Cyber War: the Challenge to National Security

Nathalie Caplan
Conflict Management and Resolution Graduate Program
University of North Carolina Wilmington
Wilmington, NC 28403
nmc2150@uncw.edu

Abstract

The Department of Homeland Security has identified the increasingly frequent attacks on cyber networks as one of the most severe national security threats to the United States. In fact, cyber is now considered a warfighting ódomain,ô along with land, sea, air, and space. Cyber attacks targeted at hijacking critical infrastructure (electrical power, pipelines, airlines, railroads, banking, etc.) are particularly alarming. Regrettably, the United States is more vulnerable to cyber attacks because of its greater dependency on cyber-controlled systems to run critical national infrastructure. Moreover, the military dependence on civilian infrastructure (computer systems and networks, satellites) heightens U.S. vulnerability. The growing reliance on cyber infrastructure opens the way to new national security threats against the United States. Potential adversaries attempting to surreptitiously avoid direct confrontation with the U.S. military can attack America through cyberspace. This paper identifies China and Iran as nations posing cyber threats, as well as explores the risks of cyber terrorism. Despite efforts by the Department of Homeland Security, the U.S. Cyber Command Unit, and the FBI, a coordinated policy must be established to safeguard critical infrastructure from cyber attack.
Key Words: Cyber Warfare; Cyber Security; National Security; Critical Infrastructure; U.S. Cyber Command Unit; STUXNET; DUQU; Cyber-Security Act of 2012; Cybersecurity Executive Order

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy." - 2010 National Security Strategy

Introduction

In the last decade, the United States has begun to recognize the importance of cyber security. On May 29, 2009, President Obama confirmed U.S. concern, stating: ñWe count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic controlé But just as we failed in the past to invest in our physical infrastructure ï our roads, our bridges and rails ï we've failed to invest in the security of our digital infrastructureé This status quo is no longer acceptable ï not when there's so much at stake. We can and we must do better.ò[1]

Cyber attacks are extremely inexpensive and easy to conduct; therefore, they will become increasingly prevalent in modern warfare. Bill Woodcock, director of a non-profit organization that monitors cyber security, asserts: ñIt costs about 4 cents per

[1] The White House: Office for the Press Secretary, "FACT SHEET: Cyber Security Legislative Proposal." Last modified May 12, 2011.

machine. You could fund an entire cyber warfare campaign for the cost of replacing a tank tread, so you would be foolish not to.ò[2] Furthermore, the United Statesô dependency on electronics and telecommunications grows daily; consequently, the vulnerability to a cyber attack is ever increasing.

Scott Borg, director and chief economist of the U.S. Cyber Consequences Unit, highlights the dangers of cyber attacks, maintaining that ñattacks of this kind, directed at critical infrastructure industries, have the potential to cause hundreds of billions of dollars worth of damage and to cause thousands of deaths.ò[3] Alarmingly, some of the attacks that would have devastating consequences are currently outlined on hacker websites and at hacker conventions.[4] Without a doubt, the United States must establish a coordinated policy to ensure that its vital infrastructure does not fall victim to a catastrophic cyber attack.

The Threat

Several potential adversaries have the capability to carry out catastrophic cyber attacks against the United States. Cyber attacks are defined as ñdeliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.ò[5] Recently, the Department of Homeland Security has identified the increasingly frequent attacks on our cyber networks as one of the most severe national security threats to the United States. In fact, ñalthough it is a man-made domain, cyberspace is now as relevant a domain for Department of Defense activities as the naturally occurring domains of land, sea, air, and space.ò[6]

Richard Clarke, senior White House advisor, argues that cyber war has emerged as the foremost security challenge of the 21st century. Clarke defines cyber war as, ñactions by a nation-state to penetrate another nationôs computers or networks for the purpose of causing damage or disruption.ò[7] Clarke contends that the United States is more vulnerable than other world nations to cyber attack, offering four reasons. First, the United States has a greater dependency on cyber-controlled system to run the essential national infrastructure, such as electrical power, pipelines, airlines, railroads, and banking. Second, the majority of U.S. critical infrastructure is privately owned. Third, the U.S. is one of the only countries in the world in which corporate owners are so politically powerful that they can prevent government regulations in their industries. Finally, the

---

[2] Markoff, John. ñBefore the Gunfire, Cyberattack.ò Last modified August 12, 2008.
[3] The U.S. Cyber Consequences Unit, "US-CCU." Last modified 2012.
[4] The U.S. Cyber Consequences Unit, "US-CCU." Last modified 2012.
[5] The National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. 2009.
[6] The U.S. Department of Defense, ñ2010 Quadrennial Defense Report.ò Last modified February 2010.
[7] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It*. 2010, p.6.

U.S. military is extremely susceptible to cyber attack.[8] These four characteristics together suggest that a potential adversary could do more cyber damage to the United States than the U.S. could do to them.

Like Clarke warns, cyber attacks aimed at hijacking critical infrastructure are particularly alarming; the possible dangers are unlimited. Dudney argues, ñThe worst attacks would be ones that physically destroy infrastructureð wrecking big electric generators, blowing up oil refineries, disrupting pipelines, crashing trains in tunnels, causing toxic chemicals to leak from chemical plants, and so forth.ò[9] A major cyber attack could not only devastate the U.S. homeland, but also impact its ability to project military power globally.

The interdependence of U.S. critical infrastructure increases its vulnerability to attack. The EMP Commission Report posits, ñThe interdependence on the proper functioning of such systems constitutes a hazard when threat of widespread failures exists. The strong interdependence of our critical national infrastructures may cause unprecedented challenges in attempts to recover from the widespread disruption and damage.ò[10] In fact, nearly all U.S. infrastructures are reliant on electrical power and/or telecommunications. So, the U.S. must take precautions to protect these two vital systems.

To make matters worse, many components of U.S. infrastructure, including ñlarge turbines, generators, and high-voltage transformers in electrical power systems, and electronic switching systems in telecommunication systems,ò could take years to repair.[11] In todayôs society, electrical power and telecommunication systems are key components of every day life. Consequently, a cyber attack on the U.S.ôs national infrastructure could have tragic consequences.

In a speech the House Energy and Commerce oversight and investigations subcommittee, Gregory Wilhusen, director of information security issues for the Government Accountability Office, argues: ñThreats to systems supporting critical infrastructure are evolving and growing. The potential impact of these threats is amplified by the connectivity between information systems, the Internet, and other infrastructure, creating opportunities for attackers to disrupt telecommunications, electrical power and other critical services.ò[12] A plethora of other industries could be affected by a cyber

---

[8] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It.* 2010.

[9] Dudney, Robert. ñCyber Militias.ò Last modified February 2011.

[10] The U.S. House Armed Services Committee, ñReport of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructure.ò Last modified April 2008.

[11] The U.S. House Armed Services Committee, ñReport of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructure.ò Last modified April 2008.

[12] Fulgham, David. ñNew U.S. Air-Sea Battle Scheme Said To Worry Beijing.ò Last modified March 20, 2011

attack, including transportation, power transmission, and pipelines. Borg maintains, ñThe total economic destruction caused by an intense campaign of such attacks could be greater than the damage done to Germany and Japan by strategic bombing during World War II.ò[13]

One of the greatest vulnerabilities to cyber attacks is the military dependence on civilian infrastructure. Deputy Defense Secretary William Lynn argues, ñJust like our national dependence, there is simply no exaggerating our military dependence on our information networks: the command and control of our forces, the intelligence and logistics on which they depend, the weapons technologies we develop and field ï they all depend on our computer systems and networks. Indeed, our 21st century military simply cannot function without them.ò[14]

Moreover, satellite vulnerability to cyber attacks has emerged as a threat to U.S national security, as the U.S. military is increasingly dependent on satellite communications. The rising interdependence between military and civilian telecommunications systems increases the likelihood of a cyber attack against commercial satellites. In fact, nearly half of the Department of Defenseôs satellite communications is dependent on civilian satellites.[15]

One reason the government has yet to defend civilian infrastructure is that it would require government regulations; in many cases, these regulations would violate privacy. Therefore, the government maintains that it is the responsibility of individual corporations to defend their networks. On the other hand, many companies argue that they have spent enough money on computer security and that defending the nation is the governmentôs responsibility.[16] In order to protect the United States from cyber attack, the government must implement safeguards to protect both military and civilian infrastructure.

A Brief History of Cyber Warfare

At a conference in Colorado Springs, Scott Borg argued that dozens of significant cyber attacks have taken place since 1998. From 1998 to 1999, these tactics were being used in the long-running conflict in Kashmir. India and Pakistan each developed cyber militias to carry out attacks against one another. Borg maintains that these cyber campaigns were ñquite significant.ò[17]

Soon after, the United States began mounting attacks. In fact, the United States utilized cyber attacks in Operation Allied Forces during the NATO airstrikes on Serbia,

---

[13] Dudney, Robert. ñCyber Militias.ò Last modified February 2011.
[14] Kruzel, John. ñCybersecurity Poses Unprecedented Challenge to National Security, Lynn Says.ò Last modified June 15, 2009.
[15] Dunnigan, Jim. "Militarizing Civilian Satellites." Last modified March 31, 2011.
[16] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It*. 2010.
[17] Dudney, Robert. ñCyber Militias.ò Last modified February 2011.

provoking an eventual counterattack by Russian hackers.[18] Also in 1999, Hamas attacked Israeli cyber targets with the help of Iranian technology. Since then, cyber attacks have emerged as a primary feature of the Arab-Israeli conflict.[19] Furthermore, in 2000, cyber attacks were used in the conflict between Turkey and Armenia. Later that year, the terrorist organization Hezbollah began to mount cyber attacks against Israel. By 2005, Indonesia and Malaysia began to utilize cyber attacks in their dispute over the Celebes Sea.[20]

The Russian attacks on Estonia in 2007 are considered to be ñWeb War One.ò Hundreds of important Estonian webpages were flooded with cyber access requests, collapsing the servers.[21] Interestingly, Estonia is one of the most wired nations in the world. It has extensive broadband penetration and utilizes Internet applications in daily life, which make it particularly vulnerable to cyber attacks.[22] As a result of the attack, Estonians could not access their online banking, newspapersô websites, or government services. Similarly, in 2007, Russia conducted cyber attacks against Lithuania. In fact, over 300 Lithuanian websites were hacked following the outlaw of Soviet symbols in the former Soviet Republic.[23]

Russia launched another significant cyber campaign in its 2008 invasion of Georgia. It mounted attacks against Georgiaôs cyber infrastructure, aiming to overload and ultimately shut down Georgian servers.[24] Servers in Georgia ñwere so flooded with incoming attacks that no outbound traffic could get through. Hackers seized direct control of the rest of the routers supporting traffic to Georgia. The effect was that Georgians could not connect to any outside news or information sources and could not send e-mail out of the country.ò[25] The attacks on Estonia, Lithuania, and Georgia reveal the capabilities of the Russian government to successfully conduct cyber war.

Challenges to U.S. National Security

In November 2011, it was revealed that two U.S. environmental imaging satellites were hacked: the Landsat 7 and the Terra.[26] The attacker gained access to the satellites

[18] Dudney, Robert. ñCyber Militias.ò Last modified February 2011.
[19] Dudney, Robert. ñCyber Militias.ò Last modified February 2011.
[20] Dudney, Robert. ñCyber Militias.ò Last modified February 2011.
[21] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It.* 2010, p.30.
[22] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It.* 2010, p.13.
[23] Fulgham, David. ñNew U.S. Air-Sea Battle Scheme Said To Worry Beijing.ò Last modified March 20, 2011.
[24] Rhodin, Sara. ñHackers Tag Lithuanian Web Sites With Soviet Symbols.ò Last modified July 1, 2008.
[25] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It.* 2010, p.19.
[26] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.

control systems; therefore, they could have potentially damage or destroy the satellites. Instead, the hackers created a specialized radio frequency signals and transmitted them to a spacecraft in Norway several times in 2007 and 2008.[27] Then, on June 20, 2011, the hackers ñachieved all steps required to command, but did not issue commands.ò[28]

Attacks such as Landsat-Terra hacking are becoming increasingly common. In fact, Army General Martin Dempsey maintains that U.S. government agencies face constant cyber attacks.[29] Similarly, Kay Sears, president of Intelsat General Corps said, ñIn 2011 alone, IntelsatONE, the terrestrial network that links customers to Intelsatôs geosynchronous communications satellites, identified about 300,000 denial-of-service attacks.ò[30] As a result, the U.S. government was alerted that it must have stronger safeguards to protect critical infrastructure from a cyber attack. China and Iran have both emerged as threat to U.S. cyber security. Furthermore, cyber terrorism has been identified as a rising threat.

The People's Republic of China

China has emerged as a cyber threat to the United States. The Report to Congress on Foreign Economic Collection and Industrial Espionage (2009 ï 2011) openly blames China for supporting cyber attacks. It reads, "The computer networks of a broad array of U.S. government agencies, private companies, universities, and other institutions -- all holding large volumes of sensitive economic information -- were targeted by cyber espionage; much of this activity appears to have originated in China."[31] The theft of sensitive economic information not only threatens U.S. national security, but also impacts the global economy.

While these attacks were aimed at stealing data, they required the same skills needed to conduct a destructive network attack.[32] Ellen Nakashima argues that the Peopleôs Liberation Army (PLA) would most likely target transportation and logistics networks before a military conflict to disrupt U.S. forces.[33] Similarly, the U.S.-China Economic and Security Review Commission told Congress, ñAuthoritative Chinese military writings advocate attacks on space-to-ground communications links and ground-

[27] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.
[28] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.
[29] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.
[30] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.
[31] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace.ò Last modified October 2011.
[32] Fox News, "Pentagon Warns China's Military Is Growing Rapidly." Last modified August 24, 2011.
[33] Nakashima, Ellen. ñChina testing cyber-attack capabilities, report says.ò Last modified March 8, 2012.

based satellite control facilities in the event of a conflict.ò[34]

In addition, U.S. officials have noted the increasing involvement of the Chinese telecommunication companies in information warfare military programs. The U.S.-China Economic and Security Review Commission claims that the three principal Chinese electronic companies ï Huawei, Zhongxing and Datang ï all receive direct government funding to develop cyber communications and intelligence gathering systems.[35] Chinese embassy representative Geng Shuang maintains that the allegations against China are groundless, stating: ñThe Chinese government prohibits online criminal offenses of all forms, including cyber attacks, and has done what it can to combat such activities in accordance with Chinese law.ò[36] However, U.S. officials continue to be skeptical. In fact, the House Intelligence Committee Chairman, Mike Rogers, is calling on the Obama administration to publically confront China and pressure it to end its illegal behavior.[37]

The Islamic Republic of Iran

Iran has emerged as a threat to U.S. cyber security. In 2011, an Iranian engineer claimed that Iran landed the CIAôs ñlostò stealth drone into hostile territory. Iranian electronic warfare specialists allegedly cut off communication links of the American bat-wing RQ-170 Sentinel.[38] Then, the droneôs GPS coordinates were altered to make it land in Iran instead of its intended location, Afghanistan. An Iranian engineer asserted, ñThe GPS navigation is the weakest pointé By putting noise [jamming] on the communications, you force the bird into autopilot. This is where the bird loses its brain.ò[39] Iranian engineers claim to be in the final stages of hacking into the droneôs secret code and revealing its top-secret technology.

General Moharam Gholizadeh, the deputy for electronic warfare of the Iranian Islamic Revolutionary Guard Corps (IRGC), maintains that Iran has technological capabilities that far exceed the ability to hack into the GPS system of a drone. In fact, he argued that Iran could change the route of a GPS-guided missile ï a weapon that moves much faster than the slow-moving drone.[40] Alarmingly, Gholizadeh maintains, ñall the movements of these [enemy drones] are being watched, and obstructing their work was

[34] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.
[35] Werner, Debra. ñHacking Cases Draw Attention to Satcom Vulnerabilities.ò Last modified January 23, 2012.
[36] Nakashima, Ellen. ñChina testing cyber-attack capabilities, report says.ò Last modified March 8, 2012.
[37] Fox News, "U.S. Calls Out China and Russia for Cyber Espionage Costing Billions,ò Last modified November 3, 2011.
[38] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.
[39] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.
[40] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.

always on our agenda.ò[41]

This 2011 incident reveals Iranôs technological prowess to the international community. This adds to the ever-widening concern regarding Iran and its foreign policy objectives. Secretary of Defense Leon Panetta maintains that the United States will continue its drone campaign over Iran to look for evidence of nuclear weapons. However, the ñstakes are higherò now that Iran has the capability to capture U.S. drones. Many U.S. officials are unconvinced of Iranôs capabilities and attribute it to a malfunction; however, there is no other explanation for how Iran obtained the drone unharmed.[42] Nonetheless, U.S. representatives are working to encrypt all drone data in Iraq.

Moreover, this event illustrates the weakness of GPS and its vulnerability to a cyber attack. Robert Densmore, former U.S. Navy electronic warfare specialist, states: ñEven modern combat-grade GPS is very susceptible to manipulation.ò[43]An attack on GPS could yield in much graver consequences. The Los Alamos reported, ñA more pernicious attack involves feeding the GPS receiver fake GPS signals so that it believes it is located somewhere in space and time that it is not. In a sophisticated spoofing attack, the adversary would send a false signal reporting the moving targetôs true position and then gradually walk the target to a false position.ò[44] To address these growing concerns, the U.S. Air Force granted two $47 million contracts to develop a new communications system to replace GPS on aircrafts and missiles.

To make matters worse, the intelligence community is convinced that Iran is responsible for a series of 2012 cyber attacks, including attacks targeting the Saudi oil industry and U.S. financial institutions.[45] According to the New York Times, Iranôs military established the ñcybercorpsò in 2011 in response to the cyber attacks on Iranôs nuclear enrichment plants.[46] Brig. Gen. Gholamreza Jalali, the head of Iranôs Passive Defense Organization, said that Iranôs cybercorps is prepared to ñto fight our enemies in cyberspace and Internet warfare.ò[47]Although Iranôs cyber capabilities are considered weaker than the capabilities of Russia and China, it is clear that Iran is emerging as a massive cyber threat to the United States and its allies.

---

[41] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.
[42] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.
[43] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.
[44] Peterson, Scott. ñIran hijacked US drone, says Iranian Engineer.ò Last modified December 15, 2011.
[45] Shanker, Thom and David Sanger, ñU.S. Suspects Iran Was Behind a Wave of Cyberattacks.ò Last modified October 13, 2012.
[46] Shanker, Thom and David Sanger, ñU.S. Suspects Iran Was Behind a Wave of Cyberattacks.ò Last modified October 13, 2012.
[47] Shanker, Thom and David Sanger, ñU.S. Suspects Iran Was Behind a Wave of Cyberattacks.ò Last modified October 13, 2012.

The Risk of Cyber Terrorism

U.S representatives have expressed concern that a variety of subnational groups will begin to conduct cyber attacks against the United States. Potential adversaries attempting to avoid direct confrontation with the U.S. military can attack America through cyberspace. In fact, there are a large number of actors that could potentially conduct a cyber attack against the United States. As a result, the U.S. fears that hostile groups or rogue nations will acquire the capability to carry out a cyber attack against the U.S. government.

Cyber-terrorism is defined as, ñthe use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.ò[48] Hostile groups could potentially hijack poorly secured computer networks to disrupt or shut down its vital functions. Today, cyber groups from across the globe are forming alliances. Although few minor incidents were reported since the 1990s, there has been no major cyber terrorist attack carried out against the United States. However, the possible consequences would be devastating.

Although it did not aim to shut down critical national infrastructure, many people consider the 2010 WikiLeaks operation as an act of cyber terrorism. The attacks, which published hundreds of thousands of classified U.S. government documents, weaken the United States by exposing government secrets. In fact, in December 2010, over 800,000 classified U.S. documents were publicized.[49] Alarmingly, top-secret government information regarding the wars in Iraq and Afghanistan were exposed. Moreover, over 250,000 top-secret diplomatic cables were stolen from the State Department records.[50] Among the information obtained included ñdiscussions on the U.S. being unable to stop Syrian arms to Hezbollah, its disappointment in Qatar to stop funding terrorism and hacking by the Chinese government of U.S. computers.ò[51]

Following the incidents, the Obama administration addressed the hackers, arguing that the attacks put ñcountlessò lives at risk, set back global counterterrorism efforts, and threatened U.S. relations with its allies.[52] Similarly, Robert Gibbs, President Obamaôs press secretary, stated: ñThese cables could compromise private discussions with foreign governments and opposition leaders, and when the substance of private conversations is printed on the front pages of newspapers across the world, it can deeply impact not only

[48] Lewis, James. ñAssessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.ò Last modified December 2002.
[49] Glick, Caroline. ñThe WikiLeaks Challenge.ò Last modified December 3, 2010.
[50] Glick, Caroline. ñThe WikiLeaks Challenge.ò Last modified December 3, 2010.
[51] Fox News, ñWikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relation.ò Last modified 2010.
[52] Fox News, ñWikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relation.ò Last modified 2010.

U.S. foreign policy interests, but those of our allies and friends around the world.ò[53]

The most worrying element of the WikiLeaks attacks is the U.S. government response. U.S officials had foreknowledge of the attacks; yet, the United States did not adequately defend against them.[54] With the damage already done, Pentagon representative Bryan Whitman released a statement, assuring the public that the Pentagon is taking additional steps to ñprevent further compromise of sensitive data.ò[55] Moreover, it recommended that the Department of Defense prevent ñcomputers from being able to copy data to removable media, limiting the platforms to move data from classified to unclassified systems, creating a two-person handling system and developing a suspicious behavior monitoring akin to systems that help credit card fraud prevention.ò[56]

Development of Weaponized Viruses – STUXNET and DUQU

The Stuxnet malware was the first major weaponized virus. It is rumored to have been developed through a joint effort between the United States and Israel; however, no country has taken credit for it. The malware was specifically to shut down key elements of Iranôs nuclear weapons program by destroying the gas centrifuges used to enrich uranium.[57] Amazingly, this program was able to penetrate Iranôs highly secure system without being discovered. In fact, Iranian officials claim that over 30,000 of their computers have been infected with the malicious software.[58]

Michael Scheidell, Chief Technology Officer of SECNAP Network Security, asserts, ñStuxnet's complexity, multi-layered design, and range of technically disparate elements suggest that a large, well-funded team is responsible for its creation-possibly a nation-state. Some analysis also points to a highly specific target-a nuclear plant in Iran. So you could conclude that a powerful entity, organization or country created Stuxnet in retaliation against Iran. We may find another scenario at the end of the day, but this one looks good, given what we know now."[59]

The Stuxnet worm focuses on Supervisory Control and Data Acquisition (SCADA) systems, which control systems such as motors, sensors, alarms, pumps, valves and other vital infrastructure. Stuxnet is capable of infecting the equipment, allowing the hacker to take remote control of the systems. The virus was orignally installed on a USB

---

[53] Fox News, ñWikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relation.ò Last modified 2010.
[54] Glick, Caroline. ñThe WikiLeaks Challenge.ò Last modified December 3, 2010.
[55] Fox News, ñWikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relation.ò Last modified 2010.
[56] Fox News, ñWikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relation.ò Last modified 2010.
[57] Dunnigan, Jim. "Deep In The Heart Of Stuxnet." Last modified January 10, 2012.
[58] Picciotti, Dean and Gregory Montanaro, ñôCry Stuxnet and Let Slip the Dogs of War?ôThe Potentially Deadly Viruses of Cyber Warfare.ò Last modified November 2012.
[59] Picciotti, Dean and Gregory Montanaro, ñôCry Stuxnet and Let Slip the Dogs of War?ôThe Potentially Deadly Viruses of Cyber Warfare.ò Last modified November 2012.

memory stick, and subsequently infected a Microsoft workstation. Then, it began to search for any system running Siemens SIMATIC WinCC software.[60] Siemens will not corroborate the number of customers it has in Iran; however, the Wall Street Journal estimates that the company had an Iranian business that netted $562.9 million in 2008.

The success of the Stuxnet virus illustrated the depth of information gathered about the Iranian nuclear program. Ralph Langer, who analyzed the Stuxnet virus, maintains that the U.S. and Israel had access to ñstolen certificates of authorization, highly protected codes that power the Siemens industrial computers, and the internal workings of Iranôs computer systems.ò[61] Experts estimate that the majority of information was collected using human intelligence, rather than computer intelligence agents. However, with DUKU, this is no longer the case.

The Duqu virus is the second major weaponized virus that has the ability to turn computers into destructive weapons. The new program uses many of the same computer codes utilized by the Stuxnet malware. However, unlike Stuxnet, Duqu does not destroy the systems it infects. Instead, Duqu secretly penetrates the systems and opens back doors that can be used to destroy the network at any time.[62] Furthermore, it embeds itself in a computer system for thirty-six days to analyze and profile the systemôs data. Then, it sends the information out through a secure server and subsequently self-destructs.[63]

Through the Duqu virus, experts have the ability to understand the inner workings of a computer network in order to develop malware to ultimately destroy the system. Moreover, the information collected by the Duqu virus allows future penetration into the network much simpler. In fact, Michael Sconzo, senior security officer at RSA, maintains that the thirty-six day window allows the program to store password patterns because most companies require password changes every thirty days.[64] It is unknown what companies the DUKU virus has infected or the extent of the information gathered from the networks. Sconzo concludes by stating: ñThere is nothing out there available to stop it.ò[65]

Although the United States is believed to be behind the development of these weaponized viruses, U.S. officials are worried that a Stuxnet-like attack could be mounted against the United States. The success of the Stuxnet and Duku viruses

---

[60] Picciotti, Dean and Gregory Montanaro, ñôCry Stuxnet and Let Slip the Dogs of War?ô The Potentially Deadly Viruses of Cyber Warfare.ò Last modified November 2012.
[61] Fox News, "Stuxnet Clone 'Duku': The Hydrogen Bomb of Cyberwarfare?" Last modified October 19, 2011.
[62] Fox News, "Stuxnet Clone 'Duku': The Hydrogen Bomb of Cyberwarfare?" Last modified October 19, 2011.
[63] Fox News, "Stuxnet Clone 'Duku': The Hydrogen Bomb of Cyberwarfare?" Last modified October 19, 2011.
[64] Fox News, "Stuxnet Clone 'Duku': The Hydrogen Bomb of Cyberwarfare?" Last modified October 19, 2011.
[65] Fox News, "Stuxnet Clone 'Duku': The Hydrogen Bomb of Cyberwarfare?" Last modified October 19, 2011.

demonstrates the fact that critical national infrastructure is vulnerable to cyber attacks. Therefore, the U.S. is in the process of revising its cyber security strategy to meet the evolving threats to national security.

United States Cyber Security Strategy

Recognizing the potential consequences of a cyber attack, the Department of Defense acknowledged the need to establish a cyber strategy. U.S. cyber security is complicated because it is very difficult to attribute cyber attacks to specific nations. Deputy Defense Secretary William Lynn maintains that this new cyber strategy allows the nationôs cyber forces to effectively attribute cyber attacks; however, he argues that it is still ña laborious process.ò[66]

Lynn notes that the military strategy alone may be ineffective against cyber attacks due to the commercial interests. In other words, criminals may employ similar tools to those used against the government and defense industry.[67] In fact, in early 2012, the Department of Defense released a press statement urging the private sector to cooperate by effectively reporting all computer network attacks.[68] National Security Agency director Gen. Keith Alexander asserts, ñWe need to see the attack. If we canôt see the attack, we canôt stop it. We have to have the ability to work with industry ï our partners ï so that when they are attacked, they can share that with us immediately.ò Consequently, the U.S. cyber strategy underlines a joint response by the government, the Pentagon, and the private sector.[69]

The Department of Defense also stresses cooperation among government agencies. The 2010 National Security Strategy reads, ñNeither government nor the private sector nor individual citizens can meet this challenge alone ï we will expand the ways we work together.ò[70] Army General Keith Alexander illustrates the federal partnership of U.S. cyber security, stating: ñU.S. cyber security as one in which Homeland Security leads in creating the infrastructure to protect U.S. interests, Cyber Command defends against attacks, FBI conducts criminal investigations, and the intelligence community gathers overseas information that could indicate attacks.ò[71]

The Department of Homeland Security plays a critical role in combating cyber attacks. The National Cyber Security Division (NCSD) works jointly with the public,

---

[66] Fulghum, David. ñCyber Planning Runs Into Bureaucratic Roadblocks.ò Last modified August 1, 2011.
[67] Fulghum, David. ñCyber Planning Runs Into Bureaucratic Roadblocks.ò Last modified August 1, 2011.
[68] Daniel, Lisa. ñDoD Needs Industryôs Help to Catch Cyber Attacks, Commander Says.ò Last modified March 27, 2012.
[69] Fulghum, David. ñCyber Planning Runs Into Bureaucratic Roadblocks.ò Last modified August 1, 2011.
[70] The White House, ñNational Security Strategy.ò Last modified May 2010.
[71] Daniel, Lisa. ñDoD Needs Industryôs Help to Catch Cyber Attacks, Commander Says.ò Last modified March 27, 2012.

private sector, and international organizations to provide a secure cyberspace.[72] The organization has two strategic objectives: ñTo build and maintain an effective national cyberspace response system, [and] to implement a cyber-risk management program for protection of critical infrastructure.ò[73] As promised, the National Cyberspace Response System works to protect critical cyber infrastructure and responds to cyber incidents. Moreover, the Cyber-Risk Management Program evaluates cyber risks, and can implement protective measures vital to safeguarding U.S. cyber infrastructure.

Furthermore, the Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council to coordinate between the private sector and the federal cyber infrastructure.[74] ñThe CIPAC represents a partnership between government and critical infrastructure owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection.ò[75]

In 2009, the Department of Defense established the Cyber Command Unit, led by General Keith Alexander. The newly formed Cyber Command Unit has three principle goals: ñManage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments; assure integrity and availability by engaging in smart partnerships, building collective self defenses, and maintaining a common operating picture; and ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.ò[76]

In May 2012, the Washington Post reported that senior military officials are advocating for the elevation of the Pentagonôs Cyber Command Unit full combat command status.[77] This act, they argue, will prove that the U.S. military takes cyber security very seriously. Ellen Nakashima reported that General Martin Dempsey, chairman of the Joint Chiefs of Staff, will recommend the change; however, President Obama has the final approval.[78]

---

[72] The White House, ñNational Security Strategy.ò Last modified May 2010.
[73] The White House, ñNational Security Strategy.ò Last modified May 2010.
[74] The U.S. Department of Homeland Security, ñCritical Infrastructure Advisory Council.ò Last modified 2012.
[75] The U.S. Department of Homeland Security, ñCritical Infrastructure Advisory Council.ò Last modified 2012.
[76] The U.S. Department of Defense,ñ Strategy for Operating in Cyberspace.ò Last modified July, 2011.
[77] Nakashima, Ellen. "Military leaders seek higher profile for Pentagonôs Cyber Command Unit.ò Last modified May 1, 2012.
[78] Nakashima, Ellen. "Military leaders seek higher profile for Pentagonôs Cyber Command Unit.ò Last modified May 1, 2012.

The FBI is leading the National Cyber Investigation Joint Task Force (NCIJTF), which unifies multiple government agencies to enforce cybersecurity.[79] In 2008, the U.S. President mandated the NCIJTF to coordinate and share information related to domestic cyber threats from all government agencies.[80] In fact, this joint task force includes eighteen intelligence agencies and law enforcement, working together to predict and prevent cyber attacks against the United States.[81]

In addition, the newly formed Defense Industrial Base Cyber Pilot Program allows for the transfer of information regarding cyber threats. In Aviation Week & Space Technology, David Fulghum states: ñUnder that program, classified threat intelligence is shared with defense contractors and their Internet service providers to help them to strengthen their defenses.ò[82] However, many major contractors have not been invited to take part in this program because funding remains unclear.

Another vital element to the U.S. cyber security strategy is the Defense Advanced Research Projects Agencyôs (DARPAôs) National Cyber Range Project.[83] Fulghum illustrates, ñThe Cyber Range is an óair-gappedô network, with no physical connections to the outside world, with servers that can simulate corporate and government networks. The idea is to insert malware into representative networks without the risk of contaminating real systems. The malware could be found on the Internet or developed by the Pentagon's or industry's own ñwhite hatò operators, who would probe network weaknesses in order to fix them.ò[84] This program is expected to be operational in late-2012.

Despite recent efforts to bolster the U.S. cyber security strategy, experts argue more actions need to be taken to effectively protect the United States from cyber attack. Richard Clarke offers a defensive strategy known as the ñDefensive Triad.ò He argues ñthe Triad stops malware on the Internet at the backbone ISPs, hardens the controls of the electric grid, and increases the security of the Defense Departmentôs networks and the integrity of its weapons.ò[85] Moreover, he offers some additional suggestions, including instituting a ñno-first-useò agreement, aimed at preventing cyber attacks from starting wars, while not limiting their use within existing conflicts.[86] Another option is to issue a

---

[79] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace." Last modified October 2011.

[80] Federal Bureau of Investigations, ñNational Cyber Investigative Joint Task Force.ò

[81] Federal Bureau of Investigations, ñNational Cyber Investigative Joint Task Forceò

[82] Fulghum, David. ñCyber Planning Runs Into Bureaucratic Roadblocks.ò Last modified August 1, 2011.

[83] Fulghum, David. ñCyber Planning Runs Into Bureaucratic Roadblocks.ò Last modified August 1, 2011.

[84] Fulghum, David. ñCyber Planning Runs Into Bureaucratic Roadblocks.ò Last modified August 1, 2011.

[85] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It*. 2010, p. 264.

[86] Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It*. 2010, p. 240.

unilateral declaration that precludes the use of cyber weapons against civilian targets. A third possibility suggested by the author is to sign international accords preventing cyber attacks on the international financial system. However, Clarke notes that the value of international agreements depends on the ability to detect violations and assign blame.

Similarly, Lynn suggests another defensive technique ï to require networks to operate improved identification management. He suggests that, in the future, information will be transmitted in encrypted form and remain encrypted as normal computer operations are executed. The 2010 National Security Strategy states: ñDefensing against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient.ò[87]

Cyber-Security Act of 2012

In response to the growing number of cyber attacks directed on both private companies and government infrastructure, Congress drafted the Cyber-Security Act of 2012. Under Senate leadership, the bipartisan legislation aims to protect the United States from cyber attack in several ways. John Brennan, assistant to the president for homeland security and counterterrorism, said that the legislation would ñgive the government the three legislative elements it needs to fend off cyberattacks: new information sharing between the government and private industry, better protection of critical infrastructure like the power grid and water filtration facilities, and authority for the Department of Homeland Security to unite federal resources to lead the government's cybersecurity team.ò[88]

In addition, the bill would require the Secretary of Homeland Security to determine which critical infrastructures are most vulnerable to cyber attack. Then, performance requirements would be set to protect the most at-risk infrastructure. ñThe performance requirements would cover critical infrastructure systems and assets whose disruption could result in severe degradation of national security, catastrophic economic damage, or the interruption of life-sustaining services sufficient to cause mass casualties or mass evacuations.ò[89] Rather than imposing mandatory participation, this bill suggests offering incentives to owners of the private-sector national infrastructure to encourage them to participate.

Furthermore, the Cyber-Security Act of 2012 would improve the security of the federal governments networks by requiring the federal government to foster a comprehensive acquisition risk management strategy. It proposes exercises and operational testing to make sure the federal agencies are prepared for a cyber attack.[90] In

[87] The White House, ñNational Security Strategy.ò Last modified May 2010.
[88] Kelly, Suzanne. ñAdministrationôs computer safety A-team urges passage of Cybersecurity Act.ò Last modified August 13, 2012.
[89] The U.S. Senate Committee on Homeland Security and Governmental Affairs. ñThe Cyber-Security Act of 2012: Summary.ò Last modified 2012.
[90] The U.S. Senate Committee on Homeland Security and Governmental Affairs. ñThe Cyber-Security Act of 2012: Summary.ò Last modified 2012.

addition, it would establish threat-information-sharing channels between the different federal agencies, as well as between the private sector and the government.[91] It ñwould provide a responsible framework for the sharing of cyber threat information between the federal government and the private sector, and within the private sector, while ensuring appropriate measures and oversight to protect privacy and preserve civil liberties.ò[92]

Unfortunately, the Cyber-Security Act of 2012 failed to garner the votes necessary to move forward, and was therefore rejected by the Senate on November 12, 2012. Opponents of this bill maintain that the government is already too involved in the private sector. In addition, the U.S. Chamber of Commerce has openly opposed the bill, arguing that it would ñimpose incapacitating pressures on businesses to inaugurate cybersecurity measures.ò[93] However, the risk is too great to ignore. Collins, Senior Republican on the Senate Homeland Security Committee, voiced his concern over this set-back, stating: "In all my years on the Homeland Security Committee, I cannot think of another issue where the vulnerability is greater and we've done less."[94] In response to Congressional inaction, President Obama remains committed to implementing cybersecurity legislation that strengthens protections for vital national infrastructure.

On November 14, 2012, the Washington Post revealed that President Obama has signed a top-secret executive order to address the cyber threats against the United States. This directive establishes ña broad and strict set of standards to guide the operations of federal agencies in confronting threats in cyberspace.ò[95] Furthermore, the executive order also aims to protect civilian networks so ñU.S. citizensô and foreign alliesô data and privacy are protected and international laws of war are followed.ò[96]

Moreover, the executive order enables the military to intervene in the case of a cyberattack. According to the Washington Post, ñthe Pentagon is expected to finalize new rules of engagement that would guide commanders on when and how the military can go outside government networks to prevent a cyberattack that could cause significant destruction or casualties.ò[97] In addition, a high priority is placed on protecting the computer systems that control critical national infrastructure.

---

[91] Rizzo, Jennifer. ñCybersecurity Bill Fails in Senate.ò Last modified August 2, 2012.
[92] The U.S. Senate Committee on Homeland Security and Governmental Affairs. ñThe Cyber-Security Act of 2012: Summary.ò Last modified 2012.
[93] Alter, Diane. ñCybersecurity Act Could Survive with Executive Order.ò Last modified November 19, 2012.
[94] Alter, Diane. ñCybersecurity Act Could Survive with Executive Order.ò Last modified November 19, 2012.
[95] Nakashima, Ellen. ñObama Signs Secret Directive to Help Thwart Cyberattacks.ò Last modified November 14, 2012.
[96] Nakashima, Ellen. ñObama Signs Secret Directive to Help Thwart Cyberattacks.ò Last modified November 14, 2012.
[97] Nakashima, Ellen. ñObama Signs Secret Directive to Help Thwart Cyberattacks.ò Last modified November 14, 2012.

Conclusion

Cyber technology has emerged as a invariable feature of modern life as individuals all over the globe interact with one another through cyberspace. In fact, from 2000 to 2010, global Internet usage increased from 360 million to over two billion users.[98] As Internet usage continues to expand, cyberspace will be increasingly relied upon by every element of U.S. society. The Department of Defense alone operates over 15,000 cyber networks and seven million computing devices all over the world. As illustrated, the nation depends on secure and reliable cyber space to protect fundamental freedoms and the very fabric of society.

The rising dependence on cyber infrastructure opens the way to new national security threats against the United States. Representative Pete Hoekstra, the ranking Republican on the House Intelligence Committee, argues, ñAs the world's number one target for spying by foreign adversaries and now clearly other hacks, the federal government must do a better job of strengthening America's computer and cybersecurity protocols. If we do not, we risk leaving exposed an Achilles heel that could cause irreparable damage to our global partnerships and international standing."[99]

By pursuing an active cyber security strategy, the Obama Administration will work to protect U.S. networks against malicious activity. However, with technological advances, cyber attacks will inevitably continue to threaten national security. Therefore, the United States must prioritize efforts to bolster cyber security for interagency, international, and critical industries. Moreover, it must continue its whole-of-government approaches to confront the challenges associated with this evolving warfighting domain.

[98] The U.S. Department of Defense, ñStrategy for Operating in Cyberspace.ò Last modified July, 2011.

[99] Fox News, ñWikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relations.ò Last modified 2010.

References

Alter, Diane. ñCybersecurity Act Could Survive with Executive Order.ò Last modified November 19, 2012. Accessed November 20, 2012. http://moneymorning.com/2012/11/19/cybersecurity-act-could-survive-with-executive-order/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+moneymorning%2FjOLe+%28Money+Morning%29.

Bumiller, Elisabeth and Thom Shanker. The New York Times. ñPanetta Warns of Dire Threat of Cyberattack on U.S.ò Last modified October 11, 2012. Accessed November 1, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

Clarke, Colin and Henry Kenyon. ñCyber Order Puts DHS In Charge Of Oversight, Sets Deadlines.ò Last modified November 20, 2012. Accessed November 25, 2012. http://defense.aol.com/2012/11/20/cyber-order-puts-dhs-in-charge-of-oversight-sets-deadlines/.

Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security And What To Do About It*. New York: HarperCollins Publisher, 2010. (accessed September 6, 2012).

Corrin, Amber. ñWhoôs Leading on Critical Infrastructure?ò Last modified November 27, 2012. Accessed November 29, 2012. http://fcw.com/articles/2012/11/27/cyber-infrastructure.aspx.

Daniel, Lisa. U.S. Department of Defense, "DOD Needs Industryôs Help to Catch Cyber Attacks, Commander Says." Last modified March 27, 2012. Accessed October 5, 2012. www.defense.gov/news/newsarticle.aspx?id=67713.

Dunnigan, Jim. "Deep In The Heart Of Stuxnet." Last modified January 10, 2012. Accessed September 5, 2012. http://www.strategypage.com/htmw/htiw/articles/20120110.aspx.

Dunnigan, Jim. "Militarizing Civilian Satellites." Last modified March 31, 2011. Accessed October 5, 2012. http://www.strategypage.com/htmw/htspace/20110331.aspx.

Federal Bureau of Investigations, "National Cyber Investigative Joint Task Force." Accessed October 6, 2012. http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

Fox News, "Pentagon Warns China's Military Is Growing Rapidly." Last modified August 24, 2011. Accessed November 5, 2012. http://www.foxnews.com/politics/2011/08/24/pentagon-warns-chinas-military-is-growing-rapidly/.

Fox News, "Stuxnet Clone 'Duqu': The Hydrogen Bomb of Cyberwarfare?." Last modified October 19, 2011. Accessed October 5, 2012. http://www.foxnews.com/scitech/2011/10/19/stuxnet-clone-duqu-hydrogen-bomb-cyberwarfare/

Fox News, "U.S. Calls Out China and Russia for Cyber Espionage Costing Billions.ò Last modified November 03, 2011. Accessed November 5, 2012. http://www.foxnews.com/politics/2011/11/03/us-calls-out-china-and-russia-for-cyber-espionage-costing-billions/

Fox News, "WikiLeaks Drop Shows U.S. Striving to Maintain Order in Chaotic Global Relations.ò Last modified 2010. Accessed September 5, 2012. http://www.foxnews.com/politics/2010/11/28/wikileak-drop-shows-fighting-increasingly-chaotic-global-relations/.

Fulghum, David. Aviation Week & Space Technology, "Cyber Planning Runs Into Bureaucratic Roadblocks." Last modified August 1, 2011. September 5, 2012. http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_08_01_2011_p28-352024.xml&p=1.

Fulghum, David. Aerospace Daily & Defense Report, "New U.S. Air-Sea Battle Scheme Said To Worry Beijing." Last modified March 20, 2012. October 5, 2012. http://www.aviationweek.com/Article.aspx?id=/article-xml/asd_03_20_2012_p02-01-438075.xml.

Glick, Caroline. The Jerusalem Post, "The WikiLeaks Challenge." Last modified Dec 03, 2010. Accessed September 6, 2012. http://www.jpost.com/Opinion/Columnists/Article.aspx?id=197761.

Johnson, Nicole. "Cybersecurity bill dies in Congress." *Army Times*, November 15, 2012. http://www.armytimes.com/news/2012/11/dn-cyber-bill-dies-congress-111512/ (accessed November 16, 2012).

Kelly, Suzanne. CNN. ñAdministrationôs computer safety A-team urges passage of Cybersecurity Act.ò Last modified August 1, 2012. Accessed October 1, 2012. http://security.blogs.cnn.com/2012/08/01/administrations-computer-safety-a-team-urges-passage-of-cybersecurity-act/.

Kelly, Suzanne. CNN. ñExecutives advocate a military approach to cybersecurity.ò Last modified August 13, 2012. Accessed October 30, 2012. http://security.blogs.cnn.com/2012/08/13/executives-advocate-a-military-approach-to-cybersecurity/.

Kruzel, John. American Forces Press Service, "Cybersecurity Poses Unprecedented

Challenge to National Security, Lynn Says." Last modified June 15, 2009. Accessed September 1, 2012. http://www.defense.gov/news/newsarticle.aspx?id=54787.

LeClaire, Jennifer. "Obama May Sign Cyber Security Executive Order." *CIO Today*, November 16, 2012. http://www.cio-today.com/news/Obama-May-Sign-Cyber-Security-Order/story.xhtml?story_id=100003G6EP88&full_skip=1 (accessed November 16, 2012).

Lewis, James. Center for Strategic and International Studies. ñAssessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.ò Last modified December 2002. Accessed September 1, 2012.

Markoff, John. New York Times, "Before the Gunfire, Cyberattack." Last modified August 12, 2008. Accessed October 5, 2012. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2.

Nakashima, Ellen. The Washington Post, "China testing cyber-attack capabilities, report says." Last modified March 08, 2012. Accessed October 6, 2012. http://www.washingtonpost.com/world/national-security/china-testing-cyber-attack-capabilities-report-says/2012/03/07/gIQAcJwDyR_story.html.

Nakashima, Ellen. The Washington Post, ñCyberattack on Mideast energy firms was among the most destructive, Panetta says.ò Last modified October 11, 2012. Accessed November 1, 2012. http://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html.

Nakashima, Ellen. The Washington Post, "Military leaders seek higher profile for Pentagonôs Cyber Command Unit." Last modified May 01, 2012. Accessed November 6, 2012. http://www.washingtonpost.com/world/national-security/military-officials-push-to-elevate-cyber-unit-to-full-combatant-command-status/2012/05/01/gIQAUud1uT_story.html.

Nakashima, Ellen. The Washington Post, ñObama Signs Secret Directive to Help Thwart Cyberattacks.ò Last modified November 14, 2012. Accessed November 19, 2012. http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

Nakashima, Ellen. The Washington Post, "U.S. Web site covering China scandal disrupted by cyberattack." Last modified April 20, 2012. Accessed November 6, 2012. http://www.washingtonpost.com/world/national-security/us-web-site-covering-china-scandal-disrupted-by-cyberattack/2012/04/20/gIQAZbRcWT_story.html.

Nakashima, Ellen. The Washington Post, ñWhen is a cyberattack an act of war?ò Last modified October 26, 2012. Accessed November 1, 2012. http://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html.

Nakashima, Ellen. The Washington Post, ñWhite House drafting standards to guard U.S. against cyberattack, officials say.ò Last modified September 7, 2012. Accessed November 1, 2012. http://www.washingtonpost.com/world/national-security/white-house-drafting-standards-to-guard-us-against-cyberattack-officials-say/2012/09/07/0fbb173e-f8fe-11e1-a073-78d05495927c_story.html.

Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace." Last modified October 2011. Accessed September 5, 2012. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

OôHarrow, Robert Jr. The Washington Post, ñCyberCity allows government hackers to train for attacks.ò Last modified November 26, 2012. Accessed November 30, 2012. http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html.

OôHarrow, Robert Jr. The Washington Post, ñIn cyberattack, hacking human is highly effective way to access systems.ò Last modified September 26, 2012. Accessed November 2, 2012. http://www.washingtonpost.com/investigations/in-cyberattacks-hacking-humans-is-highly-effective-way-to-access-systems/2012/09/26/2da66866-ddab-11e1-8e43-4a3c4375504a_story.html.

Perlroth, Nicole. The New York Times, ñAttacks on 6 Banks Frustrate Customers.ò Last modified September 30, 2012. Accessed November 1, 2012. http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?gwh=14003B9B521A7A657664D669D059F47D.

Perlroth, Nicole. The New York Times, ñIn Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.ò Last modified October 23, 2012. Accessed November 1, 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.

Peterson, Scott. The Christian Science Monitor, "Iran hijacked US drone, says Iranian Engineer." Last modified December 15, 2011. Accessed September 5, 2012. http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

Picciotti, Dean, and Gregory Montanaro. Foreign Policy Research Institute, "óCry

Stuxnet and Let Slip the Dogs of War?ô The Potentially Deadly Viruses of Cyber Warfare." Last modified November 2012. Accessed September 5, 2012.

Rizzo, Jennifer. CNN, ñCybersecurity Bill Fails in Senate.ò Last modified August 2, 2012. Accessed November 10, 2012. http://www.cnn.com/2012/08/02/politics/cybersecurity-act/index.html

Rhodin, Sara. The New York Times, "Hackers Tag Lithuanian Web Sites With Soviet Symbols." Last modified July 1, 2008. Accessed October 5, 2012. http://www.nytimes.com/2008/07/01/world/europe/01baltic.html?_r=2&scp=3&sq=lithuania&st=nyt&oref=slogin.

Sanger, David. The New York Times, ñObama Order Sped Up Wave of Cyberattack Against Iran.ò Last modified June 1, 2012. Accessed October 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

Shane, Scott. The New York Times, ñCyberwarfare Emerges from Shadows of Public Discussion by U.S. Officials.ò Last modified September 26, 2012. Accessed November 1, 2012. http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all.

Shanker, Thom and David Sanger. The New York Times. ñU.S. Suspects Iran Was Behind a Wave of Cyberattacks.ò Last modified October 13, 2012. Accessed November 1, 2012. http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html?pagewanted=all&_r=0.

The National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press, 2009. (accessed November 5, 2012).

The U.S. Cyber Consequences Unit, "US-CCU." Last modified 2012. Accessed September 5, 2012. http://www.usccu.us/.

The U.S. Department of Defense, ñ2010 Quadrennial Defense Report.ò Last modified February 2010. Accessed November 1, 2012. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf

The U.S. Department of Defense, "Strategy for Operating in Cyberspace." Last modified July, 2011. Accessed May 6, 2012. www.defense.gov/news/d20110714cyber.pdf.

The U.S. Department of Homeland Security, "National Cyber Security Division." Last modified Oct 03, 2010. Accessed September 6, 2012. http://www.dhs.gov/xabout/structure/editorial_0839.shtm.

The U.S. House Armed Services Committee, ñReport of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructure.ò Last modified April 2008. Accessed September 1, 2012. http://www.empcommission.org/docs/A2473-EMP_Commission.pdf.

The U.S. Senate Committee on Homeland Security and Governmental Affairs. ñThe Cyber-Security Act of 2012: Summary.ò Last modified 2012. Accessed September 1, 2012. http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105_-summary

The White House: Office for the Press Secretary, "FACT SHEET: Cyber Security Legislative Proposal." Last modified May 12, 2011. Accessed November 5, 2012. http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

The White House, ñNational Security Strategy.ò Last modified May 2010. Accessed September 1, 2012. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Werner, Debra. Defense News, "Hacking Cases Draw Attention To Satcom Vulnerabilities." Last modified Jan 23, 2012. Accessed October 5, 2012. http://www.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-cases-draw-attention-satcom-vulnerabilities?odyssey=mod|newswell|text|FRONTPAGE|s.