The Threat of Cyberterrorism to Critical Infrastructure

https://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/

SAM POWERS, SEP 2 2013

> *The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time…attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor.*
>
> -Leon Panetta **[1]**

Introduction

In early March of this year, DNI James Clapper and FBI Director Robert Mueller made clear in a hearing before the Senate Select Committee on Intelligence that "cyber threats" represent one of the most challenging dangers to US national security.[2] This paper will build upon the plethora of available research to unpack how the possibility of a catastrophic cyber attack or a "cyber Pearl Harbor" has become part of the zeitgeist of 21st century discussion on security and terrorism. This research will focus on a specific cyber threat, that of cyber terrorism, and attempt to prove that out of all of the threats falling under the cyber umbrella, acts that may be carried out to cause terror and loss of life through damage to critical infrastructure,[3] present the largest danger. The report will argue that terrorist organizations and "lone wolf" actors, regardless of historical precedent or their current capacity, represent the greatest threat to security, rather than states such as China and Russia.

We will begin by attempting to define cyberterrorism and show how the lack of a common definition has made the formation of effective policy difficult. The research will then explore the various vulnerabilities of critical infrastructure, particularly in the US and in other countries that rely heavily on supervisory control and data acquisition (SCADA) systems to monitor and regulate industrial operations. We will examine how terrorist groups may acquire the capabilities to conduct large scales acts of cyber terrorism against critical infrastructure, show how they would orchestrate such and attack, and explore who has been and will continue to be most susceptible.

Clearly we have yet to see a doomsday scenario like that mentioned by former US Defense Secretary Leon Panetta unfold. However, the intent to commit such attacks is not hidden from sight, with groups like al-Qaeda calling on their supporters worldwide to fight "electronic jihad" against the west.[4] Many small-scale cyber attacks are being carried out every day, and larger attacks such as the now infamous Stuxnet worm show just how vulnerable critical infrastructure, in particular, is to intrusion. This paper will argue that more needs to be done by governments, the private sector, and civil society to prevent cyber attacks from crippling infrastructure and degrading states capacity to continue their normal operations. The paper will conclude by offering recommendations to nascent institutions and systems, both public and private, to prevent groups with nefarious intentions from inflicting harm and suffering on a currently unseen scale.

What is Cyber Terrorism and How is It Different From Other Cyber Threats?

A 2009 article from the Harvard Law Record titled, "What is Cyberterrorism? Even Experts Can't Agree," echoes the current frustration of many academics, politicians, and security professionals that a clear and unanimously accepted definition of the term cannot be agreed upon. Attempts to create a common terminology for cyberterroism in the United States, for example, have thus far been exceedingly difficult, with the FBI alone publishing three distinctly different terminologies and DOD, FEMA, DEA, DHS and DOJ each having their own distinct definitions.[5] Leonard Bailey, a former member of the US National Security Division (NSD), expressed his concern stating "the area suffers from a limited lexicon…we even lack a unified definition of cyber terrorism and that makes discourse on the subject difficult."[6]

Although the need for an across-the-board definition will arise later in the recommendation section of the paper, it is key to understand why the issue of cyberterrorism has thus far been hard to explain. The various complexities and unknowns of cyber threats, and their relationship to acts that constitute terrorism make defining the term very difficult. What constitutes a cyber threat? When does a cyber attack become an act of terrorism rather than just a crime? These are all questions that continue to make it difficult for practitioners to navigate said threats and put policy into action to protect national security. This section will show how the term has evolved, and how cyberterror is distinctly different from other cyber threats.

The term cyberterrorism was originally coined in the 1980's by Senior Researcher at the Center for Strategic and International Studies (CSIS) Barry Collin as "the international abuse of a digital information system, network, or component toward an end that supports or facilitates a terrorist campaign or action." Since that time, various scholars, government officials, and security experts have worked to refine Collins broad Postgraduate School defines the term as such:

Cyberterrorism is generally understood to refer to highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act.[7]

Marie-Helen Maras, a professor of criminal justice at SUNY–Farmingdale elaborates even further on this terminology adding ,"Cyberterroists seek to attack critical infrastructure systems (e.g., water, energy, communications) so as to intimidate or coerce a government for ideological, religious, or political reasons." In an earlier excerpt from her book *Computer Forensics: Cybercriminals, Laws and Evidence*, Maras states:

A cybertrerrorist may hack into U.S. critical infrastructure in an attempt to cause grave harm such as loss of life or significant economic damage. Such attacks are aimed at wreaking havoc on information technology systems that are an integral part of public safety, traffic control, medical and emergency services, and public works.[8]

In this excerpt, Maras touches on very important themes that will be discussed later including the vulnerability of critical infrastructure and methods that an individual or group may employ to conduct acts of terrorism. As Maras mentions, it is important to note that not all acts that a terrorist organization may be involved in via the Internet, nor all cyber attacks writ large, constitute acts of cyberterrorism. Maura Conway at Dublin City University describes how an act of cyberterrorism must "instill terror as commonly understood (that is, result in death or large scale destruction), and they must have a political motivation."[9] Terrorist organizations of all colors have been utilizing the Internet for various means including fundraising, planning, and recruitment since its explosive growth in the 1990's.[10]

However, these attacks do not constitute terrorism per se as they do not directly cause large-scale death or destruction in and of themselves. As Maras explains, terrorist groups including the Liberation Tigers of Tamil Eelam (Tamil Tigers) have been responsible for conducting acts that temporarily paralyze government websites through large scale Denial of Service Attacks (DoS), but as these attacks did not cause grave and sustained harm nor loss of life, such attacks cannot be considered cyberterrorism. Thankfully, a catastrophic attack on critical infrastructure like that portrayed by Mr. Panetta and others has yet to occur. However, as the following section will show, terrorist organizations and "lone wolves" have expressed interest in conducting such attacks and have demonstrated their proficiency on a smaller scale at quite an alarming level. If left unprotected, the critical infrastructure of nations may face an attack at a much larger scale, resulting in mass casualties and degradation of vital systems that are necessary to maintain national security. The next section will highlight what vulnerabilities exist and show how a hypothetical large-scale cyberterrorist attack may unfold.

The Threat to Critical Infrastructure: How Vulnerable are We to Cyberterrorism?

A couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage.

-Fmr. Deputy Defense Secretary William Lynn**[11]**

In 2007, the turbine of an electricity generator burst into smoke in the Idaho National Laboratory, ultimately causing failure of the device. Leaked to the press shortly thereafter, this incident dubbed the "Aurora Generator Test" was conducted by DHS to show just how vulnerable American critical infrastructure is to a cyber attack. In short, engineers found that by changing the operating cycle of a power generator remotely via computer, the turbines could set fire, eventually destroying the machine.[12] By no means the first test of its kind, various scenarios have been explored by international governments to assess the vulnerabilities of critical infrastructure. However, as shown in a 2011 project conducted by global security software giant McAfee, in conjunction with CSIS, little has been done to address the large gaps in preventing such an attack from taking place.[13] A 2013 assessment by the GAO showed that improvements have been made, but not nearly at the level necessary to safeguard critical infrastructure from cyber attack.[14] This section will address the question of what vulnerabilities exist to critical infrastructure.

The Aurora Generator Test is one of the prime examples of simulations carried out to assess the vulnerabilities of Industrial Control Systems (ICS) that are used to "monitor and regulate" the majority of industrial operations (e.g., the electrical grid, water treatment, transportation). In particular, the test focused on a type of ICS called industrial Supervisory Control and Data Acquisition Systems (SCADA). In a 2003 CRS report, Dana A. Shea helps explain the role of SCADA systems and shows how they are vulnerable to attack:

"Industrial control system technologies are often employed in critical infrastructure industries to allow a single control center to manage multiple sites. Industrial control systems were originally implemented as isolated, separate networks. They were viewed as secure systems, which protected remote locations from being physically broken into and mistreated. Control systems were originally designed to be free standing networks without Internet access. Therefore, it has been necessary to add network access systems to the original systems to integrate them into the corporate structure. This has created, in the worst cases, a labyrinth of connections, which is perhaps not rigorously constructed for cyber- security or well documented.

Unfortunately, since this report was presented to Congress in 2003, progress has been slow to put security mechanisms in place to protect SCADA and other ICS that control critical infrastructure.[15] Although the Aurora Test and subsequent incidents such as the introduction of Stuxnet malware in 2010 have raised suspicion, companies and government have only lightly, thus far, embraced security mechanisms.[16] For example, rather than replacing or reforming the archaic SCADA ICS, governments and corporations have altered the system to allow for increased operational efficiency at the cost of jeopardized security.[17] The continual need for more rapid information sharing and real-time data spurred developers to step into a world that was previously closed off from the knowledge of a general computer programmer. For example, firms introduced standard computers and operating systems as well as IP based networking to allow for better control and interconnectivity so that businesses and government could run more efficiently.[18]

These "developments," however, have come at a cost, with the GAO reporting 48,562 attacks on federal agencies alone in FY 2012 alone.[19] Although none of these attacks have crippled infrastructure and caused terror through physical damage and loss of life, the possibility of such an attack is not without reason. As companies and governments begin to further embrace the Smart Grid System for example, critical infrastructure (primarily the electric grid) will become more reliant on a vast array of nodes that give IT systems more efficient control over the delivery of services but will undoubtedly open up further opportunities for intrusion from nefarious actors.[20]

At this juncture it must be made clear that the majority of research for this paper has pointed towards state actors as being the most responsible in executing the majority of cyber attacks. According to many experts, for example, the notion of cyberwar with China is not an unreal perspective.[21] Recent criticism has come from the west towards China, blaming the country for conducting cyber espionage against the US and other international targets, stealing valuable technological secrets and financial information.[22] These recent events have polarized the sino-US relationship with leaders on both sides calling for increased responsibility and an end to malicious actions.

Although the threat of a looming cyberwar with China and other nations should not be discredited, this paper will continue by looking at the threat of cyberterrorism stemming from primarily non-state actors and states that directly support terrorism such as Iran. Particular emphasis will be put on the role of Iran, as groups like the Izz ad-Din al-Qassam brigades who receive direct material support form the Islamic Republic have already carried out cyber attacks.[23] The following section will analyze the various methods by which cyberspace *could* be used directly by a terrorist organization to achieve their goals of political or ideological change through attacks that cause terror and loss of life. In addition, we will look at particular reasons as to why terrorist groups and "lone wolf" actors pose more of a threat to transnational security than states such as China, even if they are less equipped.

Current and Future Capabilities of Cyberterrorists

Last night, the FBI received a signed threat from a very credible, well-funded, North Africa-based terrorist group indicating that they intend to disrupt water operations in 28 US cities. Because the threat comes from a credible, well known source, with an organizational structure capable of carrying out such a threat, the FBI has asked utilities, particularly large drinking water systems, to take precautions and to be on the lookout for anyone or anything out of the ordinary.**[24]**

-Association of Metropolitan Water Authorities, 2001

In the summer of 2012, a video from al-Qaeda's as-Sahab media outlet calling for an "electronic Jihad," was released to the FBI. The chilling video showed an unnamed al-Qaeda operative directing "covert mujahidin" to launch waves of cyber attacks against US networks including critical infrastructure such as the power grid and water supplies.[25] This section will attempt to address the question as to what effect terrorist organizations and "lone wolfs" can have against critical infrastructure and also how could such a major cyber attack play out in the future in real time.

Terrorist organizations have demonstrated their expertize on the web in various forms for over a decade. As the recent attacks by the Tsarnaev brothers in Boston highlights, video broadcasts over social media, for example, serve as one of the many ways by which terrorist groups can recruit members and spur "lone wolf" actors to commit terrible atrocities.[26] While dissemination of propaganda and other such activity is malicious and may eventually lead to an act of terrorism taking place, acts such as small scale hacking for financial gain, temporarily paralyzing non critical websites and spreading of propaganda, do not constitute cyberterrorism.[27] What is worrisome, however, is that over the past 10 years in particular, trends have emerged that illustrate that al-Qaeda and other terrorists have taken an interest in directing their cyber capabilities towards directly hitting US infrastructure and causing mass damage. We have also learned, and have seen from example, that attacks can be orchestrated without massive funding, by single actors, who are not even affiliated with a terrorist group.[28]

In her book *Computer Forensics: Cybercriminals, Laws and Evidence,* Marie-Helen Maras provides various examples of such instances where "lone wolves" were able to break into SCADA systems, and if they so desired, could have created massive damage. For example, in 2000, a Russian man hacked into an ICS that ran a natural gas pipeline and was able to control the flow of LNG. "Hypothetically, this hacker could have easily increased the gas pressure until the valves broke, causing an explosion to occur."[29] Although many of these actors have been "lone wolves," terrorist organizations have not sat on the sidelines idly. Rather, since the new millennium, terrorist groups such as al-Qaeda, and groups supported by Iran like Hamas and Hezbollah, have been actively working towards developing a capacity to strike at the heart of the industrialized world's critical infrastructure to cause terror and havoc. [30] Former Presidential Adviser for Cyberspace Security, Richard Clarke expresses his concern on the terrorist entrée into the world of cyberwar in a PBS Frontline special. Clarke comments:

We also found indications that members of al-Qaeda were from outside of the Unites States doing reconnaissance in the United States on our critical infrastructure. Where were railroad crossings? Where were the big natural gas depositories? Where were the bridges over rivers that also carried the fiber for the backbone on the Internet? It's possible now to do that kind of targeting, which would have, in the past, required lots of people and running around the country. It is possible to sit in the cyber café in Peshawar and do that kind of reconnaissance.

The sentiment of Clarke and others is quite telling in the sense that it not only drives home the al-Qaeda and other terrorists seek the desire to destroy US infrastructure, but that they are slowly gaining the capacity to carry out such attacks. Al-Qaeda members have been tracked seeking information on SCADA systems in the US including wastewater and water supply facilities. In 2005, the al-Farouq web forum exposed a "hacker library" with information that could aid an individual in debilitating and an electric system with a keystroke.[31] In addition, in 2003 an al-Qaeda affiliate built upon an emerging trend in the US and developed an online university for "Jihad Sciences on the Internet," to instruct students on proper ways to fight electronic Jihad.[32] This sustained desire to wreak havoc on the infrastructure of western nations has thankfully yet to play out. The sophistication to carry out such a large-scale attack is hard to develop and requires substantial funding. There are, however, nation states that are willing to support such ambitions.

Iran's Role in Cyberterrorism and Possibilities for Future Attack

What I worry about is that terrorists and nations that sponsor terror, such as Iran, that demonstrate cyberattack capabilities will be far more reckless than traditional adversaries.**[33]**

-Art Coviello, CEO of security firm RSA

The asymmetric nature of the war against terrorists can be said to transcend into the cyber realm. While al-Qaeda and other groups have been able to coordinate physical attacks with modest finances, a massive cyber operation that could debilitate US critical infrastructure would require funding and advanced technical expertise. The Islamic Republic of Iran has been known historically to fund terrorists of various stripes who oppose western interests.[34] Even amidst an array of international sanctions, the nation still has the monetary prowess to fund one of worlds the largest military operations in which cyber strategy is a critical component. While nations like Russia and China are guilty of cyber intrusion into the institutions and systems of the United States and its allies, the majority of their operations are carried out for the sake of espionage.[35] Also, while the US and much of the West hold normal diplomatic ties with China and the Russian Federation, the same cannot be said about Iran.

Iran has subscribed, for the most part, to a retaliatory cyber strategy against the west. The Shamoon attack in 2012 that knocked out three-quarters of the Saudi State oil firm, Aramco, and filled screens with an image of a burning US flag was traced to Iran. The regime has consistently supplied the military arm of Hamas with information and technology to carry out attacks on US financial institutions and is currently doing the same for Bashar al-Assad in Syria. These events raise important red flags on what the future may hold for terrorists groups looking to commit large-scale attacks against the United States. Not only is the transfer of information from Iran to such entities a common practice, but also powerful viruses such as Stuxnet are now readily available on the Internet, and a black market has emerged alongside offering to the highest bidder.[36]

As the leadership of terrorists groups become younger and more tech-savvy, it is the fear that such groups will rely more heavily on a cyberterror component to achieve their ultimate goal of creating terror through destruction and death. While states like China may have the capability to carry out such acts, diplomatic and financial ties make such an occurrence unlikely. The strategic aims of the terrorist, particularly al-Qaeda and its affiliates, show that if such technology were obtained, its use would be quite certain and could be supplemented alongside a physical attack, described by secretary Panetta as a "cyber Pearl Harbor."

Putting the Pieces Together: What Can Governments, The Private Sector, and Civil Society Do To Prevent Acts of Cyberterror

Today, more than ever before, the world is united through the use of technology. From the systems that connect us to friends and family, to the rails and roads that bring us together, and the generators that power our homes, the security provided by era of previous isolation can no longer be seen as relevant. With the advent of the Internet and ICS systems developed to make industrial operations, commerce, and life in general easier, we have ushered in a new era of unprecedented insecurity. A clear example of this is shown in the number of cyber attacks currently facing the United States.

Between 2006-2012, the number of attacks increased by 782 percent, reaching 48,562 attacks in FY 2012. This paper set out by reflecting briefly on the scenario of a "cyber Pearl Harbor," or surprise cyber attack that would be so devastating to the nations critical infrastructure, that the carnage could surpass that of 9/11. Although such an attack has yet to materialize, I have argued that out of the many cyber threats facing the industrialized world, actions taken by a terrorist organization or a "lone wolf," targeting critical infrastructure would prove to not only be the most catastrophic possibility, but also the most likely future event.

As the report explained, the capacity of NSA and state-sponsored terrorists have increased drastically over the years, while the goal of wreaking havoc and death to change politics and ideology have remained solid. As generations of terrorists get younger, and more adept with technology, an unforeseen cyber attack, possibly in conjunction with a physical attack may present it self. The following section will offer suggestions to various government agencies, the private sector and civil society on how to prevent such an attack from taking place in the future.

Recommendation 1: Provide an Overarching Cyber Strategy, Develop Clear Cut Roles for Government Agencies, and Hold Private Industry Accountable

This recommendation reflects in part on the recent assessment by the GAO that concluded that current US government cyber strategy was to diffuse and not clearly defined.[37] Currently, an overarching American central cyber strategy does not exist, and even the White House National Cyber Strategy contains documents piled from over a decade, with multiple layers that make priorities hard understand. The US and other governments in the same boat (the UK and Spain to name a few) must develop concise documents that designate specific roles to agencies, allow for information sharing, and set benchmarks and methods to track progress and establish best practice. In addition, the government must hold the private sector accountable for ensuring high standards of cyber security, particularly in regards to critical infrastructure.

As a 2011 report by McAfee and CSIS illustrates, in the US, UK and Spain for example, less than 20% of companies received a government audit to assess their capacity to prevent a cyber attack.[38] In addition, 32 percent of companies had yet to design any sort of cyber strategy to deal with emerging technologies such as the Smart Grid. As these systems are critical to maintaining and regulating the nation's critical infrastructure, and an attack could jeopardize national security, it is the responsibility of the government to ensure that businesses cooperate. Such measures are already put in place in both China and Japan with high levels of interaction between business and government on various levels to guarantee operational security. The United States and its allies should learn from such approaches and hold businesses accountable in order to protect the nation from the threat of cyberterrorism.

Recommendation 2: Governments Must Engage Civil Society as Stakeholders in Increasing Cyber Resilience

Currently, populations worldwide remain untrusting of their government's ability to handle a cyber attack. While 56 percent of Chinese feel confident in the communists party's ability to thwart an attack, these numbers remain much lower for the US and Europe.[39] While initiatives such as Cyber Security Awareness Month in the US represent a good first step, more needs to be done to create a civic culture that treats cyber security as a priority.

The attacks on 9/11 left a permanent scar on the communities affected and crafted a cultural resilience against future attack. Commercials and billboards asking citizens to report suspicious activity or to "see something, say something," are ubiquitous in New York City and have proven quite effective. Between the years of 1999-2009, of the 68 terrorist plots, aware citizens thwarted 40 percent thanks to tip offs.[40] DHS has created an incident response and cyber education campaign titled *Stop. Think. Connect,* to inform citizens of the many threats present and encourage action to secure cyber space. More initiatives like this should be created and well funded. Governments should disseminate such initiatives via social media, traditional canvasing, and through radio and television and begin joint programs with public education to begin stressing the importance of cyber security at an early age.

Recommendation 3: Establish International Norms for Governance on the Web and Crackdown on International Black Market

No one entity, government body, or international organization, can or should have complete control over the Internet. However, in order to prevent malicious actors such as terrorists from disseminating information, recruiting, funding, and executing cyber attacks, more could be done on behalf of the international community. For example, in 2012, the International Telecommunication Union (ITU), an arm of the United Nations, convened in Dubai to discuss ways to revise a treaty known as the International Telecommunications Regulations (ITR) in order to open a space for discussion on how to best secure cyberspace.[41] While some of the delegates, including the US ambassador, expressed reservations, believing that such a treaty could allow for government suppression of civil liberties in cyberspace, this discussion is a necessary first step in preventing future cyber attack.

The UN has put into place various universal instruments to battle international terrorism including an overarching plan to battle global terrorism. However, amendments should be added to incorporate the role of the internet in such strategy. Ratified on October 13, 2010, GA resolution A/RES/62/272 fails to mention the role the Internet as part of the terrorist arsenal.[42] Although working groups on the topic have since been convened, clear legislation needs to be put in place, especially considering the role of state actors such as Iran in directly funding terrorism and cyber attack across the globe.

Bibliography

AFP. “US Thinks Iran behind Cyber Attack in Saudi: Ex-official.” *The Express Tribune*. N.p., Oct. 2012. Web.

Albanesius, Chloe. “Surprise Vote on Internet Issues Rattles ITU Conference.” *PCMAG*. N.p., 13 Dec. 2012. Web.

“Al Qaeda Video Calls for Electronic Jihad.” *Homeland Security News RSS*. N.p., 22 May 2012. Web

Baranetsky, Victoria. “What Is Cyberterrorism? Even Experts Can’t Agree.” *The Record*. N.p., 5 Nov. 2009. Web. <http://hlrecord.org/?p=12752>.

Blumenthal, Daniel. “How to Win a Cyberwar with China.” *Foreign Policy*. N.p., 28 Feb. 2013. Web.

Carter, Chelsea J. “Official: Cyberattacks, N. Korea, Jihadist Groups Top U.S. Threats.” *CNN*. Cable News Network, 01 Jan. 1970. Web. 25 Apr. 2013.

Cloherty, Jack. “Virtual Terrorism: Al Qaeda Video Calls for ‘Electronic Jihad’” *ABC News*. ABC News Network, 22 May 2012. Web.

Conway, M. (2002), ‘Reality Bytes: Cyberterrorism and Terrorist “Use” of the Internet’, *First Monday* 7(11).

Corbin, Kennith. “Iran Is a More Volatile Cyber Threat to U.S. than China or Russia.” *CIO*. N.p., 21 Mar. 2013. Web.

“The Dark Side of the Smart Grid – Smart Meters (in)Security.” C-4 Security, 4 Feb. 2012. Web.

Goldman, David. “The Real Iranian Threat: Cyberattacks.” *CNNMoney*. Cable News Network, 05 Nov. 2012. Web.

Himma, Kenneth Einar. “A View of Cyberterrorism Five Years Later.” *Internet Security: Hacking, Counterhacking, and Society*. Sudbury, MA: Jones and Bartlett, 2007. 2+. h*ttp://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484928*. 2007. Web.

Lister, Tim. “Dead Boston Bomb Suspect Posted Video of Jihadist, Analysis Shows.” *CNN*. Cable News Network, n.d. Web. 25 Apr. 2013.

McAfee, and CSIS. *In the Dark: Crucial Industries Confront Cyber Attacks*. Issue brief. N.p.: n.p., 2011. Print.

Magnuson, Stew. “Growing Black Market for Cyber-Attack Tools Scares Senior DoD Official – Blog.” *National Defense*. NDIA, n.d. Web. 25 Apr. 2013.

Maras, Marie-Helen. “Cybercrime Laws: Which Statute for Which Crimes.” *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning, 2012. 104-06. Print.

Meserve, Jeanne. “Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid.” *CNN*. Cable News Network, Sept. 2007. Web <http://www.cnn.com/2007/US/09/26/power.at.risk/>.

Panetta, Leon E. “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for NationalSecurity, New York City.” *Defense.gov*. N.p., 11 Oct. 2012. Web.

Porter DeNileon, Gay. “How Real Is the Threat of Terrorist Attack on Domestic Water Supplies in North America.” N.p., 2001. Web.

Rollins, John. *Terrorist Capabilities for Cyberattack: Overview of Policy Issues*. Rep. no. RL33123. N.p.: Congressional Research Service, 2007. Print.

Singer, Peter W. “The Cyber Terror Bogeyman.” *The Brookings Institution*. N.p., Nov. 2012. Web. <http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer>.

Schlachtenhaufen, Mark. “Officials: If You See Something, Say Something » Local News » The Edmond Sun.” *Local News ATOM*. N.p., n.d. Web. 25 Apr. 2013.

United Nations General Assembly. *The United Nations Global Counter-Terrorism Strategy*. Vol. Sixty-fourth Session. N.p.: n.p., 2010. Print. Agenda Item 115.

“U.S. GAO – Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.” N.p., 14 Feb. 2013. Web.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington, D.C.: United States Institute of Peace, 2006. 156. Print.

[1] Panetta, Leon E. “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for NationalSecurity, New York City.” *Defense.gov*. N.p., 11 Oct. 2012. Web.

[2] Carter, Chelsea J. “Official: Cyberattacks, N. Korea, Jihadist Groups Top U.S. Threats.” *CNN*. Cable News Network, 01 Jan. 1970. Web. 25 Apr. 2013.

[3] Critical infrastructure is defined in the USA PATRIOT Act as those “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.”

[4] “Al Qaeda Video Calls for Electronic Jihad.” *Homeland Security News RSS*. N.p., 22 May 2012. Web

[5] Baranetsky, Victoria. “What Is Cyberterrorism? Even Experts Can’t Agree.” *The Record*. N.p., 5 Nov. 2009. Web. <http://hlrecord.org/?p=12752>.

[6] Ibid

[7] Himma, Kenneth Einar. “A View of Cyberterrorism Five Years Later.”*Internet Security: Hacking, Counterhacking, and Society*. Sudbury, MA: Jones and Bartlett, 2007. 2+. h*ttp://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484928*. 2007. Web.

[8] Maras, Marie-Helen. “Cybercrime Laws: Which Statute for Which Crimes.”*Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning, 2012. 104-06. Print.

[9] Conway, M. (2002), ‘Reality Bytes: Cyberterrorism and Terrorist “Use” of the Internet’, *First Monday* 7(11).

[10] Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges* . Washington, D.C.: United States Institute of Peace, 2006. 156. Print.

[11] Singer, Peter W. “The Cyber Terror Bogeyman.” *The Brookings Institution*. N.p., Nov. 2012. Web. <http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer>.

[12] Meserve, Jeanne. “Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid.” *CNN*. Cable News Network, Sept. 2007. Web. <http://www.cnn.com/2007/US/09/26/power.at.risk/>.

[13] McAfee, and CSIS. *In the Dark: Crucial Industries Confront Cyber Attacks*. Issue brief. N.p.: n.p., 2011. Print.

[14] “U.S. GAO – Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.” N.p., 14 Feb. 2013. Web. <http://www.gao.gov/products/GAO-13-187>.

[15] “U.S. GAO – Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.” N.p., 14 Feb. 2013. Web.

[16] McAfee, and CSIS. *In the Dark: Crucial Industries Confront Cyber Attacks*. Issue brief. N.p.: n.p., 2011. Print.

[17] “The Dark Side of the Smart Grid – Smart Meters (in)Security.” C-4 Security, 4 Feb. 2012. Web.

[18] “The Dark Side of the Smart Grid – Smart Meters (in)Security.” C-4 Security, 4 Feb. 2012. Web.

[19] “U.S. GAO – Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.” N.p., 14 Feb. 2013. Web.

[20] “The Dark Side of the Smart Grid – Smart Meters (in)Security.” C-4 Security, 4 Feb. 2012. Web.

[21] Blumenthal, Daniel. “How to Win a Cyberwar with China.” *Foreign Policy*. N.p., 28 Feb. 2013. Web.

[22] ibid

[23] United States. U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. By Ilan Berman. N.p., 20 Mar. 2013. Web.

[24] Porter DeNileon, Gay. “How Real Is the Threat of Terrorist Attack on Domestic Water Supplies in North America.” N.p., 2001. Web.

[25] Cloherty, Jack. “Virtual Terrorism: Al Qaeda Video Calls for ‘Electronic Jihad’” *ABC News*. ABC News Network, 22 May 2012. Web.

[26] Lister, Tim. “Dead Boston Bomb Suspect Posted Video of Jihadist, Analysis Shows.” *CNN*. Cable News

Network, n.d. Web. 25 Apr. 2013.

[27] Maras, Marie-Helen. “Cybercrime Laws: Which Statute for Which Crimes.” *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning, 2012. 104-06. Print.

[28] ibid

[29] Maras, Marie-Helen. “Cybercrime Laws: Which Statute for Which Crimes.” *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning, 2012. 104-06. Print.

[30] Rollins, John. *Terrorist Capabilities for Cyberattack: Overview of Policy Issues*. Rep. no. RL33123. N.p.: Congressional Research Service, 2007. Print.

[31] Himma, Kenneth Einar. “A View of Cyberterrorism Five Years Later.” *Internet Security: Hacking, Counterhacking, and Society*. Sudbury, MA: Jones and Bartlett, 2007. 2+. h*ttp://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484928*. 2007. Web.

[32] ibid

[33] Goldman, David. “The Real Iranian Threat: Cyberattacks.” *CNNMoney*. Cable News Network, 05 Nov. 2012. Web.

[34] ibid

[35] Corbin, Kennith. “Iran Is a More Volatile Cyber Threat to U.S. than China or Russia.” *CIO*. N.p., 21 Mar. 2013. Web.

[36] Magnuson, Stew. “Growing Black Market for Cyber-Attack Tools Scares Senior DoD Official – Blog.”*National Defense*. NDIA, n.d. Web. 25 Apr. 2013.

[37] “U.S. GAO – Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.” N.p., 14 Feb. 2013. Web.

[38] McAfee, and CSIS. *In the Dark: Crucial Industries Confront Cyber Attacks*. Issue brief. N.p.: n.p., 2011. Print.

[39] McAfee, and CSIS. *In the Dark: Crucial Industries Confront Cyber Attacks*. Issue brief. N.p.: n.p., 2011. Print.

[40] Schlachtenhaufen, Mark. “Officials: If You See Something, Say Something » Local News » The Edmond Sun.” *Local News ATOM*. N.p., n.d. Web. 25 Apr. 2013.

[41] Albanesius, Chloe. “Surprise Vote on Internet Issues Rattles ITU Conference.” *PCMAG*. N.p., 13 Dec. 2012. Web.

[42]United Nations General Assembly. *The United Nations Global Counter-Terrorism Strategy*. Vol. Sixty-fourth Session. N.p.: n.p., 2010. Print. Agenda Item 115.

—

Written by: Sam Powers
Written at: New York University
Written for: Center for Global Affairs
Date written: May 2013