Center for International and Security Studies at Maryland
School of Public Policy, University of Maryland

Reducing the Threat of State-to-State Cyber Attack against Critical Infrastructure through International Norms and Agreements

By Jamal Henry

CISSM Working Paper

December 2010

This paper was prepared as part of the Advanced Methods of Cooperative Security Program, with generous support from the John D. and Catherine T. MacArthur Foundation and the Yamamoto-Scheffelin Endowment for Policy Research.

Center for International and Security Studies at Maryland
4113 Van Munching Hall, School of Public Policy
University of Maryland
College Park, MD 20742
(301) 405-7601

UNIVERSITY OF MARYLAND

Introduction

The global proliferation of networked computer systems within the public and private sectors presents an increased opportunity for malicious cyber attacks to disrupt the daily functions of governments, national emergency systems, the global economy, and our modern way of life. The potentially pandemic nature of network failures presents opportunities for states to work together to identify key infrastructure sectors of shared interest and formulate international norms and strategies to protect them from cyber attacks and prevent cascading failures within modern society.[1] Nation-states that share information infrastructure critical to modern social functions will have a vested interest in protecting these systems from cyber attacks while mitigating their own inclination to attack these same networks.

This paper outlines the state-to-state cyber threat to critical-system infrastructures and the role international agreements can play in limiting this threat. The paper has been structured as follows. It begins by defining a critical system and discussing the actors who pose threats to these systems and the motivations behind their decisions. This is followed by a detailed description of a hypothetical scenario that depicts the methods by which one state could attack another state's critical infrastructure, to include the motivations behind the attack. In conclusion, it makes recommendations regarding the development of an international agreement designed to limit this specific type of attack.

Critical Systems

This paper uses the USA PATRIOT Act's definition of a critical system as: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[2] This infrastructure serves as the foundation of several key industries that are critical to modern social functions: the electrical, telecommunications, water, chemical, and energy sectors.[3] These industries use industrial control systems (computer-based control systems that are used to monitor and manage sensitive processes and physical functions) that are increasingly reliant on modern advances in telecommunications and computing—such as wireless transmitting devices, control system computers, dial-up modems, and the Internet.[4] Of all types of industrial control systems, the most common types are supervisory control and data acquisition (SCADA) systems, distributed

[1] Ralstona, P. A, J. Graham, and J. Hieb, "Cyber Security Risk Assessment for SCADA and DCS Networks," *ISA* Transactions, vol. 46, no. 4 (October 2007), pp. 583-594.
[2] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept And Obstruct Terrorism (USA PATRIOT ACT)*, Public Law 107-56, Title X, Section 1016.
[3] Dana A. Shea, "Critical Infrastructure: Control Systems and the Terrorist Threat," Congressional Research Service, updated January 20, 2004.
[4] To amend the *Federal Power Act*, HR 2195 IH, 111th Cong.

control systems (DCS) and programmable logic controllers (PLC).[5] Additionally, many of these systems are connected to the Enterprise Computer System associated with respective industries.

Threat Identification

In *Live Free or Die Hard*, Hollywood's version of a coordinated cyber attack against U.S. critical infrastructure, a highly motivated computer terrorist pays unwitting computer hackers around the world to develop individual parts (functions) of a computer program that he plans to use to hold America hostage. Properly combined, the complete code gives the terrorist (a disgruntled former Department of Defense security expert) the access and subsequently the ability to shutdown power grids, disrupt U.S. government networks, air-traffic control systems, public traffic systems, etc., bringing U.S. society to a screeching halt.[6] The terrorist is successfully stopped before he can conduct his final attack on the U.S. financial sector, thanks to the heroic efforts of one off-duty police officer and one computer hacker.

Stopping an attack of the magnitude portrayed in this movie would have involved several agencies working in close coordination with one another; however, the movie does a good job of depicting the human threat and the type of virtual coordination computer criminals, terrorist organizations, and state actors can employ if they are intent on carrying out a cyber attack. This particular attack would have required an enormous amount of resources and dedication on the part of the attackers, an effort which would have been worthwhile only for extremely motivated, malicious actors. In contrast, critical systems are under constant threat from malicious actors, such as poorly trained or disgruntled employees, hackers, computer criminals, terrorists, and state actors.[7] While each potential threat poses a different level of risk to critical systems, only three types of malicious actors are motivated enough to generate the greatest concerns about carrying out a successful cyber attack against national infrastructure: computer criminals, terrorists, and state actors.

Computer criminals and terrorists pose a significant cyber risk to critical information technology infrastructure and systems due to their motivations and ability to recruit talent. Computer criminals and terrorists are motivated by a range of factors, including the destruction of information, monetary gain, unauthorized data alteration, blackmail, exploitation, revenge, competitive advantage, and economic espionage.[8] Both types of organizations are able to recruit

[5] *USA Patriot Act*; For a simple overview of control system types, see Micrologic Systems, "SCADA Primer," available at www.micrologic-systems.com/primers/scada.html, or Dan Capano, "Distributed Control Systems Primer," available at waterandwastewater.com/www_services/ask_dan_archive/toc.htm.

[6] Bruce Willis, Justin Long, Timothy Olyphant, *Live Free or Die Hard*, directed by Len Wiseman (\Twentieth Century Fox Film Corporation, 2007).

[7] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology," *Risk Management Guide for Information Technology Systems* (2002).

[8] Ibid.

talented individuals of differing backgrounds either through promises of monetary gains or by virtue of shared ideology. Consequently, a successful cyber attack by either type of actor would likely result in a monetary reward or political statement. In the case of organized crime, network data flows associated with financial transactions would be heavily monitored by information technologies, forcing criminals to raise alerts as they attempt to siphon off electronic funds. These goals require criminals and terrorists to quickly acknowledge their attacks, which weakens their effectiveness, as information technology security personnel can quickly search for the exploited vulnerabilities and implement security countermeasures (also known as system hardening). These countermeasures limit sustained damage to the overarching systems. The threat announcements also serve as a mechanism for identifying individuals and organizations to target in law enforcement/military counterstrikes.

State actors are the most capable threat, as they have the ability to funnel significant resources and talents into these efforts, and see cyber attacks as an appropriate countermeasure to an overwhelming threat.[9] State actors can have several motivations for conducting cyber attacks, ranging from economic espionage or political blackmail to the desire for a military advantage in the form of asymmetric warfare.[10] State actors can deem cyber warfare to be a vital national interest and put the full force of government resources (military and civilian talent) behind it. Additionally, like in the movie scenario, state actors also have the ability to outsource this skill set to proxy parties.[11]

What separates cyber attacks perpetrated by state actors from those done by criminals and terrorist is how success is measured. State actors do not need to announce their attack to achieve success. The direct results of a cyber attack, for instance, the disruption of services or espionage, are best achieved and *sustained* by maintaining covert cyber capabilities. These covert capabilities also help insulate state actors from the political fallout (diplomatic, economic, and military retribution) associated with publicly indentified cyber attacks. According to the 2008 threat assessment presented by then-director of national intelligence Michael McConnell, Russia and China are the two nations with the greatest cyber capability and the desire to conduct cyber attacks against the United States.[12] Perceptions of the Russian and Chinese cyber threats are based on several incidents and statements, including the attacks on Estonia in 2007 and on Google in 2010.

In April 2007, a real-world scenario similar to the one captured in *Live Free or Die Hard* played out in the former Soviet republic of Estonia. Malicious actors successfully used remote-controlled computers dispersed over 76 different countries to target and conduct Distributed

[9] John J Kelly, III and Lauri Almann, “eWMDs,” *Policy Review*, no. 152 (2009), p. 39.
[10] “Risk Management Guide for Information Technology Systems,” p. 3.
[11] For example, see David Eshel, “Israel Adds Cyber-Attack to IDF,” *Aviation Week*, February 9, 2010.
[12] Michael McConnell, “Annual Threat Assessment of the Director of National Intelligence,” written testimony to the Senate Select Committee on Intelligence,” February 5, 2008.

Denial of Service (DDoS) attacks against key Estonian services such as banking, telecommunications, media outlets, and even the Estonian Ministry of Defense.[13] Many cyber experts, the Estonian government included, believe that Russia was behind the 2007 Estonia attack and suggest that the attack was a response to the Estonian government's removal of a Soviet-era sculpture from a square in its capital city, Tallinn.[14] Similarly, before the 2008 Russian invasion of Georgia, there were several DDoS attacks against the Georgian government.[15]

The recent global recession highlights the expanding tensions between the rising power, China, and the current superpower, the United States, on economic, political, and military issues.[16] For example, U.S. arms sales to Taiwan and the U.S. president's meeting with the Dali Lama have generated criticism among Chinese military leaders.[17] To further intensify the state of affairs, several Chinese generals have openly advocated modernizing military doctrine to include cyber capabilities.[18] Many cybersecurity experts view the recent attacks against Google servers by Chinese actors (at a Chinese University that has been known to send many of its graduates to the People's Liberation Army) as evidence of this. This action in particular has generated criticism from U.S. government officials.[19]

Vulnerability: Prevalence of Threats

The interconnectedness of the Internet is what makes critical systems vulnerable to both benign and malicious attacks.[20] An unintended consequence of the reliance on new computing and telecommunication technologies is that it creates systems that are increasingly vulnerable to cyber threats from overseas actors.[21] According to Joseph M. Weiss, a cybersecurity expert, until 2000, some industries did not fully understand the possibility that these systems could be networked together to increase efficiency and lower costs.[22] As such, the security of stand-alone systems fell well below optimal efficiency and reliability.

[13] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, vol. 15, no. 9, September 2007.
[14] Ibid.
[15] Dennis Blair, "Annual Threat Assessment of the Director of National Intelligence," written testimony to the Senate Select Committee on Intelligence, February 29, 2009.
[16] Tom Gjelten, "Chinese Attack on Google Seen as Cybertheft," National Public Radio, January 18, 2010.
[17] John Pomfret, "U.S. Sells Weapons to Taiwan Angering China," *Washington Post*, January 30, 2010.
[18] Larry Wortzel, "Preventing Terrorist Attacks, Countering Cyber Intrusions, and Protecting Privacy in Cyberspace," testimony before the Subcommittee on Terrorism and Homeland Security, U.S. Senate, November 17, 2009.
[19] Ibid.
[20] Hugo Teufel, "Privacy Impact Assessment for Einstein 2," U.S. Department of Homeland Security, National Cyber Security Division, May 19, 2008.
[21] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009.
[22] Joseph M. Weiss, "Control Systems Cyber Security: The Need for Appropriate Regulations to Assure the Cyber Security of the Electric grid," testimony to the Committee on Homeland Security's Subcommittee on Emerging Threats, Cyber-security, and Science and Technology, October 17, 2007.

Another factor is that the reliability and availability of critical systems is typically more important to industry than requirements of confidentiality. As such, anything that adversely affects the former is frowned upon. Weiss also notes that information technology security practices, such as port scanning, which can be used to gain access to a system, can damage older-generation PLCs and are often discouraged.[23] Security activities such as port scanning also use large amounts of computer system resources. These resources are shared with more functional features of PLCs and are not available to them until activities such as port scanning have ended. Resource sharing occurs at very high speeds but still produces a noticeable degradation in system capabilities overall. Also, many of the control systems used in the United States are outdated, as they were created during a time when the greatest risk to our national infrastructure was posed by physical attacks or a disgruntled employee.[24]

No one network infrastructure is more important than the production of a continuously reliable supply of electricity, the backbone for all other systems.[25] Michael Assante, the vice president and chief security officer of the North American Electric Reliability Corporation (NERC) put it this way: “We, as an industry, must also consider the effect that the loss of that substation, or an attack resulting in the concurrent loss of multiple facilities, or its malicious operation, could have on the generation connected to it.”[26]

Threat Scenario: An Energy-Sector Cyber Attack

In 1997, the concept of NERCnet was born. The system was designed to allow “all” participants in the electric power industry to communicate in order that businesses could run reliably and securely. NERCnet is a shared communications infrastructure platform designed to securely receive and transmit “proprietary” energy information between NERC facilities. At the time, many of these businesses did not have robust connections to the Internet, so it is unlikely that this network was “impervious to outside ‘attack’ while being open to all intended users.”[27]

Weak information technology security measures in one business’s network create vulnerabilities for the entire system. Because of weak security measures, two attack scenarios are possible. In the first, a nation-state “outsources” a DDoS attack against control systems to take them off line,

[23] Ibid.

[24] “The Smart Grid: An Introduction,” Department of Energy’s Office of Electricity Delivery and Energy Reliability, 2008.

[25] “Grid 2030: A National Vision for Electricity’s Second 100 Years,” Department of Energy’s Office of Electric Transmission and Distribution, July 2003.

[26] Michael Assante, “Critical Cyber Asset Identification,” North American Electric Reliability Corporation, a letter to “Industry Stakeholders,” April 7, 2009.

[27] North American Electric Reliability Council, “Agenda Item 2: NERCNet,” agenda for the Joint Engineering Committee/Operating Committee meeting, July 8, 1997.

shutting down portions of an electrical grid or the entire grid. A second scenario could involve a nation-state taking control of this architecture and using it to elicit a reaction from the attacked state.

There are two methods for hacking into any computer system: the first is through brute force, manually scanning target networks from the Internet to determine weaknesses and vulnerabilities that would be key to exploit; the second is to exploit human errors.[28] Criminals and terrorists can employ either method, but as mentioned earlier, state actors pose the greatest threat to these types of SCADA systems.

Assumptions

Throughout the following hypothetical attack scenario, we make several assumptions about likely state-to-state cyber campaigns. The first is that the attacking state (state X) has a group of sophisticated *hackers* that are familiar enough with computer security, architecture, and programming to successfully complete an attack against another state (state Y). Second, we assume that this team has been given the authority/freedom to act on behalf of the attacking state. Third, the attack's objectives are well outlined, i.e. the attack is meant to give the attacking state a strategic or tactical advantage over state Y. Fourth, the hackers of the attacking nation have already co-opted several geographically dispersed and unrelated computer systems (botnets) to use as their attack platform, in an effort to obfuscate the attacking state's role.[29]

The particular scenario described below assumes that the attacking state has already identified a NERC facility as the initial target of their cyber campaign. In planning the attack, the hackers decided to exploit human errors to gain access to systems.

Identifying a Target Network

The first step for the attackers is to gather as much information as possible related to the target computer systems and their security postures through a technique known as footprinting. Footprinting involves performing computer-network reconnaissance by employing computer security tools and techniques to reveal the target's Internet profile and computer network infrastructure (e.g. Internet, intranet, remote accesses, operating systems, employee profiles, etc).[30] The ultimate goal is to reduce a target to a collection of computer systems (technical network information) and resources (social human information) that can be exploited by the attacker. Given NERCnet's structure, an attacker interested in disrupting an electrical substation would first gather as much publicly available information about NERC facilities and any

[28] Stuart McClure, Joel Scambra, and George Kurtz, *Hacking Exposed: Network Security Secrets & Solutions,* 5th Edition (New York: McGraw-Hill, 2009).
[29] Jivesh Govil and Jivika Govil, "Criminology of BotNets and their Detection and Defense Methods," Proceedings of the 2007 IEEE International Conference on Electro-Information Technology, 2007.
[30] McClure, Scambra, and Kurtz, *Hacking Exposed.*

connected management companies. For the purposes of this scenario, a fictional entity, NNCompanyZ, manages the relevant NERC facilities.

Attackers would gather both social and network-related information. Network information that could be gathered for an attack includes: Domain Name System (DNS), Internet-accessible Internet Protocol (IP) addresses (cyber street address), computer system architecture, services running, OSs, etc. A DNS correlates a computer's IP address (ex. ###.###.###.###) into a word that people can more readily remember. Using DNS query tools, such as NsLookup, an attacker can take NNCompanyZ's Domain Name NNCompanyZ.com and identify an IP address (192.168.0.4) associated with one of the company's computers.[31] The attackers can then use a function known as Ping to determine what type of OS is associated with the IP address 192.168.0.4. For instance, if a Ping sent to 192.168.0.4 returns a response of Time To Live (ttl) 128 the attacker has gained several pieces of valuable information: machine 192.168.0.4 is operational; machine 192.168.0.4 is connected to the Internet (potentially accessible remotely); machine 192.168.0.4 is running a version of Microsoft Windows operating system; NNCompanyZ likely has additional machines running Microsoft Windows operating system (associated services); the attacker should focus on Windows operating system vulnerabilities and exploits.[32]

Social information that could be gathered for an attack includes: company web pages, subsidiary organizations, geographical location details, personnel contact information, security postures, current events, disgruntled employees, etc. If an attacker inserts the previously gained IP address of 192.168.0.4 into WHOIS websites, such as Whois.net, the attacker could identify contact information for the individuals associated with NNCompanyZ's website: full name, email address (joe.systemadminstrator@NNCompanyZ.com), location, and phone number.[33] WHOIS queries will also reveal the names of other machines. The attackers could then use this information, particularly email addresses, to gain information that could be used in social engineering techniques through popular search engines (Google, Yahoo, etc.), to identify group forums and other email addresses used by employees of NNCompanyZ. Additionally, an attacker could use these same search engines to see if any company employees are members of social networking sites such as Facebook or Myspace (these sites are often linked to web-mail accounts), using these to gain additional information on employees.[34]

Gaining Access to the Target Network

The next step in the attack would require the attackers to gain access to any machine inside NNCompanyZ. This is often referred to as a foothold. To accomplish this goal, the attacker

[31] Harry Newton, *Newton's Telecom Dictionary*, 21st Edition (Gilroy, Calif.: CMP Books, 2005)
[32] McClure, Scambra, and Kurtz, *Hacking Exposed.*
[33] The full URL is http://whois.net/.
[34] McClure, Scambra, and Kurtz, *Hacking Exposed.*

would use previously gained network and social information to launch a phishing (pronounced fishing) attack against targets of opportunity, NNcompanyZ employees with low computer-security awareness due to poor training.

The attacker could then set up a mirror version of the NNCompanyZ website (NNCompanyZ.com), known as a spoofed website, which would look almost identical to the original (NNCompanyZ.com).[35] Included in the web page could be images, known as web bugs, of legitimate items (i.e. company logos, etc.) and cookies that can monitor and store key private information about visitors such as type of web browsers used, IP addresses, passwords, and the number of site visits.[36] The spoofed webpage could also contain hyperlinks that are embedded with malicious tags or scripts created using cross-site scripting techniques.[37] The attacker could then send unsolicited emails, using a fictitious @NNCompanyZ.com address, to all potential victims at the company that redirect them to the mirrored site. Any NNCcompanyZ employee who visits the mirrored site from work will unknowingly execute the malicious code onto his/her work computer (192.168.0.4) by clicking any of the links, creating an opportunity for an additional computer program known as Rootkit to be left behind, providing the attacker a mechanism to covertly copy directories, update system registries, and use local-user applications to communicate to the Internet.[38] Additional programs or spyware, such as keystroke loggers, could also be implanted within a victim machine(s), and the information they harvest can be forwarded to the attackers to enable the next step of the attack.

Network Enumeration

Once the attackers have established a foothold within the network, the next step is to perform a more robust and intrusive form of internal footprinting to gather information necessary to access systems associated with the overall objective of the cyber attack. This technique is referred to as network enumeration. Network enumeration involves a process where additional users' accounts (specifically privileged accounts such as system administrators'), shared services, software, internal network computers systems, and operating systems are identified.[39] Attackers could use tools and techniques similar to those used in step 1 (Ping and NsLookup) to gather internal network information, but additional custom network survey tools (Nbtscan, SuperScan etc.)

[35] "How to Recognize Spoofed Web sites," an online tutorial prepared by Microsoft Security and available at www.microsoft.com/protect/frau/phishing/spoof.aspx .

[36] Stefanie Olsen, "Nearly Undetectable Tracking Device Raises Concern," CNET News, July 12, 2000.

[37] "Cross-Site Scripting (XSS)," an entry on the Open Web Application Security Project (OWASP).

[38] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis, "A Multifaceted Approach to Understanding the BotNet Phenomenon," Proceedings of the 6th ACM SIGCOMM conference on Internet Measurement, pp. 41-52, October 2007.

[39] McClure, Scambra, and Kurtz, *Hacking Exposed.*

could also help to create a network topology that could be used as a road map to get to the ultimate target, the control systems.[40]

Returning to the attacker foothold machine, 192.168.0.4, the attacker can begin to look for a NNCompanyZ machine that connects to the electrical substation's network. Because this machine is running Windows, the attacker can use NetBIOS-based tools such as Nbtscan. By issuing the command *C:\>nbtscan 192.168.0.0 /24*, an attacker could gain information on other internal computer systems such as their host names, IP addresses, associated users, and MAC addresses, as well as to identify any network shares that could host other closely held information.[41] Network mapping tools are commonly used by system administrators, and if 192.168.0.4 is used by a system administrator, many of these tools may already be installed on the computer system, for the attacker to access. Accessing passwords obtained from the keystroke logging software installed earlier, the attackers may be able to remotely log in to the system administrator machine, 192.168.0.6, and find documents detailing the location of the machine that can remotely communicate with the electrical substation control systems. If the documents list the machine's IP address as 192.168.0.7, the attackers would easily be able to determine that the system exists and is running a version of Windows.

Identify Vulnerable System Services & Programs

As a next step, the attackers could identify exploitable vulnerabilities within the target computer systems in order to gain access to them. Unlike earlier steps, where the attackers simply tricked NNCompanyZ employees into installing malware, the attacker would have to identify all of the services and programs running on the machine and correlate them to known vulnerabilities. This can be accomplished by using network tools (SuperScan, Netcat) known as port scanners.[42] Identifying security-patch updates and querying systems to see if they have received them is an additional method for pinpointing vulnerable systems.

Port scanners attempt to connect to remote TCP and UDP protocol ports to determine if services associated with those ports are running/listening. From the system administrator's machine, 192.168.0.6, the attacker could issue a NetCat command (*C:\>nc –v –n –z –w1 192.168.0.7*), which would attempt to connect to each port on the system and return a response of open for the ports that it can reach. In this case, one response would be: [192.168.0.7] 23 open. This would indicate that Port 23, which is associated with the command Telnet, is open on the 192.168.0.7 machine and is able to remotely connect into the control system. The attacker can now tailor exploits that remotely target Port 23. Additionally, the attacker can develop/find exploits for other open ports.

[40] For additional information about SuperScan, see www.foundstone.com.
[41] McClure, Scambra, and Kurtz, *Hacking Exposed.*
[42] McClure, Scambra, and Kurtz, *Hacking Exposed.*

Security patches are “critical” updates to software programs and operating systems issued by manufactures to address known security vulnerabilities and to protect against viruses and worms. The patches can be pushed out to targeted systems remotely, or system users can go directly to manufacturers’ websites to download them. Attackers often research newly released patches because many people opt to manually download patches instead of having their systems automatically updated, thus allowing their systems to remain vulnerable for an extended period of time. In the attack scenario described above, the attackers can identify the most vulnerable system services by comparing the services running, discovered through port scans, to recently issued patch updates for the same services, using standard search engines such as Google.[43]

For instance, the attacker could identify a recent Microsoft Windows patch that has been issued for several Windows OSs, one of which is currently running on 192.168.0.7. The machine has not yet received the patch, because system users are concerned that any modification will disrupt the control system, causing the electrical substation to shut down and producing a massive power loss.[44] Using additional malicious code (viruses, worm, custom scripts, etc.) based on this particular vulnerability, the attacker could successfully exploit 192.168.0.7. Once access is achieved, the attacker could implant the system with backdoors and rootkits, which would provide continuous access to the system for later visits.

Covering their Tracks

The primary goal of sophisticated attackers is to surreptitiously break into computer systems to ensure prolonged access to compromised machines. Once a security system administrator identifies a compromised system it is his duty to remove the system and reduce the attacker’s ability to maintain unauthorized access. Audit logs are the primary tools in the system administrator tool belt for detecting unauthorized system access. In ideal circumstances, these logs contain all network transactions, and a savvy system administrator can develop scripts and programs to quickly identify erroneous actions.

Conversely, a savvy attacker will take the time to edit these same logs, removing any indication of their presence and their backdoors/rootkits.[45] In general, an attacker tries to mitigate his detection and complicity throughout an entire attack. By using a Botmachine (192.168.255.303), he can obfuscate the true IP address from which attack commands were issued (192.168.155.33). The hypothetical attacker would know that the NNCompanyZ system logs include the IP address 192.168.255.303 and would take great pains to remove this IP address from all computer logs.

[43] McClure, Scambra, and Kurtz, *Hacking Exposed.*
[44] Joseph M. Weiss, “Control Systems Cyber Security.”
[45] McClure, Scambra, and Kurtz, *Hacking Exposed.*

Additionally, an attacker can use a rootkit such as Hacker Defender to achieve greater stealth and create a backdoor.[46]

Achieve Final Objectives

For the purposes of this scenario, let's assume that the attackers maintain access to the compromised systems until they are caught or given a direct order from state X. During this time, the attacker could either collect as much information on the end-target system as possible or begin a DDoS attack.[47] The DDoS attack would begin shutting down the control systems and subsequently the electrical substation.

State X decides to maintain accesses within NNCompanyZ and the connecting electrical substation in state Y. It also directs the attacker to identify other NNCompanies within state Y to gain complete access to its electrical grid system. It could use this access as leverage in the event that hostilities between the states arise as a consequence of territorial disputes over Island XYZ.

Exploring International Agreements on Cybersecurity

The above attack scenario illustrates several problems facing efforts to stem cyber attacks against critical infrastructure. First, a disruption of state Y's power grid weakens only state Y, where state X's electrical system continues to run unhindered (provided state Y is not prepositioned for a retaliatory cyber or military strike). Second, the architect behind the attack, state X, has strategic diplomatic and military incentives for conscripting hackers to gain control of state Y's electrical system. Third, proving that state X is connected to the attack will be very difficult; the use of hackers creates a secondary layer between state Y and liability for the attack. An attacker's ability to operate in more than 192 countries simultaneously means that there is little likelihood of being indentified.[48] Finally, in the unlikely event that the attacker is identified, the limited patchwork of domestic and international laws and punishments would not sufficiently deter other attackers.

Recent cases, such as the 2007 "Uppsala hacker" and the 1994 conviction of Julian Assange (founder of Wikileaks), depict the problems that domestic and international laws confront in attempting to deter international and domestic hacking. In the case of the Uppsala hacker, a conviction in Sweden did not guarantee that the offender would also be prosecuted in the United

[46] For additional information about Hacker Defender, see www.f-secure.com/v-descs/hacdef.shtml.
[47] Anestis Karasaridis, Brian Rexroads, and David Hoeflin, "Wide-Scale BotNet Detection and Characterization," Proceedings of HotBots '07, the First Workshop on Hot Topics in Understanding Botnets, April 10, 2007.
[48] For a complete list of Internet usage statistics, see www.internetworldstats.com.

States.[49] Meanwhile the fine levied against Assange following his conviction on 25 counts of hacking and related crimes was relatively small.[50] The only way to successfully prosecute an attacker is for nations to build a common framework or set of standards that discourages attacks from occurring in the first place. This framework must also establish mechanisms to prosecute and convict cyber perpetrators, with the penalties tough enough to deter other would be perpetrators.

Creating such an arrangement would be a challenge, as it would require legal and technological cooperation among nations who actively guard their technological capabilities as a matter of national security. Any framework or international agreement that would seek to decrease states' internal motivations to transform cyberspace into a platform for attacking civilian facilities and institutions, while increasing the number of cyber barriers to nonstate actors' intent on conducting similarly malicious cyber campaigns, would need to be sufficiently broad and sufficiently detailed. At a minimum, it would require the creation of a new international organization responsible for the collective protection and management of the information technology infrastructure supporting critical facilities and institutions. This organization would be responsible for working with specific industries to create open-architecture systems based on new international standards. And it would also be responsible for staffing newly formed International Network Operation Centers (iNOCs) that are capable of overseeing day-to-day network performance, rapid threat detection and prevention, as well as sharing and coordinating threat information with signatory states and private-sector companies. Signatory states would have to develop domestic legislation to support the legal implementation of any new international agreements.

Prior Attempts at International Cyber Defense

The Council of Europe's Convention on Cybercrime was the first international treaty designed to address the global nature of cyber-threats and recognize the risks to financial institutions, critical infrastructure facilities, and government systems.[51] In 2001, the Council of Europe (which includes 25 members of the European Union and 20 additional European nations) along with Canada, Japan, South Africa, and the United States convened to develop a legal convention to deal with the international threat of cyber crimes. The meeting was partly in response to the devastating effects of the September 11th terrorist attack in the United States, and partly in response to the increasing number of criminal cyber attacks against European financial institutions.

[49] Linus Larsson, "Alleged Cisco Hacker Convicted in Sweden, Bewails Fate," *Computer World*, November 21, 2007.

[50] Raffi Khatchadourian, "No Secrets: Julian Assange's Mission for Total Transparency," *The New Yorker*, June 16, 2010.

[51] Kristin Archick, "Cybercrime: The Council of Europe Convention," Congressional Research Service Report, July 22, 2004.

The convention that emerged from the effort identifies several key areas in which nations can work together to deter computer crimes. While the convention's main focus is cyber crime, it also addresses several key issues relevant to future cyber treaties that are likely to focus on politically motivated cyber attacks against critical infrastructure: data and system interference, misuse of devices, search and seizures (trans-border), and real-time data collection. However, the convention does not directly address the issue of cyber warfare. Another limiting factor is Russia's and China's nonparticipation in the treaty due to concerns about the potential violation of their sovereignty.

Mitigation through Risk Sharing

Any future international agreement to limit the threat of cyber attacks would require the participation of all nations with strong offensive cyber attack capabilities, including Russia and China.[52] Unless the nations with the most to gain are properly motivated to participate in an agreement, the effects will be minimal. The fundamental challenge will be to motivate all necessary states to agree on how to manage the risks posed by critical systems in order to decrease the strategic motivations of cyber attacks.

In general, nations that agree that there is a shared risk to a common resource will be more inclined to share in the protection of that resource.[53] Therefore, the scope of any agreement should focus on systems that major nations feel they have strategic reason to protect. It is a daunting challenge to identify the information technology networks that need protection when nations (specifically Russia, China, and the United States) view the Internet in different ways—for example, as either a strategic/sovereign asset or a common resource. But it is not an unprecedented one.[54] Several instances in recent history demonstrate how overwhelming support for an international agreement resulted from a perceived shared threat: the Nuclear Non-Proliferation Treaty (NPT), the Outer Space Treaty, and agreements regarding maritime piracy and international terrorism.

Of these three examples, the most relevant to a potential agreement on cyber attacks are the agreements on maritime piracy and international terrorism. The technological sophistication and expertise necessary to build nuclear weapons or to put weapons of mass destruction in space present so high a barrier to most nations that it has been easier for them to become a party to the NPT and the Outer Space Treaty than it would be to participate in prohibited activities.[55] To violate or ignore either treaty, a nation would have to develop or procure specific infrastructure

[52] Michael McConnell, "Annual Threat Assessment of the Director of National Intelligence."

[53] See "Comfort Blanket for the Gulf," *Economist*, December 5, 1992, pp. 39-40.

[54] Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law*, vol. 27, no. 1 (2009), pp. 192-251.

[55] Office of General Counsel, Department of Defense, "An Assessment of International Legal Issues in Information Operations," May 1999.

and equipment and devote a tremendous amount of financial resources and human capital to the tasks. Cyber attacks on the other hand can be conducted on borrowed infrastructure that is stored anywhere in the world and carried out by a small number of people drawn from an increasing large number of computer professionals.

The technological sophistication and expertise to conduct cyber attacks is closer to the expertise required to conduct both terrorism and piracy.[56] Therefore, we focus on treaties and international frameworks aimed at bridging opposing national viewpoints on international piracy and international terrorism to see if it is possible to formulate a more inclusive version of the Council of Europe's Convention on Cybercrime.

A Foundation for Future Agreements

Major competing states have previously agreed to work together to combat the threat of piracy and international terrorism because they believed that piracy and terrorism posed credible threats to their security. We will begin our discussion with maritime piracy laws, as these are the more established of the two.

International maritime piracy laws serve as the foundation on which international bodies, such as Interpol, defend against and prosecute piracy.[57] Like cyber activities, piracy typically occurs beyond the boundaries of any one state. As a consequence, nations have agreed to treat piracy as a violation of international law, granting nations the ability to prosecute maritime piracy on the "high seas." This is one of the defining principles of universal jurisdiction.[58] This approach defines the scope of piracy as any activity that threatens lines of communication or trade, or regional stability. As such, nations treat the open seas as a global commons.

Over time, national self-interest and a countries' reliance on the maritime trade of energy have increased participation in piracy agreements to more than 155 nations, including China.[59] Indeed, piracy is one among a few issues for which policies are consistent no matter what type of government is in power. In this sense, anti-piracy laws have helped to create international norms that have subsequently been applied to non-state actors who threaten common resources.

International efforts to contain and discourage terrorism have a less even record of success. Terrorists share some traits and tactics with pirates, including the use of violence and fear, and

[56] Ibid.
[57] James Kraska and Brian Wilson, "Maritime Piracy in East Africa," *Journal of International Affairs*, vol. 62, no. 2 (2009), pp. 55-68; see also, "Agreement of Co-Operation Between The International Maritime Organization and the International Criminal Police Organization – INTERPOL," 2005
[58] Ibid.
[59] Zou Keyuan, "Seeking Effectiveness for the Crackdown on Piracy at Sea," *Journal of International Affairs*, vol. 59, no. 1 (2005), pp. 117-134.

the capacity to act outside of national boundaries. But the spectrum of motivations behind terrorism, primarily political grievances, makes it difficult to collectively address it with cohesive international norms. Indeed, sovereign nations have only recently begun to address terrorism, with the first international agreement on terrorism, the League of Nations' Convention for the Prevention and Punishment of Terrorism, only being enacted in 1937. Since then, an additional 13 international agreements regarding terrorism have been negotiated.[60] The relatively short history of international agreements dealing with this issue allows nations' interpretations of these agreements to vary, making prosecuting international terrorism difficult.[61] Universal jurisdiction is not as well established for terrorism as it is for piracy. [62] Additionally, terrorists, like the hackers in our attack scenario, can be conscripted by a nation-state to carry out an attack on its behalf, complicating enforcement.[63]

Define Critical IT Infrastructure

The first goal of any new international agreement on cyber attacks should be to determine its scope: What critical infrastructure should it encompass? This list should be designed to encourage participation by as many key nations as possible.[64] Bringing nations such as China and Russia under the same treaty will be challenging, as these nations do not necessarily share Western interpretations of the Internet as a common resource used for the free flow of information.[65] China, in particular, views the Internet as a strategic resource it can control and shape within its own borders. To entice China to participate, an agreement should limit its scope to specific types of infrastructure.

One way to limit an agreement's scope would be for potential parties to agree to a list of specific elements of infrastructure that are key to societal function. Parts of the financial industry infrastructure have historically been vulnerable to external, violent threats such as piracy and terrorism. Indeed, "pirates have been a major impediment to trade among 'civilized' states, while terrorism similarly causes modern commerce to stop in its tracks."[66] The global economic crisis of 2007-2010 graphically depicted the societal ramifications of financial system failures, ranging from demonstrations of civil unrest to increases in organized crime.[67] Therefore, any international treaty should focus on the information technology infrastructure supporting

[60] A list of UN action to counter terrorism is available at www.un.org/terrorism/instruments.shtml.

[61] Steven Swanson, "Terrorism, Piracy, and the Alien Tort Statute," *Rutgers Law Journal*, vol. 40, no.1 (Fall 2008) pp.159-217.

[62] Stephan Wilske and Teresa Schiller. "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?" *Federal Communications Law Journal*, vol. 50, no.1 (December 1997), pp. 117-78.

[63] Mariamand Karouny and Laila Bassam, "Israel Attack on Iran Could Ignite Middle East: Hezbollah," Reuters, March 18, 2010.

[64] Shackelford, "From Nuclear War to Net War."

[65] See "Comfort Blanket for the Gulf," *Economist*, December 5, 1992, pp. 39-40.

[66] Swanson, "Terrorism, Piracy, and the Alien Tort Statute."

[67] Peter Apps, "Financial Crisis Fuels Unrest and Crime, but War Risk Eases," Reuters, June 8, 2010.

financial systems, communication systems (emergency systems, air traffic control), and the electrical systems that support the first two. In contrast, infrastructure associated with military organizations would not be covered by this treaty. Military organizations have insular structures that are separate from the societies within which they sit. Additionally, militaries inherently evoke national security concerns when asked to limit their capabilities.

Financial Systems

Cyber attacks on key financial systems pose the potential to bring the world economy to a halt. Due to the interconnectedness of the modern banking system, protecting this infrastructure would seem to be the first logical step in defining what infrastructure can be universally accepted as critical infrastructure. The degree to which the global economic crisis illustrates the interconnectedness of the world's financial markets makes global banking networks—commercial banks, insurance companies, mutual funds, and other financial institutions that carry out transactions—the ideal vehicles for spurring international cybersecurity cooperation and norms.[68] Most cyber attacks against financial institutions are carried out by criminal organizations; these crimes threaten the entire system because ransoms paid by one bank to prevent a DDoS attempt will spur second and third attempts. Additionally, banks are vulnerable to cyber attacks for obvious profit reasons, but they typically do not report attacks for fear of scaring customers away or causing a run on the bank. Private banks would be more apt to share this information with the federal government, if the government agreed to keep it private.

Emergency Systems

Even as financial institutions look to protect the data within their networks, other systems that they do not control remain vulnerable. Any international agreement on cyber attacks should also address vulnerabilities in computer network systems that are used by operations protected under the Geneva Convention during times of war. This sector includes fire, rescue, emergency medical services, and law enforcement organizations tasked with saving lives and property from accidents and disaster. This category should include both critical medical networks and supporting electrical grid infrastructures.

Energy Systems

These systems provide the electrical power used by all other sectors. Most electrical systems are currently designed to provide power to a particular region or geographical area. Thus, it should be possible to isolate and deem as critical infrastructure parts of the electrical system that govern, say, emergency response centers.[69] In contrast, electrical systems that provide electricity to

[68] General Accounting Office, "Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors," July 2004.
[69] Gorman, "Electricity Grid in U.S. Penetrated by Spies."

military bases would not be covered under an agreement, unless participants had previously agreed to protect the electrical systems for certain facilities, such as those where nuclear weapons are safeguarded. Yet, as nations move to smart grids, the control of electrical grids will be influenced more and more by advanced communication technologies, and electricity will be redirected to where it is needed. This will make it more difficult to isolate certain sections of the electrical system.

An International Organization

If an agreement is to increase the international community's (signatory nations') capability to defend against cyber attacks, it must increase the community's ability to recognize the signs of an attack, share critical information across disparate industries, and, most importantly, limit the desire and motivation for a state to attack. (Many of these issues were originally addressed in the Convention on Cybercrime). One way to do this would be to create an international security organization composed of information technology security representatives from each signatory state, and to task the organization with coordinating and collaborating joint security measures with states and industries.[70]

Standards and Shared Systems: Complexity and Risk

As its first step, the new organization could address the strategic motivations of states that conduct cyber attacks and spread the risks and the associated costs of defending key information technology infrastructure to all parties through the use of shared hardware platforms that are based on international standards. Using shared information technology resources would limit states' motivation and capability to use cyber attacks asymmetrically against critical systems.

Sharing resources would also dramatically shift states' decision calculus. One suggestion has been to expand the concepts of NercNet and information sharing and analysis centers (ISACs) to participating nations and create one umbrella organization capable of monitoring and defending all critical information technology infrastructure. The administration of George W. Bush initially proposed this concept in the form of the Cyber Warning Information Network (CWIN).[71] The benefit of this type of organization would be that it would build on existing organizations, such as the ISACs which were developed under President William J. Clinton for the banking and finance, telecommunications, and energy industries.[72] Information sharing is most effective when all parties are able to used shared terminology. The most effective way to develop a system of

[70] Mohamed Dafir Ech-Cherif El Kettani and Taieb Debbagh, "NCSecMM: A National Cyber Secuirty Maturity Model for an Interoperable 'National Cyber Security' Framework," Proceedings of the 9th European Conference on E-Government, 2009, pp. 236-247.

[71] Joseph Patterson Hyder, "Cyber Security Warning Network," in K. Lee Lerner and Brenda W. Lerner (eds.) *Encyclopedia of Espionage, Intelligence, and Security*, (Farmington Hill, Mich.: Gale, 2004).

[72] Ibid.

shared terminology is to create an entirely new system based on newly designed security protocols and standards.

International Standards: Reduction of Complexity

The development of common international standards for large computer systems would both increase information sharing and reduce complexity, increasing cybersecurity.[73] If all nations adopt the same standards, security practices and protocols can also become more standard, as can the methods employed by network security personnel to detect attacks.[74]

Individual companies, industries, and governments currently develop their own security mechanisms to protect computer networks and data critical to their operation. The result is a hodgepodge of encryption schemes, protocols, network infrastructures, computer architectures, and levels of security, each of which reflects the understanding of the particular system administrator.[75] Some industry experts believe that this level of complexity and diversity provides its own form of protection by preventing one attack from successfully compromising all systems–an idea that security professionals refer to as security through obscurity.[76] This type of security often creates a false sense of protection, however, as complex systems are not just harder for attackers to understand but also for those in charge to understand.

Indeed, complex systems are often less secure because complexity increases the number of security bugs, modularity becomes difficult to maintain, and the testing requirements and scenarios of vulnerabilities expand exponentially. These systems are hard to fully understand and more importantly they are hard to analyze. As demonstrated in the hypothetical attack scenario against NNCompanyZ, would-be attackers do not need to understand all of a system’s perimeter defenses, they simply need to isolate the most easily accessible point. If a system is designed to provide security through obscurity, a complex attack would be difficult to detect.[77]

Creating international standards for common and familiar information technology platforms would decrease the learning curve for basic cyberdefenses, increasing system administrators’ ability to successfully defend their networks.[78] Standardization accomplishes this by creating more learning cycles for more advanced cyber security training, which would allow network

[73] Yonghee Shin and Laurie Williams, “Is Complexity Really the Enemy of Software Security?” *Proceedings of the ACM Conference on Computer and Communications Security*, 2008, pp. 47-50.
[74]Ellen Fussell Policastro, “Security Standard Hopes to Go Global,” *InTech*, vol. 54, no. 4 (April 2007), p. 68.
[75] Weiss, “Control Systems Cyber Security.”
[76] Shin and Williams, “Is Complexity Really the Enemy of Software Security?”
[77] Jaap-Henk Hoepman and Bart Jacobs, “Increased Security Through Open Source,” *Communications of the ACM*, vol. 50, no. 1 (January 2007), pp.79-83.
[78] Margareth Stoll, “E-Learning Promotes Information Security,” in M. Iskander (ed.), *Innovative Techniques in Instruction Technology, E-Learning, E-Assessment and Education* (2008), pp. 309-314.

administrators to identify, detect, and defeat sophisticated attacks against their systems.[79] For example, a system administrator who has a Cisco Certified Network Associate certification and is familiar with Cisco routing equipment, the de facto industry standard, is far more valuable in the information technology market than a professional who does not have this training and experience. Moreover, common international protocols and standards are just that, international. An information technology professional in China will have the same basic understanding as a professional in the United States regarding the Open System Interconnection (OSI) model.[80] The International Standard Organization (ISO)'s early attempts to define networking protocols and distributed applications have dramatically advanced computer development.[81] Similar organizations could develop system-specific security standards for each of the previously defined critical infrastructure nodes.[82]

Shared Systems: Shared Risk

Once international cybersecurity standards are developed, nations could build a common computer infrastructure that is responsible for previously agreed upon systems that are too important to fail, essentially expanding the ideas of the NercNet to other key nations and critical nodes. This shared infrastructure would create a strong framework for information sharing and physical information technology platforms to which party nations would have equal access and understanding. A common system architecture would have several broad benefits. It would make educating information technology professionals regardless of their nationality far simpler. Sharing responsibility for network failures would also ensure that nations, specifically the United States, China, and Russia, accept shared responsibility for the protection and availability of the critical network infrastructure system. A shared infrastructure would also distribute the financial penalties of cyber attacks among the three main parties and create a shared incentive for identifying robust solutions to attacks.

Any critical infrastructure node that features new computer architecture systems should be based on open-system design principles, with consideration for industry specific standards. An "open system" architecture would draw on common knowledge and expertise from all participating nations.[83] In the article "See Past Self-Proclaimed Experts' Open-Source Security Evaluations," Michael Wolfe argues that the primary flaw with open systems is that they require trust from all

[79] A learning cycle, conceptualized by David Kolb, reflects a cycle comprised of experience, reflection, theorizing and experimenting. See David A. Kolb, *Experiential Learning; Experience as the Source of Learning and Development* (New Jersey: Prentice-Hall, 1984).

[80] Barry Boehm, "A View of 20th and 21st Century Software Engineering," Proceedings of the 28th International Conference on Software Engineering, May 20-28, 2006.

[81] General Accounting Office, "Critical Infrastructure Protection."

[82] Kate McMillan, "Technology Standards Pros Aid Homeland Security," *Computer*, vol. 35, no. 5 (May 2002), pp. 104-5.

[83] Hoepman and Jacobs, "Increased Security Through Open Source."

parties involved.[84] In reality, an open-system architecture for critical infrastructure would not need to be 100-percent open. Making certain information available only to parties to an agreement would provide a certain level of trust between nations. All of the parties would also have a vested interest in correcting problems found within the system architecture.[85] This would decrease system complexity, while maintaining the specific security requirements at each location.

As this system develops, it should aim to include modularity to ensure that if a system is compromised, the entire network is not taken down with it. System administrators should also build in the capability to track changes to the system and return a system to its best-known working state. This capability would serve two functions: it would allow a compromised system to return to working order and, in the event that a system is improperly configured or that new updates reduce network availability, the system can quickly be returned to a functioning state.[86]

Detection and Prevention: Technical Security Controls

In order to create an active cyber defense, you first need to have the ability to detect system vulnerabilities and attacks. In the case of the NNCompanyZ, this would require system administrators and users to realize that all of their systems are vulnerable to attack. These same individuals would also need to understand that vulnerabilities to one part of the system present vulnerabilities to the entire system. As a first step in an open system, a system administrator should catalogue all network equipment that could be exposed to malicious codes (viruses, worms, Trojans, etc.).

Detecting an attack on this system would require systems capable of real-time data collection, as outlined in Article 20 of the Cyber Convention. This requirement addresses the need to gain historical knowledge of attacks and to keep a running total of all the packets that may potentially harm computer infrastructure. Collecting data of this nature helps to detect ongoing attacks and is the only way to protect against live-network attacks. As part of a real-time data collection system, each physical location within a network actively monitors whether its systems are under attack—by either sophisticated or unsophisticated attackers.

One common way to identify problems within large, robust networks is through the use of Intrusion Detection Systems (IDS). IDS can be designed to flag key events based on a specific set of defined rules (signatures) or through anomaly-based detection.[87] A signature-based

[84] Michael Wolfe, "See Past Self-Proclaimed Experts' Open-Source Security Evaluation," letter to the editor in *Communications of the ACM*, vol. 50, no.5 (May 2007), p. 7.
[85] Hoepman and Jacobs, "Increased Security Through Open Source."
[86] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems," a special publication of the National Institute of Standards & Technology, 800-30, July 2002.
[87] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology, SP800-94, February 2007.

detection system compares network activity to previously identified threats, while anomaly-based detection creates defined traffic lanes for network data and flags traffic that veers outside of these bounds. With either system, statistical, characteristic, behavioral, protocol, or traffic information signatures determine which information is collected.[88] If something unusual occurs, an IDS typically collects data on the computers that generated the event: the source IP addresses; the source port; the time of communication; the destination IP address; the protocol used to communicate; and the destination port.[89]

The Department of Homeland Security's EINSTEIN Passive IDS System is the type of shared monitoring platform that could be implemented as part of an international agreement. EINSTEIN scans network traffic for malicious codes and activity using either pre-defined signatures or, in the absence of a pre-defined signature, abnormal traffic.[90] This type of monitoring is called passive monitoring, as it does not seek to block or respond to anomalous network traffic.[91] This is an important distinction, as other types of security scanning, such as port scanning, are likely to be viewed as unacceptable to most control systems, because of their potential to slow down systems and make them unavailable.[92]

This reliance on passive monitoring reflects system administrators' prioritization of network availability over the potential compromise of network security. Indeed, most critical systems cannot be taken off-line for security procedures or maintenance; both functions must occur on live systems/networks. To improve security and not impact availability, smarter solutions are needed. Were the United States, China, and Russia to develop a shared detection monitoring platform it would increase transparency by providing attack information to all parties simultaneously (mechanisms for sharing this security information will be discussed later on in the paper).

Another benefit of having a robust and well-reviewed audit and security logging system at each network facility is that it would provide additional information about who is trying to access the system, both internally and externally.[93] A shared detection system would need to have access to the same logs and data to determine the effectiveness of security at each individual critical node and to address weak links in the security infrastructure chain.

In addition to subscribing to the principles of an international agreement, nations could work with information technology security firms to further develop virus detection and eradication

[88] Ibid.
[89] Ibid.
[90] Simon Parkin, Aad Van Moorsel, and Robert Coles, "An Information Security Ontology Incorporating Human-Behavioral Implications," Proceedings of the 2nd International Conference on Security of Information and Networks, 2009.
[91] Ibid.
[92] Weiss, "Control Systems Cyber Security."
[93] McClure, Scambra, and Kurtz, *Hacking Exposed.*

technologies based on international standards for each industry. This would help to ensure that personal computers and workstations do not serve as platforms for attacks to control systems. This effort would require system software to be kept up to date with publicly released security patches. Information from joint logs would serve as a mechanism for developing new signatures for IDS systems and building better anti-virus products.

The next stage of setting up a strong cyber defense is to attempt to ensure that only authorized users have access to systems. This is typically done through authentication and is a key function of prevention. Critical industries and security experts should focus on jointly developing authentication mechanisms that incorporate the use of passwords, smart cards, digital certificates, Kerberoses, and other authentication methods. While authentication technology should be incorporated at all critical nodes, the type of authentication used is likely to differ from industry to industry. Each node's site administrator would likely determine who can access files remotely based on group associations. New forms of access controls at the software and hardware levels should also be developed, as should non-repudiation controls, which store information about users for future identification, either through shared cryptographic keys or other standards. Each industry should adopt a special form of protected communication channels via VPNs, IPSEC, cryptographic protocols, etc. to minimize the threats of replay and packet sniffing/eavesdropping.

Certain keys will undoubtedly have to be shared with governments for law enforcement purposes, prompting privacy concerns. To address these concerns and the potential for non-repudiation to store user data, these new systems should include technological mechanisms to hide internal system transitions. This will also limit the threat of social engineering.

Detection and Prevention: Management Controls

The new international organization would have to be more active than the international sharing and analysis centers (ISACs) currently in use.[94] In addition to managing international networking operating centers (iNOCs), the organization would be responsible for ensuring that threat information is shared among participating nations and that training and staffing requirements at the iNOCs are met.

The structure and location of each iNOC will also be crucial. Each participating nation should host a center, and each primary iNOC should have an integrated staff, with representatives from each signatory nation, to increase transparency. A particular center's information technology staff should be put through standardized training before being handed responsibility for monitoring network security for a particular area of critical infrastructure. Ideally, the centers

[94] Esther Gal-Or and Anindya Ghose, "The Economics Incentives for Sharing Security Information," *Information Systems Research*, vol. 16, no. 2 (2005), pp. 186-208.

will operate around the clock and take into account global time zones. This will help to develop a liability regime and lead to the delegation of responsibilities for managing systems.

In developing security plans for their assigned industries, each iNOC should develop a thorough understanding of the type of network infrastructure that they are trying to protect. These plans should take the shape of formally agreed upon plans of action. To mitigate the risk of internal threats from iNOC employees, the backgrounds of staff given access to vulnerable critical systems should be thoroughly checked and standard personnel security controls, such as a separation of duties, access registration, and termination procedures for removing compromised individuals, should be implemented. One way to build trust between participating nations would be for iNOC staff to rotate their duties on a regular basis so that no single individual ever has full control of a system.

As personnel transfer from one set of duties to the next, each iNOC would be responsible for structuring and enforcing training requirements and periodic refresher courses. The requirements should be simple: employees must understand why they are doing what they are doing.[95] Users should be aware of safe e-mail handling policies and why they should not install any unnecessary software or software that has been deemed unsafe due to known problems.[96] They should be instructed to avoid clicking on links in e-mail messages, especially in unsolicited e-mails. Also, whenever possible, file-sharing networks should be discouraged. Educating users will reduce dangerous incentives and motivate users to protect their systems.

The network of iNOCS would ostensibly submit to periodic system audits by an international governing body of information technology professionals.[97] The survivability of the whole critical system were one part attacked should be part of any audit. This will test site staff in the face of an attack and promote survivability systems. While such a program may create challenges for the hacker community, it may also discourage state-sponsored activities (professional hackers).

Deterrence through Domestic Policies

The final piece of an effective cyber defense is the most difficult to attain. An effective system needs to tilt the cost-benefit risk calculation of conducting a cyber attack in a way that discourages attacks. Doing this lies outside the control of any system administrator no matter how good he or she is. Another way of understanding this challenge is to acknowledge that no international agreement will suffice as long as participating nations have weak domestic rules and laws. To ensure that individual nations are encouraged to develop stringent domestic laws

[95] Stoll, “E-Learning Promotes Information Security.”
[96] Parkin, Moorsel, and Coles, “An Information Security Ontology.”
[97] R. A. Williams, D. L. Colwell, and C. F. Sanders, “Lessons Learned in Preparing for IAEA Inspections,” Proceedings of the INMM 28th Annual Meeting (1987), pp. 142-143.

and rules, security representatives to the new international organization should have the ability to directly communicate with domestic leadership.

Developing strong domestic laws that criminalize cyber attacks would further bolster and legitimize the international régime. For example, the Council of Europe's Convention on Cybercrime contains several articles that address domestic policy issues. Articles 4 and 5 address the issues of data and system interference and how nation states should deal with them. These articles stress the need for nations to assume some sort of liability for actors who act within their borders to commit attacks. By not domestically criminalizing cyber attacks, a nation would risk becoming a haven for criminals and bases of operations for other nations to conduct attacks. (An apt analogy would be Al-Qaeda's ability to train, plan, and conduct operations in sovereign Afghanistan.) Additionally, these articles define cyber attack as the damaging, deletion, deterioration, alteration, illegal transmission, or the suppression of computer data and systems.

The Convention on Cybercrime's focus on addressing the "misuse of devices" and providing for substantial search and seizures mechanism (Articles 6 and 19) should also be emulated in any international agreement. Information acquired through iNOC search and seizure operations would serve as the foundation for investigations into the geographical origins of attacks. The parties to the agreement could then assign financial penalties to the nations where an attack originated, assuming it is possible to identify its origins. Doing this would shift liabilities and financial obligations for an attack from the attacked site to the attack's point of origin. At the very least, this type of financial penalty could motivate nations to develop stiffer domestic cyber laws, limiting potential attackers' abilities to freely gain information and tools, and to focus on prosecuting major criminal masterminds instead of more middling "script kiddies."

The Possible Effects of an International Agreement on the Attack Scenario

Were the proposed international agreement in place, the attacker(s) targeting the NNCompanyZ would have faced several new challenges to successfully complete their cyber campaign, provided that state X and state Y were members of the agreement. The attack scenario's first assumption would remain intact, as nations are likely to continue to employ sophisticated *hackers* capable of both completing (blackhats) and defending (whitehats) against cyber attacks regardless of international agreements. The second assumption (that the attackers have been given authority/freedom to act on behalf of state X in a cyber campaign against state Y) and third (that the scope of the attack has been outlined, i.e. the outcome of the attack should enable the attacking state X to achieve some type of strategic or tactical advantage over the attacked state Y) would now change because a disruption at the NNCompanyZ and the electric sub-station would now affect both state X and state Y. Provided that both state X and state Y have generated strong domestic legislation aimed at those planning and executing cyber attacks, the number of compromised systems should be much smaller than in the previous scenario.

Under this new scenario, we also assume that the attackers have identified a single NERC facility as their initial target, but because of the new international arrangements, to be successful they will need to be familiar with the specific protocols and equipment surrounding this specific facility, to include firewalls, IDS, security policy, computer network architecture, authentication mechanisms, etc. Newly developed authentication mechanisms would also restrict attackers ability to freely move from one system to the next without direct physical access and access to severely restricted credentials. Another roadblock would be new access standards that restrict employees to performing work procedures on specific equipment deemed critical, equipment whose access to the Internet is severed.

Were state Q to target NNCompanyZ, and state Q was not a signatory to the agreement, a slightly different chain of events would occur. The first, second, and third assumptions would remain as they were in the initial attack scenario. In this scenario, however, defensive activities would not commence until the attack began. Information technology administrators associated with NNCompanyZ would begin mitigation and prevention once the attack was detected. Because all of the iNOCs would have a unified attack notification system, administrators at companies associated with NNCompanyZ would begin locking down their systems as if the attack would soon come to them. Solutions (mitigation) to the attack would then be coordinated among all the iNOCs instead of the local NNCompanZ iNOC. A parallel effort to identify the attacker would be coordinated among all iNOCs extending beyond the centers responsible for critical energy infrastructure. If an iNOC were able trace the origin of the attack to state A, a signatory to an agreement against State-to-State Cyber Attacks, state A, on behalf of state Y, would begin a criminal investigation. State A would be able to use all of the collected data associated with the attack because it is a signatory to the treaty, which would allow it to identify the attackers. It would be difficult to identify State Q as the instigator of the attack, but if it is, economic sanctions or a retaliatory strike could be legitimate options.

Conclusion

The capabilities of information technology continue to advance by leaps and bounds, and the use of the technologies continues to proliferate to more and more facets of modern society. The information technology architecture designed specifically for key critical infrastructure systems is likely to continue to be vulnerable unless nations instill a shared sense of vulnerability and protection. Expanding on agreements such as the Council of Europe’s 2001 Convention on Cybercrime and focusing on ways for nations such as Russia and China to cooperate with the United States and Europe are key to ensuring the effective protection of critical infrastructure. And to accomplish these goals, nation-states will have to begin seeing critical infrastructure nodes as common resources. Additionally, nations will have to develop strong domestic laws and policies to combat and punish malicious cyber attackers within their borders to support effective international governance. The role of network security will need to go hand in hand with the development of new networked infrastructure.

About the Author

Jamal Henry was an information technology technician in the U.S. Air Force Reserve for 8 years. He received an M.S. in international affairs from Georgia Institute of Technology and an M.S. in computer science from Johns Hopkins University. His B.S. is in computer science from the University of Southern Mississippi. The views expressed in this paper are the author's alone and do not represent the views of U.S. Air Force reserve or the Department of Defense.

Glossary

Backdoor – This feature allows unauthorized access to system functionality after an initial system compromise (see Rootkits).

Botnets **–** Commonly referred to as a network of Bots (derived from robot), botnets are computer systems that have been implanted with software that allows them to be remotely controlled by a central administration point. Botnets are a combination of computer shell scripts and backdoors that are placed on a machine after it has been exploited via another type of malware.

CIA **–** An abbreviation for Confidentiality, Integrity, and Availability.

Flaw **–** Errors that occur within information technology systems.

Hacker – An individual that gains access to computer systems by exploiting system security vulnerabilities.

Intrusion Detection System – A tool that can be used to identify problems within large, robust networks by flagging key events based on a specific set of defined rules (signatures) or through anomaly-based detection.

Kerberos – A network authentication protocol that was developed at MIT.

Malicious Code – A type of program or code specifically designed to cause harm to an information technology system.

Open Source System **–** A type of system where the system design is freely available to the general public for additional development and testing. These systems are based on widely supported and consensus-based standards that are often subject to peer review.

Packet Sniffing – A process equivalent to phone/wire tapping in which all packets involved in a client/server data exchange are captured sequentially for later inspection.

Port Scanning – A technique used to scan a computer system's ports to understand which are available for use and to define the computer's operating system.

Replay Attack – A network attack in which a valid data transmission is fraudulently and/or maliciously retransmitted to determine the origin, destination, and purpose of the valid transmission.

Signatures **–** A characteristic of email traffic that is generated based on known malicious network traffic.

System Hardening – A security measure that reduces the number of potential security risks to a system by removing non-essential software programs and utilities.

Rootkit – Software that provides outside access to a computer system while remaining hidden from the system's administrators.

Telnet **-** A program that allows users to remotely connect to a computer. The default telnet port is 23.

Trojan Horse – A transport vehicle for a worm or virus that disguises itself as a legitimate program. Once a Trojan horse is executed, the virus or worm can be executed.

Virus – A type of malicious code that can attach itself to system resources and harm legitimate system programs by corrupting, deleting, or moving important data sectors.

Vulnerability – The security weakness of the system.

Worm – Similar to virus, this malicious code consumes system resources while replicating itself and spreading, but it does not remove files.

Author Bio - TK