Nikhil Garg
TC 357 – Inman
Final Research Paper

American Cyber-security Policy in the 21st Century

The digital revolution of the last two decades has increased the quality of life of Americans, making information more available and further connecting the world. However, as communication technology has developed, security in cyber-space has been unable to keep up. In the last five years, cyber-security has been recognized as one of the biggest issues in defense facing the United States, and much ink, political capital, and money has been spilt in trying to address the situation. 'Cyber-security' encompasses numerous questions, many of which require wholly unique solutions. A large subset of the cyber problem deals with 'on the ground' issues related to military operations, such as attacks on operational communications or hardware (such as drones). Such issues will not be addressed, as they are military tactical concerns with in-house military solutions. In this paper, I focus on the foreign policy issues surrounding the cyber threat to United States infrastructure, government systems, and military technologies. I recommend that the United States:

1) Continue developing and investing in robust cyber-security technology
2) Regulate cyber-security practices at companies that own and operate critical infrastructure
3) Mandate cyber-security practices and hold accountable military contractors who allow U.S. military contracted designs and technologies to be stolen
4) Pursue an international structure and norms against the use of cyber-attacks and thefts during peacetime

    a. In pursuit of such a norm, clarify its own doctrine on the use of aggression in the cyber domain during peacetime

5) Cooperate with other countries in finding and prosecuting non-state actors who are conducting cyber-attacks, such as Anonymous

Critical United States infrastructure includes electricity grids, traffic signals and roads, nuclear plants, and dams. A large cyber-attack on an electricity grid could cause massive power outages throughout the country, or an attack on a nuclear plant could cause a meltdown. Such an attack is possible because most critical systems – bridges, power plants, the electric grid, for example – are at least partially managed by control systems which monitor, regulate, and directly change various aspects of the system. An attack is no longer farfetched or theoretical. In 2008, the CIA revealed that it knows of at least one instance in which a cyber-attack through the internet "disrupt[ed] power equipment … and caused a power outage affecting multiple cities" [1]. More recently, on September 8th, 2013, an attack on a security camera system caused a major tunnel in Israel to close for two straight days [2]. Such attacks cause physical damage and could potentially kill people, and the threat is real and not going away. Unfortunately, as control systems become even more ubiquitous and take larger roles, successful attacks can only become more dangerous.

The next type of cyber-attack is that against government systems and websites. In this scenario, an organization or foreign country launches a cyber-attack on an electronic system with the intent to render it unavailable, either through a distributed denial of service (DDOS) attack or a more sophisticated mechanism. In 2009, for example, an attack (most likely by the North

Koreans) targeting the United States and South Korean successfully limited access to numerous sites including those of the Treasury Department and Federal Trade Commission [3]. In a more drastic scenario, an attack targeting polling stations, for example, could severely compromise the results of an election, or other attacks could destroy government information stored on servers. Though such attacks do not always cause physical damage, they can disrupt government operations and cause economic damage.

Finally, an attack may target military systems and those of key contractors in order to assess capabilities or to steal technologies. In this scenario, an attack installs some sort of worm into target systems. This worm collects data and sends it back to the attacker. By installing worms on military and contractor computers, a foreign country can collect plans and research on various technologies. China, especially, has targeted United States military contractors in order to catch up on military technology. Pentagon reports indicate that Chinese hackers have already stolen designs for, among other aircraft, the Black Hawk helicopter and the F-35 Fighter [4]. Several United States cybersecurity companies recently reported that China has been systematically attacking contractors involved in drone design and manufacturing for the United States military [5]. Such attacks not only cause trillions of dollars in economic damage (the development of the F-35 itself will cost the United States about $1.4 trillion) [4], but also compromise the United States' military advantage. The Chinese threat is discussed specifically later in this paper as a case study for potential solutions.

The attacks above can be conducted by both other nations, as in traditional military attacks, and non-state actors, such as terrorist and vigilante groups. The United States most likely does not have to worry about a large, traditional military attack by another nation – its military is simply too powerful. Cyber-attacks are different, however. It is an asymmetric weapon; defense is much harder than offense, and the cost-of-entry barrier is less than that of a physical weapon. Furthermore, the source of an attack is not immediately clear, lending plausible deniability to an attacking nation, at least until a thorough analysis of the code is conducted. Finally, as discussed in detail later, a lack of international structures and laws to deal with cyber-attacks leaves a victim nation with few avenues, short of retaliatory cyber and traditional attacks, to respond. As such, faced with a daunting disadvantage in terms of traditional military capacity, countries may use cyber-attacks to, at the minimum, annoy stronger powers. Furthermore, just as terrorist groups have upended the typical military balance between nations, non-state actors have become a significant threat in cyber-space. A cyber act-of-terror has similar causes and consequences as traditional terrorism does. However, again due to a lack of international agreement concerning cyber-attacks, nations can support cyber-groups with impunity[1], and prosecuting a group across borders is difficult. Such actors include both 'Hacktivist' organizations that use cyber-attacks to achieve certain (often ambiguous) objectives and more traditional terrorist organizations In the status quo, hactivist organizations, such as Anonymous, have been more active in carrying out attacks. Anonymous is a loose amalgam of hackers and activists who carry out attacks, often DDOS attacks, against organizations they oppose. For example, after the death of Aaron Swartz, a young Internet activist, Anonymous brought down and defaced the website of the United States Sentencing Commission [6]. In December 2011, the organization declared war on the United States government in response to the SOPA bill in Congress [7]. The U.S. is not the only country facing its attacks. In April 2012, Anonymous declared war on China and hacked numerous

[1] Even more so than they can with traditional terrorist groups

government sites [8]. Though some people tend to laud Anonymous' stances the fundamental fact remains that it is not safe for a shadowy group to have power to damage the United States government if the government acts in a way the group does not like.

Before recommending solutions for the cyber-threat, it is important to analyze the status quo problems that contribute to the United States' vulnerability. Most fundamentally, the United States federal government has too few legal and technological avenues, both domestically and globally, to reduce the security threat and respond to attacks in the status quo.

First, critical infrastructure is almost exclusively managed by private companies – energy distributors, for example. Private companies, especially military contractors, have repeatedly been victims of various kinds of cyber-attacks. In the Chinese technology thefts detailed above, for example, military contractors were the largest targets [4]. Devising a cohesive strategy or adopting best practices and technologies becomes difficult when doing so must be coordinated with numerous private companies.

Second, even if the government could enforce security mechanisms, the necessary technology simply may not exist or even be possible. Experts continually find new weaknesses in computing systems and zero day exploits[2] are, by definition, impossible to foresee. Best practices for security technologies cannot completely protect against such vulnerabilities, and more robust

[2] "a virus or other exploit that takes advantage of a newly discovered hole in a program or operating system before the software developer has made a fix available—or before they're even aware the hole exists" [37]

technology must be developed. Until such robust systems are developed, however, companies and the government must follow what best practices they can.

Third, no international standards, codes of conduct, or accepted practices have been developed governing cyber-attacks. Though cyber-attacks have occurred and are an increasing danger, countries do not yet have adequate legal avenues[3] to respond to attacks. Though the legality and ethical nature of United States' use of cyber-attacks is out of the scope of this paper, I discuss possible avenues the United States can use to prevent and respond to cyber-attacks on its infrastructure, government, and military.

Governmental leaders are not blind to the threat and the lack of acceptable responses in the status quo. They recognize the problem and have committed to further develop cyber security. In 2007, several United States Representatives and the Center for Strategic and International Studies released a report entitled "Securing Cyberspace for the 44th President," describing the nascent threats and presenting a high-level roadmap for addressing the problem [9]. In February 2009, soon after his inauguration, President Obama ordered a 60-day review of the US's cyber-security programs, resulting in a report that described in stark terms the threats facing the United States, the government's current inability to respond to those threats, and a plan forward [10], [11]. Numerous other private organizations, researchers, and academics published reports detailing the problem and recommending solutions.

[3] I use "legal" avenues in both senses of the word: responses which are considered legal under international law, and responses that appeal to the enforcement of some international standard through some international organization

However, an overarching national strategy to address the threats has yet to be properly implemented. The Cyber Intelligence Sharing and Protection Act (CISPA), which would have allowed companies to share the information they have collected on Internet traffic with the government, died after significant opposition from privacy groups, and President Obama has indicated opposition to its resurrection [12]. More recently, the Cybersecurity Act of 2012 failed in the United States Senate, even after support from President Obama and, to a limited extent, privacy advocates [13], [14]. In response, President Obama in February 2013 issued an Executive Order to direct the National Institute of Standards and Technology (NIST) to develop cybersecurity best practices and to increase information sharing about attacks between companies and the government. NIST released its preliminary framework for best practices on October 22, 2013, and it remains to be seen whether these efforts will be successful in increasing security [15]. While more advanced security technologies are developed, such best practices may reduce the risk of successful cyber-attacks.

These current attempts to increase the use of security practices in the United States must continue, and I argue that they should be drastically extended in scope. The legislative and statutory solutions taken as of yet are voluntary and educational. The Department of Homeland Security hosts training sessions for factory owners and operators of infrastructure in which it tries to instill the importance of taking security measures [16]. These sessions are effective in leading operators to take practical security measures. Similarly, the NIST standards for private infrastructure owners could improve security, if its recommendations are followed. However, as Thomas Rid argues in “Cyber-Sabotage is Easy,” factory and infrastructure operators have, by and large, not yet installed basic security because they do not yet believe the threat is real [16]. Security measures cannot continue to be optional in regards to critical infrastructure.

I recommend that United States federal government mandate and regulate security measures (such as those recommended by NIST) on certain infrastructure systems and at military development contractors. Voluntary measures are an important first step, but I argue that companies will not get serious about the threat until mandated to do so. The federal government already regulates many aspects at privately owned factories, infrastructure systems, and military contractors. More specifically, increased regulation and investment in security can follow the model the Obama administration and the Federal Energy Regulatory Commission have created in modernizing the U.S. electric grid. Just as the electric grid (and other infrastructure) faces a cyber-threat, it also faces a threat of “severe breakdowns” due to aging equipment and an inability to utilize renewable sources, and the fragmented energy market has been unable to find a solution [17]. In response, the Obama administration is requiring utility companies to “collaborate on regional planning” and is investing in grants that will incentivize companies to upgrade their respective grids with smart meters and advanced sensors [17]. A similar program can mandate that utility companies work together on securing the grid and can provide grants to help companies do so. Chemical plants and other factories can follow the same collaborative model and mandates, especially because most chemical plants have similar structures and control systems. Such plants are already heavily monitored through environmental and safety regulations, and cyber-security will soon be no less important. However, increased regulations may be difficult to pass in a tough economic and political climate, and the Obama administration may have to use executive orders when it can, as it did with the NIST standards and the smart grid upgrades.

While drastically increased cyber-security regulations may have to wait for the appropriate political time, the military can, and should, begin to regulate cyber-security more stringently among its contractors. The United States military has a close relationship with many of its largest contractors and is often their biggest customers. Consequently, the military and the federal government are in a position to mandate that its contractors follow specified security protocols as part of their contracts. As described above, the contractors have been unable to police themselves on cyber-security and are the target of sophisticated Chinese hacking designed to steal U.S. military technologies. I recommend that the U.S. mandate that any contractor follow certain best practices to encrypt its data and isolate its networks from the internet as a whole. As with private companies, such a mandate has a recent predecessor. In the several years before 2012, numerous reports came out detailing the use of bogus and potentially vulnerable Chinese microchips in technologies developed by military contractors [18], [19]. Contractors were using these parts because they were less expensive than parts made elsewhere and continued to use them despite the reports. Finally, in 2012, Congress in the National Defense Authorization Act mandated that military contractors could not purchase "electronic parts from unknown and suspicious suppliers" [20]. Since then, the threat of vulnerable Chinese microchips has receded, though the military is still finding out the extent of the damage. A mandate to follow best cyber-security practices may not stop all cyber-attacks, as more sophisticated defense systems may have to be developed for that goal, but it can reduce the threat and system vulnerabilities.

Unfortunately, these attempted and recommended solutions (both those that have failed in Congress and those that have yet to be fully implemented), only address part of the cyber-security problem. Cyber-defense is important, but more important is an international order in which cyber-attacks are infrequent and as taboo as traditional attacks. In the status quo, attacking countries have benefited from the lack of international laws or structures to govern cyber-warfare, and so have been able to attack without fearing the consequences typically associated with a military attack.

This scenario has already played out. In 2007, after a disagreement, state-sponsored “Russian cyber-militias launched a denial of service attack on Estonia that paralyzed the nation's banking infrastructure and civil services” [20]. As a NATO ally, Estonia “invoked Article 5 of the NATO charter,” which, in a traditional attack, would have required other NATO allies to consider the attack as if it was against all NATO members. [20]. However, the immediate response was muted because 1) they did not view that the attack met the standards in the charter, and 2) due to the nature of cyber-attacks, Estonia could not, without a doubt, blame Russian actors until much after the incident. As a result, other NATO nations helped restore the affected services but Russia was not punished or officially held responsible [21]. Since then, NATO has enhanced its joint cyber-defense capabilities and Estonia has pushed for an international dialogue on cyber-warfare, but little progress has been made on a larger scale [21]. Russia, encouraged by this non-response, has encouraged militias within the country to launch cyber-attacks against government services and websites in Georgia, Lithuania, and Kyrgyzstan in the last several years [22]. Assuming a constant state of cyber-attacks globally is undesirable, cyber-attacks must be responded to in some significant manner. Though immediate offensive counter-attacks may not be feasible due to the difficulty of pinpointing an exact attacker, nations must be punished for their actions in the cyber space.

To solve this problem and to make possible an effective diplomatic response to cyber-attacks, the United States must first fight to establish international standards for cyber-warfare and cyber-attacks. Such an international standard must have two characteristics: it must equate damage caused by cyber-attacks to those caused by traditional means; and, just as with state-sponsored terrorism, it must hold governments accountable for the actions of groups supported by the government[4]. Without the former, a legal, punitive response (such as sanctions) to cyber-attacks will be less justifiable. Without the latter, a country can simply hide behind shadow groups that carry out its orders, as in the case of the Russian attacks.

This fight will be difficult because, though other countries may use attacks such as those by China and Russia, the United States, through Stuxnet, is one of the few countries to have launched a sophisticated cyber-weapon specifically targeting physical (nuclear) infrastructure of another nation outside of wartime[5]. The United States may have a natural response: that its attack was meant to delay Iran from developing an even more dangerous weapon (a nuclear weapon), while attacks by other nations are meant to either steal weapon information or potentially damage civil infrastructure. However, even the Obama administration has recognized, internally at least, the damage that Stuxnet can cause to United States interests in cyber-security. A leaked

[4] And, just as with state-sponsored terrorism, solutions must be found for cases in which no clear, direct link connecting a group to a country is available.

[5] Though the United States and Israel have not officially claimed responsibility for the attacks, leaks, including by Edward Snowden, paint the undeniable picture that the two countries were responsible [36].

memo on offensive and defensive capabilities expresses concern about the “unintended or collateral consequences” of its offensive actions and capabilities [16]. Limiting access to and preventing development of cyber weapons is nearly impossible, but the United States can help develop norms against using cyber tactics by disavowing its own past use and committing to not using them absent actual war. Not doing so puts the world in a state of perpetual cyber-warfare, as states continually try to get an advantage by using such weapons.

The international norm on nuclear weapons provides an imperfect yet useful analogy for the United States’ dilemma. Though the United States is the only country to ever use nuclear weapons, it has led a global movement to limit access to nuclear technology and ban the surface level testing and use of such weapons. It has been successful in doing so by limiting its own arsenal (such as through the bilateral START treaties), adhering to the testing prohibitions, and simply not using the weapons further. The resulting norms have justified sanctions and punitive measures on countries who attempt to develop nuclear weapons, such as Iran and North Korea. Furthermore, international organizations and cooperation between nations have developed to prevent non-state actors from accessing and using a nuclear weapon. UN Security Council Resolution 1540 mandates that the nuclear states protect their nuclear arsenals appropriately [23]. Since then, nuclear states have formed several initiatives along with the International Atomic Energy Agency to mandate certain security protocols [23]. Though countries may not always agree regarding nuclear policy and access, they work together for the mutual interest of preventing nuclear terrorist attacks. Similar agreements for cooperation can be developed concerning cyber-attacks by non-state actors.

The above discussion about international norms and cooperation begets several concerns: how exactly can a country be held responsible for attacks by groups only loosely (and unofficially) connected to its military? How can a country *prove* that a given nation is responsible for the attacks? How can an international norm be developed when countries cannot even agree on the basic facts and current extent of cyber-attacks? How can a country be punished for attacks that only cause economic damage?

Consider China as a case study. United States action in response to Chinese attacks to steal intellectual property serves as an illustrative example for what can and cannot work in pursuit of a diplomatic solution to cyber-attacks[6]. As discussed above, for much of the past decade, attacks originating from China have attacked United States military operations and contractors, though the People's Liberation Army (PLA) has denied responsibility. The United States has as of yet been ineffective in stopping these cyber-attacks through diplomatic means (though it has engaged in a constant cat-and-mouse game of defending against cyber-attacks). Its diplomatic options and actions themselves have been limited. For years, though Chinese hacking has been an open secret, the government refused to formally accuse China of cyber-attacks because it did not have proof of a direct connection between the PLA and the hackers.

This year, however, several events escalated accusations and progressed talks between China and the United States concerning cyber-security. First, in February, security firm Mandiant released a

[6] A more detailed study of United States/Chinese cyber-security relations would be out of the scope of this paper, as that would require an analysis of warfare capabilities and a comparison of United States network centric capabilities versus increasing Chinese capabilities A leaked Chinese military report reveals that many in the Chinese military consider preparation for total (cyber, space) war with the United States a key priority. Their plans include simulations for destroying United States satellites [33].

report explaining the existence of an expert hacking group headquartered in a PLA building. This group has been responsible for a large number of international cyber-attacks [24], [25]. The report is filled with specific information concerning the makeup of the experts in the group, the attacks it carried out, and the connections to the PLA. This report illustrates that though finding proof of cyber-attacks may be difficult, especially in the short term, it is not impossible. Attackers can be traced through a network. Following this report, in May, the Pentagon released a report that accuses China of conducting cyber-attacks [26], [27]. However, even with this proof and accompanying accusation, the United States is left with no legal international avenue to punish the Chinese, or, at the least, is unwilling to take such actions. Thus, in June, 2013, President Obama employed the only pressure he could, when Chinese President Xi Jinping visited the United States [28]. Unfortunately, no progress in abating Chinese attacks has been made, despite the Mandiant report, the Pentagon report, and direct Presidential discussions concerning cyber security. Without an accepted international mechanism to deal with such attacks and punish an attacker, the U.S. simply cannot stop other countries from attempting to hack its systems and steal its technologies.

China responds to these accusations by noting, correctly, that it is also the victim of cyber-attacks, most of which originate in the United States. Jason Healy argues that “China not only has a cyber problem, it has a valid *U.S.* cyber problem” [29]. The United States is the “largest single point of origin of cyber attacks against China,” according to the Chinese press, and the statistics are largely accurate [29]. There is a crucial difference between the attacks by China and those against China, however: while there is evidence that the PLA is conducting organized attacks against U.S. military contractors, there is no such evidence that the attacks against China are U.S. government-led. Nevertheless, the U.S. is hurt by its secretive yet demonstrated offensive capabilities, and its inability to police criminal cyber-activity within its borders. The U.S. must learn that its attacks (against Iran) and any future cyber attacks kill its credibility in pressuring others to cease their attacks. The United States cannot be naïve in not developing capabilities in the new military domain, especially defensive capabilities, but it needs to develop a responsible use doctrine that forbids use of cyber-attacks (within the definition this paper addresses) outside of declared war. Without such a doctrine, the Chinese and others are able deflect attention away from their attacks by playing the victim.

On the other hand, another event this year, in April, may lead to a path forward to stopping Chinese cyber attacks. Secretary of State John Kerry announced a joint task force between the U.S. and China was for cyber issues [30], and the meeting between the two presidents also included discussion of joint action. Though it remains to be seen whether this task force can bring meaningul results, it is a sign that both countries recognize the threat of non-state actors to their cyber-security, even as they may not yet be willing to stop their own offensive capabilities. If this task force can produce meaninful results, the U.S. will learn that even occasionally hostile nations can cooperate regarding the threat of non-state actors. As such, the U.S. should pursue engagement with the Chinese and other nations regarding the prosecution and neutralization of non-state cyber threats, such as Hacktivist organizations and terrorist groups. A larger, direct problem between nations attacking each other should not hinder cooperation for mutual interest.

The China case study presents many lessons for the United States on the international stage – it must be aggressive and thorough in finding attackers, but it must be willing to work with other countries on common interests in the cyber-domain, as in any other issue. It needs some international law, norm, or structure through which it can seek to hold attackers accountable, but it must be willing to reconsider its own actions and the perspectives of other nations.

The cyber-security problem is fraught with issues that United States cannot immediately change and uncertainties regarding technology still to be developed. However, the unknowns and the uncontrollable should not prevent the United States from doing what it can. The United States must attack the problem on two fronts. It must make its infrastructure, government systems, and military technologies more secure, but it must also wage a diplomatic battle to lessen the use of cyber-attacks on the global stage. The recommendations outlined in this paper will not permanently eliminate the cyber-security threat, which may be impossible. However, they will help the United States continue its reevaluation and improvement of its cyber defenses.

Works Cited

[1] T. Espiner, "CIA: Cyberattack caused multiple-city blackout," 22 January 2008. [Online]. Available: http://news.cnet.com/2100-7349_3-6227090.html. [Accessed 15 October 2013].

[2] D. Estrin, "AP Exclusive: Israeli tunnel hit by cyber attack," 27 October 2013. [Online]. Available: http://www.usatoday.com/story/tech/2013/10/27/ap-exclusive-israeli-tunnel-hit-by-cyber-attack/3281133/.

[3] "Federal Web Sites Knocked Out by Cyber Attack," 08 July 2009. [Online]. Available: http://www.foxnews.com/story/2009/07/08/federal-web-sites-knocked-out-by-cyber-attack/.

[4] E. Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," 27 May 2013. [Online]. Available: http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_print.html.

[5] E. Wong, "Hacking US Secrets, China Pushes for Drones," 20 September 2013. [Online]. Available: http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?_r=0.

[6] B. Brumfield, "Anonymous threatens Justice Department over hacktivist death," 27 January 2013. [Online]. Available: http://www.cnn.com/2013/01/26/tech/anonymous-threat/.

[7] J. Boone, "In response to SOPA, Anonymous hackers target US government," 16 December 2011. [Online]. Available: http://www.globalpost.com/dispatch/news/regions/americas/united-states/111216/anonymous-hackers-sopa-vote-congress.

[8] Wall Street Journal, "Anonymous Hacks Chinese Government Websites," 4 April 2012. [Online]. Available: http://blogs.wsj.com/chinarealtime/2012/04/04/anonymous-hacks-chinese-government-websites/.

[9] Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency," Washington, DC, 2008.

[10] M. Roy, "Obama Orders 60-Day Cyber-security Review," 10 February 2009. [Online]. Available: http://www.eweek.com/c/a/Security/Obama-Orders-60Day-Cyber-Security-Review/.

[11] "Cyberspace Policy Review: Assuring Trusted and Resilient Information and Communications Infrastructure," Washington, DC.

[12] "Beyond CISPA: The cybersecurity bills you need to worry about right now," 15 May 2012. [Online]. Available: http://www.digitaltrends.com/web/beyond-cispa-the-cybersecurity-bills-you-need-to-worry-about-right-now-cybersecurity-act-of-2012-secure-it-act/.

[13] J. Rizzo, "Cybersecurity bill fails in Senate," 2 August 2012. [Online]. Available: http://www.cnn.com/2012/08/02/politics/cybersecurity-act/index.html.

[14] White House Office of the Press Secretary, "Op-ed by President Obama: Taking the Cyberattack Threat Seriously," 19 July 2012. [Online]. Available: http://www.whitehouse.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously.

[15] NIST Press Release, "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments," 22 October 2013. [Online]. Available: http://www.nist.gov/itl/cybersecurity-102213.cfm.

[16] T. Rid, "Cyber-Sabotage Is Easy: So why aren't hackers crashing the grid?," 23 July 2013. [Online]. Available: http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it?page=0,2.

[17] Bloomberg News, "U.S. Electric Grid Gets Regulatory Jolt Into 21st Century," 10 October 2012. [Online]. Available: http://www.bloomberg.com/news/2012-10-10/u-s-electric-grid-gets-regulatory-jolt-into-21st-century.html.

[18] C. Arthur, "China-sourced fake chips used in US military, says BusinessWeek," 6 October 2008. [Online]. Available: http://www.theguardian.com/technology/blog/2008/oct/06/security.china.

[19] "US weapons 'full of fake Chinese parts'," 8 November 2011. [Online]. Available: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8876656/US-weapons-full-of-fake-Chinese-parts.html.

[20] D. Perry, "U.S. Senate Warns of Counterfeit Electronics in the Military," 23 May 2012. [Online]. Available: http://www.tomsguide.com/us/hardware-government-military-chip-counterfeit,news-15308.html.

[21] S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security,* vol. 4, no. 2, 2011.

[22] W. C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review,* vol. 11, 2009.

[23] F. Steinhausler, "Legal Instruments to Prevent Nuclear WMD Use by Non-State Actors," *Strategic Insights,* vol. 8, no. 1, 2009.

[24] A. C. Estes, "Chinese Army Hackers Are Trying to Bring Down U.S. Infrastructure, After All," 18 February 2013. [Online]. Available: http://www.thewire.com/global/2013/02/chinese-army-hackers-are-trying-bring-down-us-infrastructure-after-all/62270/.

[25] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 2013.

[26] D. E. Sanger, "U.S. Blames China's Military Directly for Cyberattacks," 6 May 2013. [Online]. Available: http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?_r=0.

[27] Department of Defense, United States of America, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," 2013.

[28] J. Gerstein, "Obama and Xi talk cyber to press, not so much each other," 8 June 2013. [Online]. Available: http://www.politico.com/politico44/2013/06/obama-and-xi-talk-cyber-to-press-not-so-much-each-165727.html.

[29 J. Healy, "China Is a Cyber Victim, Too," 16 April 2013. [Online]. Available:

] http://www.foreignpolicy.com/articles/2013/04/16/china_is_a_cyberwar_victim_too.

[30] Reuters, "U.S., China agree to work together on cyber security," 13 April 2013. [Online]. Available: http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413.

[31] "Zero-day attack," [Online]. Available: http://en.wikipedia.org/wiki/Zero-Day_Exploit.

[32] J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies,* vol. 22, no. 3, pp. 365-404, 2013.

[33] B. Gertz, "China's Military Preparing for 'People's War' in Cyberspace, Space," 30 July 2013. [Online]. Available: http://freebeacon.com/china-military-preparing-for-peoples-war-in-cyberspace-space/.

[34] "Hacker group Anonymous is a nuisance, not a threat," 20 January 2012. [Online]. Available: http://money.cnn.com/2012/01/20/technology/anonymous_hack/.

[35] R. B. Andres, "Cyber-Gang Warfare," 11 February 2013. [Online]. Available: http://www.foreignpolicy.com/articles/2013/02/11/cyber_gang_warfare?page=0,1.

[36] E. Nakashima and J. Warrick, "Stuxnet was the work of U.S. and Israeli experts, officials say," 1 June 2012. [Online]. Available: http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials.

[37] L. Seltzer, "The Zero-Day Attack," 2 November 2005. [Online]. Available: http://www.pcmag.com/article2/0,2817,1879939,00.asp.