22/eveningnews/main6422768.shtml.

21. Specifically, the NCSD achieves its objectives by the coordinated efforts of three different programs: (1)The National Cyberspace Response System, which coordinates "cyber leadership, processes, and protocols that will determine when and what action(s) need to be taken as cyber incidents arise," including cybersecurity preparedness and the NCAS; (2) the Federal Network Security branch, which serves as a single point of accountability for federal cyber-infrastructure security; and (3) cyber risk management programs, which "assess risk, prioritize resources, and execute protective measures critical to securing our cyber-infrastructure." www.dhs.gov/xabout/structure/editorial_0839.shtm.

22. McCarthy, *supra* note 20.

derstand the tools and techniques hackers use on a regular basis.[23] More recently, the Defense Advanced Research Projects Agency hired a former hacker, Peiter C. Zatko – known to the online world as "Mudge" – to manage the Strategic Technology Office, where he will evaluate funding for research projects to defeat cyber attacks.[24]

Response. Although awareness and reduction of the likelihood of successful attacks are good starting points, they may not always be enough to prevent acts of cyberwarfare. Richard Clarke has noted that market forces and self-interest alone have produced lackluster results, and has called for a regulatory response to the cyberthreat in the form of standards and rules for when and how the standards should be implemented.[25]

Others have advocated that a better approach is to simply do away with questions of whether or not a given attack is state sponsored at all. Former director of the National Security Agency General Michael Hayden (Retired), for example, has suggested that the United States forget about trying to determine whether a specific attack is state sponsored, and instead just hold nations responsible for all malicious activity that can be demonstrated to originate in them.[26]

One proposed legislative response, recently introduced by Senators Joseph Lieberman (Independent-Connecticut), Susan Collins (Republican-Maine), and Thomas Carper (Democrat-Delaware), would be to grant the President broad emergency powers to force covered critical infrastructures, including telecom providers, financial institutions, and software companies, to "immediately comply with any emergency measure or action" DHS orders in cases of emergency or during acts of cyberwarfare. Senate bill 3480, introduced on June 10 and promptly dubbed by the press the Internet "Kill Switch Bill,"[27] would also require covered critical infrastructures to develop and certify to a

---

23. Associated Press, *Wanted: computer hackers … to help government* (Apr. 19, 2009), *available at* http://www.nationalterroralert.com/updates/2009/04/18/wanted-computer-hackers-to-help-government.

24. Elinor Mills, *Hacker 'Mudge' gets DARPA Job*, C|Net News: InSecurity Complex (Feb. 10, 2010), http://news.cnet.com/8301-27080_3-10450552-245.html.

25. Clarke initially denounced regulation as a means to combat attack. More recently, his view has changed, and he argues that regulation frequently represents the only real impetus for change in the IT industry. Richard Clarke, To Regulate or Not to Regulate? That Is the Question, Remarks at RSA Security Conference (Feb. 16, 2005).

26. Kim Zetter, *Former NSA Director: Countries Spewing Cyberattacks Should Be Held Responsible*, Wired.com (July 29, 2010), *available at* http://www.wired.com/threatlevel/2010/07/hayden-at-blackhat/#ixzz0x1Fq07WI.

newly created "Director of Cyberspace Policy" sector-specific security measures and policies for handling cyber vulnerabilities.[28]

The Cyber Security Research and Development Act is at 15 U.S.C. § 7401 et seq.

The National Institute of Standards and Technology research program on computer-system security is covered at 15 U.S.C. § 278h.

The Critical Infrastructures Protection Act of 2001 is codified at 42 U.S.C. § 5195c.

A criminal statute dealing withfraud and related activity involving a computer is at 18 U.S.C. § 1030.

See generally the LexisNexis Matthew Bender treatise Computer Law.

Also of possible interest is an article by Bruce Zagaris, World Summit Fixes on Proposed Cybercrime Prevention and Enforcement Initiatives, 26 International Enforcement Law Reporter 291 (July 2010).

Click here for more Emerging Issues Analyses related to this Area of Law.

About the Authors. Carey Lening is an intellectual property, privacy, and technology attorney in Washington, DC. **Kirsten Koepsel** is Director, Legal Affairs & Tax, Aerospace Industries Association in Arlington, VA. **Ron Weikers** is Managing Partner of Weikers & Co. | Software-Law.com in Manchester, NH, and Adjunct Professor of Law at the University of New Hampshire School of Law. Any views expressed herein are solely the authors', and do not reflect the views of their respective employers.

---

27. Declan McCullagh, *Lieberman defends emergency Net authority plan*, C|Net News (June 15, 2010), http://news.cnet.com/8301-13578_3-20007851-38.html.

28. Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010), available at http://thomas.loc.gov/cgi-bin/query/z?c111:S.3480.