2012

Cyber Security and the Government/ Private Sector Connection

Jeffrey F. Addicott
St. Mary's University School of Law, jaddicott@stmarytx.edu

Spring 2012
Vol. 21, No. 3

pass it on

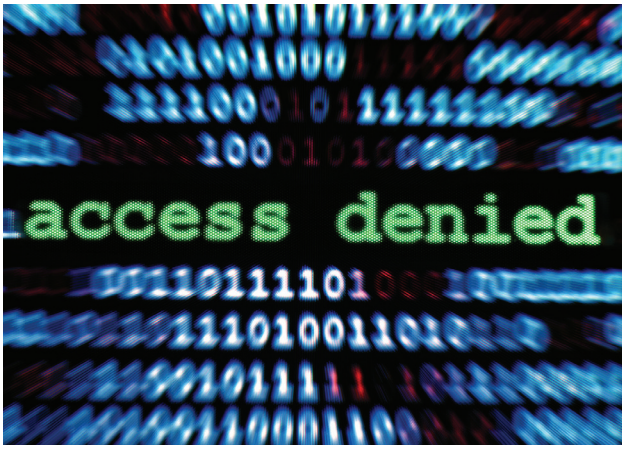
The newsletter of the American Bar Association's Government and Public Sector Lawyers Division

Cyber Security and the Government/Private Sector Connection

By Jeffrey F. Addicott

Recent escalation of alleged Chinese-based hacking of U.S. defense companies and the U.S. Chamber of Commerce, and the coordinated cyber attacks that shut down the entire nation of Estonia in 2007 illustrate the scope of the cyber security threat that exists today. Whether emanating from a terrorist organization, criminal element, severe weather incident or human error, a significant cyber disruption is very likely to affect the United States in the foreseeable future; it is naïve to think otherwise.

Despite these serious risks, most experts agree that the United States does not currently possess a sufficient cyber security framework to adequately protect cyberspace and the information it contains, processes, and transmits. In part, this is because over 85 percent of the critical infrastructure in the United States is controlled by private industry. In most instances, government cyber security standards do not apply to the civilian sector. While the government has embarked on a variety of initiatives with private and public entities to protect against the threat of cyber disruption, many legal and policy issues remain unanswered.



The greatest concern is an intentional cyber attack against the electronic control systems, e.g., the Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, or any equivalent system that regulates the operational functions of our critical infrastructure through thousands of interconnected computers, servers, routers, and switches. The centralized computer networks that monitor and control our entire critical infrastructure present tempting targets. Even a single SCADA disruption could cause enormous economic and physical damage across broad sections of the country. The impact could include massive human casualties, wide-scale economic damage, and significant disruption of national readiness for war.

However, not all disruptions of an information system's confidentiality, integrity, or availability (CIA) constitute a cyber attack. In fact, most disruptions of information systems are caused by unintentional human error and are called cyber incidents. The National Institute of Standards and Technology defines a cyber incident as:

> An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional.

Generally, there are four types of cyber attacks. First, the most common type of cyber attack is service disruption or the distributed denial of service (DDoS) attack, which aims to flood the target computer with data packets or connection requests, thereby making it unavailable to the user or, in the case of a website, unavailable to the website's visitors. DDoS attacks are often conducted utilizing "zombies"—computer systems controlled by a "master" through the utilization of "bots" or "botnets." Service disruption could directly affect any aspect of the critical infrastructure, causing regional or even global damage. A second, but related, type of cyber attack is designed to capture and then control certain elements of cyberspace in order to use them as actual weapons. This strategy was allegedly used in April, 2010 when a state-owned telecommunications company hijacked 15 percent of the internet traffic in the United

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

Tips for Practitioners

Ensure that you are familiar with the applicable state law associated with cyber issues where you practice. Many states have enacted legislation that now requires businesses to notify affected persons when a cyber security breach occurs and personal information is compromised. In addition, some states also require businesses to provide "reasonable" cyber security protections.

Ensure that you have the appropriate level of cyber security to protect the information that you store and transfer. Hiring an outside cyber security professional to evaluate your cyber security protocols and procedures is encouraged.

Understand the criminal statutes—both state and federal—related to prosecuting cyber crime.

States, which included the Pentagon's network and Secretary Gates' office. The third category of cyber attack is aimed at theft of assets from, for example, financial institutions. This activity includes not only theft, but also extortion and fraud. Finally, a cyber attack can be a conventional explosive attack on a physical structure, such as a building that houses a SCADA.

The central focus of cyber security is protection of an information system's CIA. According to the 2005 Congressional Research Service report, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, cyber security refers to:

> a set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software data, as well as other elements of cyberspace. The activities can include security audits, patch management, authentication procedures, access management, and so forth. They can involve, for example, examining and evaluating the strengths and vulnerabilities of the hardware and software used in the country's political and economic electronic infrastructure. They also involve detection and reaction to security events, mitigation of impacts, and recovery of affected components. Other measures can include such things as hardware and software firewalls, physical security such as hardened facilitates, and personnel training and responsibilities.

Starting with the Reagan Administration and continuing to the Obama Administration, the government's approach to cyber security has been one of cooperative engagement and not mandatory regulation. With minor exceptions, when private industry works with the government, the theme of engagement predominates all of the federal laws, executive orders and presidential directives associated with cyberspace. The National Strategy to Secure Cyberspace specifically recognizes that cyberspace constitutes "the control system of our country." In addition, the document recognizes that a comprehensive national strategy must protect against such cyber attacks which "can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life."

In May 2009, the Obama Administration released its Cyberspace Policy Review with a key recommendation centered on the engagement strategy

Editor
Laura Beliveau

Staff Editors
Katherine Mikkelson
Susan Kidd

Comments, letters to the editor and other suggestions
Editor, Government and Public Sector Lawyers Division
American Bar Association
740 15th Street, NW
Washington, DC 20005
202-662-1020

E-mail
GPSLD@americanbar.org

Visit our homepage
www.governmentlawyer.org

Reprint requests must be made in writing to copyright@americanbar.org.

Editorial Statement
Pass It On provides a forum for the discussion of issues of special concern to government and public sector lawyers. *Pass It On* is edited by members of the Government and Public Sector Lawyers Division. Publishing and editorial decisions are based on the editors' judgment of the quality of the writing, the timeliness of the article, and the potential interest to the readers of *Pass It On*. The views in *Pass It On* are those of the authors and may not reflect the official policy of the American Bar Association or the Government and Public Sector Lawyers Division. No endorsement of the views should be inferred unless specifically identified as the official policy of the American Bar Association or the Government and Public Sector Lawyers Division.

AMERICAN BAR ASSOCIATION
Government and Public Sector Lawyers Division

of improving partnerships between the private sector and the government. According to the Cyberspace Policy Review:

> Some members of the private sector continue to express concern that certain federal laws might impede full collaborative partnerships and operational information sharing between the private sector and government. For example, some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership models might be viewed as 'collusive' or contrary to laws forbidding restraints on trade.

Cooperation between the government and the private sector is currently weak. Unfortunately, it is a hard fact that very few private companies have exhibited interest in joining the cyber security effort to the degree that the various government strategies require. Partnering the private industry with the government is imperative to an effective cyber security system. Eventually, the government may be forced to implement mandatory programs to ensure that private industry shares information and develops systems that are more secure. To date, the complacent habit of dealing only with realized threats has not imparted a sense of urgency that will ultimately be necessary to protect the cyber world. Executive Order 13249, signed in January 2010, directs agency heads to promulgate rules and procedures for the sharing of sensitive information with private sector entities and directs the Department of Defense to inspect, accredit and monitor private sector facilities where classified information is or will be used.

Senate Bill 2105 was introduced in February to strengthen computer defenses for private businesses such as banks, telecommunications, transportation, and utilities. The bill would require the Department of Homeland Security to assess the risks

Common Techniques for a Cyber Attack

Type	Description
Spamming	Sending unsolicited commercial email advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use email bait to "phish" for passwords and financial data from the sea of internet users.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. Email spoofing occurs when the sender address and other parts of an email header are altered to appear as though the email originated from a different source. Spoofing hides the origin of an email message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate website. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed website when the user types in a legitimate web address. For example, one pharming technique is to redirect users—without their knowledge—to a different website from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent website when the user types in a legitimate address.
Denial of service attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. Denial of service attacks compromise the availability of the resource.
Distributed denial of service	A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.
Trojan horse	A computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

Source: GAO-07-705, June 2007

and vulnerabilities of such systems to determine which should be required to meet certain risk-based security standards. The bill envisions that DHS would work with company officials to develop performance requirements based on current industry standards. A third party assessor could be used to verify compliance. The bill also proposes information sharing between companies and the federal government with respect to threats, incidents, best practices and fixes. Whether this bill passes and will lead to closer coordination between the private and public sectors remains an unanswered question.

Professor Jeffrey F. Addicott is the Director of the Center for Terrorism Law at St. Mary's University School of Law, San Antonio, Texas. An active duty Army officer in the Judge Advocate General's Corps for twenty years (he retired in 2000 at the rank of Lieutenant Colonel), Professor Addicott spent a quarter of his career as a senior legal advisor to the United States Army's Special Forces. As an internationally recognized authority on national security law, terrorism law and human rights law, Professor Addicott lectures and participates in professional and academic organizations both in the United States and abroad, and is a frequent contributor to national and international news shows including FOX News Channel and MSNBC. Professor Addicott has published over 20 books, articles, and monographs on a variety of legal topics. Addicott's most recent book is Terrorism Law: Cases, Materials, Comments. *This article is a modified version of a chapter in the 6th edition.*

ABA MILITARY PRO BONO PROJECT

The ABA Military Pro Bono Project connects junior-enlisted, active-duty military personnel and their families to civilian attorneys who provide free representation for civil legal issues beyond the scope of services provided by military legal assistance offices. The Project accepts case referrals from military legal assistance attorneys (i.e., JAG attorneys) across the country and around the world, and connects these service members with pro bono attorneys throughout the United States. The Project also includes Operation Stand-By, through which attorneys may volunteer to provide lawyer-to-lawyer consultations to military attorneys in need of information on substantive or state-specific legal issues. For more information or to register as a volunteer with the Project, visit **www.militaryprobono.org**.

E-Discovery in Government Investigations and Criminal Litigation

April 13, 2012
Los Angeles, CA • Millennium Biltmore Hotel

Sponsored by the ABA Criminal Justice Section and cosponsored by the Division.

Discounted registration for government, nonprofit and academics.

See **www.americanbar.org/crimjust** for agenda and registration info.

upcoming division events

Spring Executive Committee Meeting*
May 11 – 12, 2012
Des Moines, IA
***only officers are required to attend**

ABA Annual Meeting
August 3 – 5, 2012
Chicago

Division Fall Meeting
October 19 – 20, 2012
Boulder, CO

FOCUSED FORWARD
ABA 2012 Annual Meeting Chicago

Third National Conference on Employment of Lawyers with Disabilities

May 8, 2012 | Washington, DC | Wardman Marriott Park

Sponsored by the Commission on Disability Rights, cosponsored by the Division.
Discounted registration for government, nonprofit and academics.

See **www.americanbar.org/groups/disabilityrights.html** for agenda and registration info.