



The School for Ethics and Global Leadership

U.S. RESPONSE TO IRANIAN CYBER CHALLENGES

The School for Ethics and Global Leadership, Summer 2016
July 29, 2016

Table of Contents

Sections	Pages
History and Background	3-9
Legal Considerations	10-15
UN and the International Community	16-21
US Government: State and Defense	22-28
The Business Community	29-32
Bibliography	33-39
Appendix A	40-41

Background

Warfare and the Cyber Domain

Cyber warfare (see Appendix A) became the new form of artillery in the 21st century. Cyber warfare, a borderless and anonymous attack over the cyber domain, is a powerful act of war that exploits computer systems and software vulnerabilities.¹ As tensions between political groups rise across regions, it is crucial to understand the concept of cyber warfare in order to take preventative measures for the safety of all nations.

Cyber warfare is the conflict that results from the use of malware (see Appendix A) to disarm a nation's information network or infrastructure (see Appendix A) system. It takes advantage of the connection of computer networks to gain control of a country's infrastructure system. A cyber weapon can invade a server through an exploit in the software and can obtain confidential information to harm the infrastructure systems, such as water systems, of a country.² This exploit also means that finance corporations, among other targets, can be hacked and can lose large sums of money and customers' private information.³ Cyber warfare continues to affect various government agencies and has been ignored as a serious threat for far too long.

From Estonia to Iran, cyberattacks (see Appendix A) have become more frequent, easier to carry out, and have allowed the attackers to maintain their anonymity. In 2009, Stuxnet, a worm (see Appendix A) that exploited Windows Software, replicated itself automatically.⁴ Different from weapons and artillery used in war, cyber warfare includes malware that is controlled via the Internet.⁵ The attacks attract less attention, resulting in law enforcement officials not suspecting any dangerous activity.⁶ Individuals secure their identity behind a server, leaving authorities capable of only tracing the server, not the individual's identity.⁷ Many countries have begun to look into what measures to take in order to protect their country because one can incite cyber warfare without much effort.⁸

At the core of cyber warfare is the declaration of war. Cyber warfare allows one to attack systems without needing to be physically present and without calling attention to the premeditated attack. Countries are finding themselves at risk of being a target of cyber warfare. Each country has the right to declare war against a group or another nation, but one question comes up. Because cyber warfare allows users to remain anonymous, declaring war against nation-states is hard to prove. As cyber warfare continues to gain momentum, it is every country's responsibility to establish a stable security system in order to protect their citizens and their nation's information.

¹ Sharon Weinberger, "Is This the Start of Cyberwarfare?" *Nature*, vol. 474 (2011) : 142-145.

² Weinberger, "Is This the Start?" 142-145.

³ Stas Filshinskiy, "Privacy and Security Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air?" *Communications of the ACM*, no.56, (June 2013): 28-30.

⁴ Ibid,142-145.

⁵ Thomas A. Berson and Dorothy E. Denning, "Cyberwarfare" *IEEE Security and Privacy*, vol. 9 (2011): 13-15.

⁶ Filshinskiy, "Privacy and Security?"142-145.

⁷ Ibid.

⁸ Kelsey D. Atherton, "Cyber Attacks are America's Top Security Threat. That's Better News Than It Sounds" *Popular Science*,

Case Study: Estonia

In 2007, Estonia became the target of a series of anonymous cyberattacks that infiltrated government websites, online banking networks, and national news agencies. The attacks began on April 26, 2007 after the Estonian government removed the Bronze Soldier Statue, a monument dedicated to the Soviet War.⁹ The removal of the statue exacerbated the divide between the country's two largest ethnic groups, Estonians and Russians. To many ethnic Russians, the monument was a source of pride; however, the largest ethnic group in the country, Estonians, believed the statue represented the oppression they faced from 1944-1991 under Soviet rule. Hackers manipulated the uneasy political situation to their advantage. Additionally, Estonian citizens were highly dependent on the internet and technology at the time of the attacks.¹⁰ Over 60 percent of Estonia's population reported that they used the internet "for 'crucial' services everyday."¹¹ Despite their reliance on technology, Estonia lacked defensive protocols and cybersecurity technologies, which made the country vulnerable to cyberattacks.¹²

Initially, the attacks targeted government websites. The unknown hackers compromised government websites through denial-of-service (DoS) (see Appendix A) attacks. DoS attacks are aimed at specific targets, and they block access to targeted networks, servers, or websites to legitimate users. Hackers are able to block access to the specific targets by implementing different types of technological warfare including overwhelming servers with irrelevant information, obstructing routing information, and blocking communication between two different targets. Using DoS strategies, the hackers seized control of the Estonian Parliament's website and the prime minister's Reform Party website. The Estonian Minister of Defense Jaak Aaviksoo first discovered the hack when he was not able to sign in to the Reform Party's website. As the information about the attacks spread through Estonian Government agencies, the hackers continued to attack Estonian technology. During the second week of strikes, the perpetrators focused on local news websites such as the Postimees, Estonia's most prominent newspaper. By the end of the week, the websites of various news agencies had been knocked offline.¹³ The government discovered, while being attacked, that the majority of hacking systems were outside of Estonia. After this discovery, both the country and private companies began to take action by blocking international information requests. However, these actions did not deter the attackers. On May 9, 2007, the hackers unleashed their most sophisticated attack on Hansabank, Estonia's largest bank. By May 10th, the bank was forced to shut down internet operations. Shutting down internet operations meant that a population that conducted 97 percent of its banking transactions online was not able to make deposits online, operate ATMs, or use checking cards internationally. In just three weeks, hackers were able to bring down government websites, news sources, and the country's largest bank.¹⁴

⁹ Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, April 4, 2009.

¹⁰ Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

¹¹ Richards, "Denial-of-Service."

¹² Ibid.

¹³ Davis, "Hackers Take Down."

¹⁴ Richards, "Denial-of-Service."

An attack of such magnitude was unprecedented in the world of cyber warfare. Journalist Joshua Davis echoed this sentiment when he wrote, “never before had an entire country been targeted on almost every digital front all at once.”¹⁵ The hackers attacked a range of different targets from small news sources to government agencies, which revealed that in today’s technologically advanced world anybody can become a target of a cyber attack. The Estonian cyber attack of 2007 revealed the crippling nature of attacks and the range of infrastructure that hackers can target and destroy.¹⁶

Case Study: Aramco Attacks

By 2012, the world had witnessed dozens of large-scale cyberattacks including attacks on businesses; however, the cyber war waged on the Saudi Arabian oil company Aramco was unprecedented. Unlike most business targets, Aramco wielded tremendous influence globally and was incredibly wealthy. Aramco, which according to *Bloomberg* could be valued over \$2.5 trillion, is the largest producer of oil globally.¹⁷ Despite the company’s wealth, it still fell victim to an attack that *The New York Times* placed “among the most destructive acts of computer sabotage on a company.”¹⁸

The Aramco hack was meticulously planned. On the morning of August 15th, 2012, 55,000 Aramco employees did not report to work.¹⁹ Instead, they stayed at home to prepare for Lailat al Qadr, which translates to “the night of power,” one of Islam’s holiest nights of the year.²⁰ While its employees were preparing for the night of power, Aramco was losing control over its cybersystems. At 11:08 A.M., a computer virus (see Appendix A) known as “Shamoon” began to infiltrate company computers.²¹ Within hours, the virus destroyed or infected over 30,000 computers.²² The virus erased data including documents and emails from three-quarters of Aramco’s computers and replaced the files with an image of a burning American flag.²³ As a result of the cyber attack, the company was forced to shut down its internal network, disable employee emails, turn off internet access, and cease selling oil to domestic gas trucks for 17 days.²⁴ As a result of the attacks, the company’s internal network system remained offline for five months.²⁵

The Aramco hack revealed to the international community that no country, company, or individual is safe from the threat of cyber warfare. The world was forced to realize that if a company as powerful as Aramco could be hacked, any entity could be too. A small group of hackers known as “The Swords of Justice” claimed responsibility for the attack, proving that a small organization can wreak havoc on a large established business.²⁶ In the world of cyber warfare, it is not size of the parties involved that matters; rather, it is knowledge, technology, and execution.

¹⁵ Davis, “Hackers Take Down.”

¹⁶ Richards, “Denial-of-Service.”

¹⁷ Javier Blas, “Too Big to Value: Why Saudi Aramco Is in a League of Its Own,” *Bloomberg*, January 7, 2016.

¹⁸ Nicole Perlroth, “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back,” *The New York Times*, October 23, 2012.

¹⁹ Ibid.

²⁰ Ibid.

²¹ Ibid.

²² Jose Pagliery, “The Inside Story of the Biggest Attack in History,” *CNN Money*, August 5, 2015.

²³ Pagliery, “The Inside Story.”; Perlroth, “In Cyberattack on Saudi Firm.”

²⁴ Perlroth, “In Cyberattack on Saudi Firm.”; Pagliery, “The Inside Story.”

²⁵ Ibid.

²⁶ Ibid.

Stuxnet

In recent years, cyber war weapons have become a powerful tool in the ever-evolving state of warfare. In the Israeli-Iranian conflict, the first major cyber warfare weapon, Stuxnet, attacked Iran without any visible army. The Stuxnet worm targeted the Iranian Natanz military base without Iranian officials knowing. Although neither Israel nor the United States confirms using it, it was clearly an attack on the cyber domain. Unlike common cyber-weapons that act as keystroke loggers or information overload viruses, the Stuxnet attack was far more complex and did not require Internet access. The virus also attacked controllers, which are devices like pumps, valves, motors, which all make up gas pipelines or power plants.²⁷ The worm was spread over USB sticks and local-area networks (LAN) and infected every Windows PC it could find, but specifically attacks controllers from Siemens and in the Iranian Natanz uranium enrichment plant.²⁸ Symantec, a cybersecurity (see Appendix A) company, reports that Stuxnet attacked Iran as infections concentrated on Iranian hosts. Of all infected hosts, 58.31 percent were found in Iran while the other infected hosts were dispersed across numerous countries collaterally.²⁹ Symantec also reports that “the ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries.”³⁰ The complex weapon actually spun the centrifuges at the enrichment facility out of control while relaying to engineers that they were operating at a standard rate.³¹ Since the attack affected almost 70 percent of the Siemens computers in Natanz, it is widely believed that Stuxnet was designed to sabotage uranium programs to prevent Iran from developing nuclear capabilities.³² The ultimate effects rendered between one to five thousand centrifuges useless.³³

Iran’s Response

The Stuxnet cyber worm was part of a broader operation, *Olympic Games*, launched allegedly by a joint Israeli-American cyber task force that began in the Bush administration. Stuxnet was the first sustained use of cyber weapons.³⁴ President Obama continued to covertly support complex cyberattacks against Iranian nuclear facilities and power plants. According to anonymous national security members, Iranians discovered this code before the worm was used; however, the administration ultimately implemented the worm.³⁵ Initially, Iran was reluctant to accept that its enrichment facilities were subject to Stuxnet’s wrath despite numerous technology firms --- including Seculert (see Appendix A) and Symantec --- had acknowledged the worm’s effects.³⁶

Iran announced in 2011 that it was strengthening its military cyber unit and General Gholamreza Jalali said that the military was ready “to fight our enemies” in “cyberspace (see Appendix A) and Internet warfare.”³⁷ The government agency founded in 2011 by the Iranian president was called

²⁷ Ralph Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE Software Magazine*, May 2011, 49-51.

²⁸ Clay Dillow, “Stuxnet Worm Is A ‘Game Changer’ For Global Cybersecurity,” *Popular Science*, November 2010.

²⁹ Eric Chien, Liam Murchu, and Nicolas Falliere, “W32.Stuxnet Dossier,” *Symantec*, version 1.4 (2011): 5-7.

³⁰ *Ibid.*, 2.

³¹ *Ibid.*

³² Dillow, “Stuxnet Worm Is A ‘Game Changer’ For Global Cybersecurity.”

³³ David E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*, June 1, 2012.

³⁴ *Ibid.*

³⁵ *Ibid.*

³⁶ Chien, Murchu, and Falliere, “W32.Stuxnet Dossier,” *Symantec*.

³⁷ Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*.

“Supreme Cyberspace Council” and was promised \$1 billion for the cyber-warfare program.³⁸ This investment went into the acquisition of new technologies, investments in cyber defense, the creation of a new cadre of cyber experts, investment in technological training in universities, and the creation of Basij, a national intelligence communications network.³⁹ They have run the ‘Cyber Defense Command’ since 2010² and under the Basij Cyber Council, trained 1,500 ‘cyber-warriors’. In 2013 President Hassan Rouhani assumed office, granting the Islamic Revolutionary Guard Corps an annual cybersecurity budget of about 19.8 million US dollars.⁴⁰ According to advisors present in the Situation Room, Obama knew that the United States’ military investment and usage of the cyber domain would cause other countries to engage in a “cyber weapon arms race.”⁴¹

According to Keith Alexander, the head of the National Security Agency and Cyber Command, the need for cybersecurity is immediate as he calls it the “greatest transfer of wealth in human history”.⁴² Alexander estimates that it costs the United States government alone \$340 billion per year.⁴³ Cyber weapons can now cripple enemy states’ infrastructure which before only conventional weapons could accomplish.⁴⁴ In the rapidly advancing world of technology, the increasing need for cybersecurity is becoming apparent.

Iranian Advances

Iran has outsourced the development and strengthening of its cyber security technologies to countries such as North Korea and China.⁴⁵ Iran has separated itself from the global cyberspace, which has helped them to strengthen its defense against cyberattacks and espionage.⁴⁶ The Iranian Internet source, the Halal Internet, has two IP addresses for every computer that is connected. One IP address allows users to connect globally and the other can only be accessed within the country. Iran has created a national cyber protection system called “Shahpad,” which according to the head of the project, Mohammad Naderi, monitors potential attacks across the cyber domain and alerts Iranian security centers of the possible cyber invasions.⁴⁷ The Iranian cyber police, known as FATA, is another effort by the Iranian government to control cyberspace. *The New York Times* reported that FATA has become aggressive when searching for opposition to the government’s positions.⁴⁸ The Army of the Guardians of the Islamic Revolution (IRGC) had been recruiting and training cyber soldiers to spy on protesters and spreading Iranian government propaganda through its Cyber Defense Command.⁴⁹ Iran has created and implemented numerous cyber policies that have greatly improved its ability to attack other nation’s information and infrastructure.

³⁸ Yaakov Katz, “Iran embarks on #1b. Cyber-warfare program,” *The Jerusalem Post*, December 18, 2011.

³⁹ Golnaz Esfandiari, “Basij Members Trained to Conquer Virtual World,” *Payvand Iran News*, August 21, 2010.

⁴⁰ Natasha Bertrand, “Iran is building a non-nuclear threat faster than experts ‘would have ever imagined,’” *Business Insider*, March 27, 2015.

⁴¹ Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*.

⁴² Josh Rogin, “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History,’” *The Foreign Policy Group*, July 9, 2012.

⁴³ Ibid.

⁴⁴ Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*.

⁴⁵ Ibid.

⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ Shafa, “Iran’s Emergence as a Cyber Power,” Strategic Studies Institute.

United States Administrations

The United States has released many cyber-security initiatives in an attempt to reduce the number of global cyber conflicts. *The New York Times* reported that Israel and the United States have become partners in order to combat cyber warfare, specifically attacks from Iran.⁵⁰

The Clinton Administration released a Presidential Decision Directive (PDD) in 1998 with the goal of protecting critical infrastructure. The plan called for the elimination of significant vulnerabilities, a system to identify and prevent attempted attacks, and a plan for alerting, containing, and rebuffing an attack in progress.⁵¹ This plan was followed in 1999 by the Protection of National Security and Public Safety Act, which defined president's power over the export of encryption products.⁵²

The Bush Administration in 2004 developed The National Strategy to Secure Cyberspace, which was a way to protect and combat any direct threats to the "infrastructure that is essential to our economy, security, and way of life".⁵³ President Bush also devised the Comprehensive National Cybersecurity Initiative(CNCI) in order to allow the federal government to take in identifying current and future cyber threats, discovering current and future telecommunications and cyber vulnerabilities and respond to addressing entities that want to steal or manipulate protected data in secured federal systems.⁵⁴ The CNCI is an accumulation of policies that were organized between the Bush administration and the United States Computer Emergency Readiness Team (US-CERT) which is a subdivision to the Department of Homeland Security.

The Obama Administration has developed many initiatives under the Department of Defense Strategy for Operating in Cyberspace to build off on the CNCI, which was launched by President Bush. Strategic Initiative is the concept to treat cyberspace as an operational domain to organize, train, and equip so that the Department of Defense (DoD) can take full advantage of cyber space's potential. Strategic Initiative 2 is to employ new defense operating concepts to protect DoD networks and systems. Strategic Initiatives 3 is to partner with other US government departments and agencies and the private sector to enable a whole-of- government cybersecurity strategy. Strategic Initiatives 4 is to build robust relationships with US allies and international partner to strengthen collective cybersecurity. Lastly, Strategic Initiatives 5 is to leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.⁵⁵ The Cybersecurity Act of 2015 was also passed by Congress during Obama's administration in which establishes the

⁵⁰ David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran", *New York Times*, 2012, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.

⁵¹ Bill Clinton, "Presidential Decision Directives/NSC-63," The White House Washington, 1998, May 22, 1998, <http://fas.org/irp/offdocs/pdd/pdd-63.htm>.

⁵² Ibid.

⁵³ George W. Bush, "The National Strategy to Secure Cyberspace," The White House Washington, 2003, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

⁵⁴ John Rollins and Anna C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," Congressional Research Service, 2009, March 10, 2009, <http://bit.ly/2aj9Shm>.

⁵⁵ "Department of Defense Strategy for Operating in Cyberspace," Department of Defense, 2011, July 2011, <http://csrc.nist.gov/groups/SMA/isfab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.

framework for sharing threatening cybersecurity information between the federal and state government and the private entities.⁵⁶

Despite all policy efforts, both national and international, cyber warfare is still an ongoing problem that needs some sort of relief. Cyber warfare can be traced back to the origins of technology and has a great effect on international relations. However, in this report we have come up with a series of policies that we thought would be best in combating cyberattacks against the US from Iran.

⁵⁶ David J. Bender, "Congress Passes the Cybersecurity Act of 2015," *The National Law Review*, 2015, December 20, 2015, <http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015>.

Legal Considerations

Global Law

The invention and development of a complex cyberspace has opened the international community to a plethora of threats and what some have referred to as “a fifth domain of war-fighting.”⁵⁷ A question that has puzzled the international community is how we can apply existing standards of war to this mostly uncharted domain. There are three main areas of international law that govern cyber warfare; *jus ad bellum* (the right to war), the law of neutrality, and *jus in bello* (the law of armed conflict). First is the principle of *jus ad bellum*. The most specific source of law governing *jus ad bellum*⁵⁸ among the international community today is the UN charter. This charter lacks specific information regarding measures of self defense (see Appendix A). The law of neutrality raises a debate over whether hostile powers can lawfully use “the telecommunications infrastructure of neutral states for the purpose of cyberattacks (see Appendix A)”⁵⁹ and, subsequently, what the role of neutral states must be towards those involved in an attack on infrastructure in a given territory. The law of neutrality is “a fundamental principle of international law that applies whatever type of weapons might be used”.⁶⁰ In *Jus in bello*, often referred to as the International Humanitarian Law (IHL), “cyber warfare must be distinguished from phenomena... such as ‘cyber criminality’ and ‘cyber terrorism’.” However, when IHL does apply, “it must be clarified to what extent its rules and principles... can be transposed to cyber warfare.”⁶¹ This step is crucial as the existing warfare regulations such as IHL have not been adapted to apply to the complexities that exist in cyberspace. Nils Melzer, a participating expert in a process sponsored by the North Atlantic Treaty Organization’s Cooperative Cyber Defence Centre of Excellence, notes that “the fact that cyber warfare is conducted in cyberspace does not exclude that it may produce kinetic or other non-electric effects outside the cyber domain.”⁶² This intertwined nature between virtual and physical harm is what makes clear and specific regulation so difficult.

According to international law, neutrality is a fundamental principle that “applies whatever type of weapons might be used.”⁶³ The principle states that a neutral state is to prevent its territory from usage by belligerents. This traditional war principle has been used to apply to cyberattacks. In return, the belligerents “must respect the inviolability of neutral territory and “are forbidden to move troops, or convoys of either munitions of war or supplies across the territory of a neutral Power.”⁶⁴ Another portion of the study that is of particular relevance to the issue of cyber warfare is that neutral states are “not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals,” as long as it applies the same policy towards all belligerents.”⁶⁵ However, a gap exists in applying this war regulation as a target’s “geographical routing cannot normally be

⁵⁷ United Nations Institute for Disarmament Research. *Cyberwarfare and International Law*. By Nils Melzer.

⁵⁸ This translates to “Right of war” in Latin

⁵⁹ Ibid.

⁶⁰ Ibid.

⁶¹ Ibid.

⁶² Ibid.

⁶³ International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, advisory opinion, 1996, § 89.

⁶⁴ Melzer. United Nations Institute for Disarmament Research. *Cyberwarfare and International Law*.

⁶⁵ Art. 8, Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), 1907.

controlled so as to completely avoid the use of neutral telecommunications infrastructure.”⁶⁶ As a result of this lack of accuracy the question of “whether the information and payloads transmitted by the belligerents through neutral cyber infrastructure constitute actual weapons systems (which would violate the law of neutrality) or mere communication data (which would be permissible)” . The answer to this question fluctuates depending on the exact design and nature of the attack. However, neutral states are obliged to restrict belligerent states from carrying out acts of cyber warfare from within their territory, “but not the routing of belligerent cyber operations through their publicly accessible communications infrastructure.”

Current American Cyberlaw

The current American cyberlaw includes 4 primary pieces of legislation, the first three of which were signed into law on December 18th, 2014. The Cybersecurity Workforce Assessment Act requires the Secretary of Homeland Security to annually assess the cybersecurity workforce of the Department of Homeland Security.⁶⁷ The National Cybersecurity Protection Act of 2014 establishes a center specifically for cybersecurity in the Department of Homeland Security.⁶⁸ The Cybersecurity Enhancement Act of 2014 provided a voluntary public-private partnership aimed at spreading public awareness and education, with a public-private partnership created to enhance research regarding cybersecurity.⁶⁹ The Cybersecurity Act of 2015, the most recent cybersecurity legislation regarding the American government, states that the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Department of Justice all must develop procedures to share cybersecurity information with private and public entities to raise public and private awareness of cybersecurity between branches of government and the American people.

Jus ad Bellum and Jus in Bello

Consistency and predictability are the key to creating a robust set of laws. These two principles, predictability and consistency, allow man to understand the legal ramifications attached to their decisions. In the extraordinarily complex world of cyber warfare, it is especially important to create a law that fits these principles. Cyberlaw which exhibits consistency and predictability will create widespread confidence in states’ security of cyberinformation.

Laws of war have been categorized into jus ad bellum and jus in bello criteria.⁷⁰ Jus ad bellum, or the law relating to force, requires “a competent authority to order the war for a public purpose”, “a just cause”, “the means must be proportionate to the just cause”, “all peaceful alternatives must have been exhausted,” and “a right intention on the part of the just belligerent.”⁷¹ No state has yet claimed a cyber-attack as an “armed attack,” nor have they said it constitutes as a prohibited use of force. Over time, cyberattacks have become much more prevalent and dangerous to national

⁶⁶ Melzer. United Nations Institute for Disarmament Research. *Cyberwarfare and International Law*.

⁶⁷ “Cybersecurity Legislation | Cybercrime Laws | Cyber Security News - ISACA.” *Cybersecurity Legislation | Cybercrime Laws | Cyber Security News - ISACA*, January 6, 2016.

⁶⁸ “S.2519 - 113th Congress (2013-2014): National Cybersecurity Protection Act of 2014.” *Congress.gov*. Sen. Carper, Thomas R. [D-DE], December 18, 2014.

⁶⁹ “Cybersecurity Legislation | Cybercrime Laws | Cyber Security News - ISACA.” *Cybersecurity Legislation | Cybercrime Laws | Cyber Security News*

⁷⁰ Sternstein, Aliya. “Pentagon Contractors Developing Lethal Cyber Weapons.” *NextGov.com*. November 4, 2015. Pg 39-40

⁷¹ Ibid.

security, suggesting countries need to use a universal definition for when cyberattacks constitute as a use of force or armed attack.

Considering cyber warfare is indeed a type of “warfare,” it is critical to use the rules of “jus ad bellum” when determining whether cyber warfare is appropriate or not. The main issue is figuring out and creating a universal definition for when cyberattacks classify as a use of force. The best answer that has emerged is to determine when the effects of a cyber attack are similar to effects that implicate the UN Charter.⁷² A cyber attack which interrupts an air-traffic system, resulting in deaths for example would be considered a use of force. On the other hand, a cyber attack which involves espionage, (the practice of spying in order to obtain political or military information) would not be called a use of force.

The Nicaragua case serves as an example for asserting two key criteria for the right of self-defense. During the Nicaragua Case, the International Court of Justice recognized “necessity” and “proportionality” as requirements for the right to self-defense.⁷³

Necessity relates to the idea of “jus ad bellum” or right to war. In order for there to be true “necessity”, there must be no other way to address the problem. Necessity is determined by the time between the attack and the act of self-defense being short. Additionally, necessity requires taking into account performing negotiations and investigations in this short period of time.

Proportionality suggests that self-defense should be considering the range, duration, and location of the initial armed attack. The term proposes taking into account the intensity of the armed attack (see Appendix A) before using self-defense. Therefore, the inherent problem of cyber-attacks qualifying as self-defense is that it is much more difficult to measure the intensity of computer attack in a way that would be done in a traditional attack.⁷⁴ Cyberattacks are uncertain in the outcome produced, making it impossible to take into account the scale of the damage. Considering it is extraordinarily difficult to measure the ‘proportionality’ of cyberattacks, we suggest that cyber-attacks in self-defense be prohibited.

Tallinn Manual

The Tallinn Manual is an academic, non-binding study on how international law--in particular international humanitarian law--applies to cyber conflicts and cyber-warfare.⁷⁵ A group of experts was brought together in Tallinn, Estonia by North Atlantic Treaty Organization (NATO CCD COE) to address the boundaries and specifics of cyber warfare.⁷⁶ Although useful for many cases, the Tallinn Manual is not enough to define certain acts of cybercrime as cyber-warfare or terrorism.⁷⁷ This is evident in the cases of the Georgian War, the Sony attack, and the Red October Virus that will be elaborated on later, where the exact terminology is still unclear.

⁷² Journal of International Commercial Law & Technology. 2013, Vol. 8 Issue 3, p179-189. 11p.

⁷³ Ibid.

⁷⁴ Journal of International Commercial Law & Technology. 2013, Vol. 8 Issue 3, p179-189. 11p.

⁷⁵ "What Limits Does the Law of War Impose on Cyber Attacks?" - ICRC. June 28, 2013. Accessed July 26, 2016.

⁷⁶ Wolff Heintschel von Heinegg, “The Tallinn Manual and International Cyber Security Law” *Yearbook of International Humanitarian Law* (2012): 1-10

⁷⁷ "Cyber Defence Training." CCDCOE. 2014. Accessed July 26, 2016.

The Manual was created by a team of experts to have a culmination of cyber research as well as cyber defense training. Collaborated on by an international group of lawyers and scholars, the Tallinn Manual was a three year project based off of protocol for air and missile warfare. It uses traditional war forms to help define the “new” form of cyber warfare. The Manual addresses *jus in bello* and *jus ad bellum*, along with the law of neutrality.⁷⁸ Although the manual is not an official international document it is used as a main reference on cybercrime.

According to the manual, any cyber activities that are deemed under the specific level of force described by *jus ad bellum* are not addressed in the Tallinn Manual. The only legality examined is when cyber activities have shown “use of force” or “armed attack” under the *jus ad bellum*’s administration or are considered relevant compared to an armed conflict under the administration of the *jus in bello*.⁷⁹ An example of the manual being consulted for the correct terminology is in 2014 when the former speaker of the House, Newt Gingrich, called an attack on Sony by North Korea an act of war. In order to confirm the legitimacy of Gingrich’s statement, experts referred to the Tallinn Manual and found that the attack did not correlate with the qualifications for cyber warfare.⁸⁰

A current example of the Tallinn Manual’s applicability is in regards to the United States plan for utilizing a cyber weapon against Iran. Before the Iranian Nuclear Deal was achieved, the United States had plans to construct a cyber weapon in order to disable Iran’s infrastructure. The weapon’s mission, named Nitro Zeus was put on hold once the Iranian Nuclear Deal was struck and is not known to have ever been in use. The manual cannot determine whether the weapon is an actual attack, however the manual can provide guidance on whether a weapon is shelved or not. According to the text, a cyber operation may be considered an act of force if it is carried out by the military or a private entity. Nitro Zeus is allegedly under military authority and in conclusion with the Tallinn Manual’s definition of attack, had the weapon been put in use it would be considered an act of war against Iran.

The Tallinn Manual lacks appropriate guidelines for cyber territory. When cyberspace has no concrete borders it is difficult to classify attacks, and which country (or any country at all) should be held accountable for attacks that can’t be proven as government lead. In the case of the Georgian War, several Georgian websites were attacked but no sustainable proof was found confirming a state-sponsored attack.⁸¹ This difficulty regarding classification is also exhibited through the Red October Virus, a virus that obtained classified information from government embassies, agencies, corporations, and military sites in 60 countries over the course of 5 years.⁸² There was no way to find the purpose or origin of this virus which supports the conclusion that although the Tallinn Manual is an extremely useful guideline on cyber conflicts, the UN and the international community need to establish official laws on what is deemed cyber warfare and how to combat cyberattacks.

⁷⁸ Heintschel von Heinegg, “The Tallinn Manual and International Cyber Security Law” *Yearbook of International Humanitarian Law* (2012)

⁷⁹ "Research." CCDCOE. 2014. Accessed July 26, 2016.

⁸⁰ Sanger, David E., and Mark Mazzetti. "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." *The New York Times*. 2016. Accessed July 26, 2016.

⁸¹ Oliver Kessler and Wouter Werner, “Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare” *Leiden Journal of International Law* (2013): 799-801,

⁸² Kessler and Werner, “Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare” *Leiden Journal of International Law* (2013)

Varying Interpretations and Implementations of Cyber Law

Chapter I, Article 2(4) of UN Charter writes, “all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”⁸³ Although the UN’s principles for avoiding conflict declare how countries should not make attacks against the territories of other states, the terminology used in this principle has multiple definitions. This leaves room for interpretation and may allow conflict to arise while technically continuing to follow the UN’s principles. Some hackings do not qualify as attacks that are illegal under UN Charter I, as they do not attack a specific government or territory. However, if hackers are hacking into government information that threatens the privacy of a territory and people, then the hackings break UN Article 2(4). However, some have argued that cyber warfare does not fall within the boundaries of *Jus ad Bellum* or self-defense, unless there are physical attacks being made, and only if the attacks bring as much harm to the country that a non-cyber act of war would bring.⁸⁴

Chapter I, Article 51 of the UN Charter reads, “nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”⁸⁵ Defining cyber warfare as an “armed attack” would allow countries who have been victims of cyber attacks to retaliate against their hacker.⁸⁶ The definition of what qualifies as an “armed attack,” and whether an act of cyber-warfare meets that criteria, determines the appropriate response of hacked countries. Cyber warfare should be defined as an armed attack, as computers can cause as much harm (stealing millions of dollars, hacking into private governmental information, invading the privacy of certain individuals or companies), if not more, than traditional weaponry. Additionally, if an act of cyber warfare results in physical damage, many researchers are more inclined to view that act as an “armed attack.”⁸⁷ If acts of cyber warfare are labelled as “armed attacks,” then according to the UN Article 51, countries are entitled to self-defense. The next area of confusion comes from the uncertainty of what an appropriate response of self-defense is and whether that response should remain online, or be extended to conventional military attacks that cause physical damage.

Researchers Oona A. Hathaway and Rebecca Crootof write that, “states may only use defensive armed force in response to a cyber-attack if the effects of the attack are equivalent to those of a conventional armed attack.”⁸⁸ However, other specialists and government officials insist that in order for countries to defend themselves against cyber-warfare, they must have the ability to do so

⁸³ United Nations, *Charter of the United Nations*, 24 October 1945

⁸⁴ Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aliene Nowlan, William Perdue, Julia Spiegel. “The Law of Cyber-Attack.” *California Law Review* 100, no. 4 (August 2012): 817-85; Schmitt, Michael N. “The Law of Cyber Warfare: Quo Vadis?” *Stanford Law & Policy Review* 25:269-300; Melzer. United Nations Institute for Disarmament Research. *Cyberwarfare and International Law*.

⁸⁵ United Nations, *Charter of the United Nations*, 24 October 1945

⁸⁶ Ibid.

⁸⁷ Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aliene Nowlan, William Perdue, Julia Spiegel. “The Law of Cyber-Attack.” *California Law Review*

⁸⁸ Ibid.

online.⁸⁹ The United States Department of Defense stated in a 2011 report to Congress that the “U.S. military continues to have all necessary capabilities in cyberspace to defend the United States and its interests,” displaying how certain governments defend their nation from cyber-attacks, through launching other acts of warfare online.⁹⁰ As exhibited through the approaches of the US Department of Defense, and researchers Hathaway and Crootof, the criteria of self-defense against a cyber-attack is broad and has much room for confusion and misinterpretation. We propose that acts of self-defense against cyber warfare, are not made online, but through economic sanctions, and military action as a last resort.

The complicated and unstable definitions of “armed attack,” “self-defense,” and “territorial integrity,” exemplify how the appropriate, lawful ways to respond to cyberattacks depend on each individual or government’s interpretation of terms like these. This makes it complicated to have one set of laws that apply to cyber warfare, when different governments and individuals have different interpretations of the terms.

A country’s interpretation of one term could result in an entire unlawful war in terms of the UN’s law. A war that has the potential to take place completely in cyberspace, or extend to the physical territory of another country. Because the weight of this wide range of definitions is so heavy and has the capability in resulting in further conflict, it is vital for all countries to have one set of determined vocabulary and definitions.

Recommendations

One focus now needs to be redirected from creating laws relating to cyber warfare, to creating one shared and agreeable set of definitions in order to clearly identify when cyber activities shift to cyber warfare. Additionally, up until now traditional rules of war have been manipulated to try to apply to this new domain of war. However, the foundation of these regulations are not complex enough to apply to be adapted to the world of cyberspace. We must adopt the guidelines of the Tallinn Manual which are specific to issues of cyber warfare as official law to govern this Fifth Domain. Considering it is impossible to measure the “proportionality” of cyberattacks, we need to prohibit using cyber warfare in self defense. Instead of using cyber attacks in self defense, we suggest it is appropriate to place economic sanctions on countries that perform cyberattacks. If economic sanctions still do not prevent nations from these continued acts of aggression, military force shall be called for as a last resort, and only if approved by the UN.

- Need for one universally accepted set of definitions for different cyber warfare terms. This will avoid misinterpretation of terms such as “armed attack” and “self-defense”
- Adopt Tallinn Manual as official, universal guidelines, rather than just a reference source
- Prohibit using cyber warfare as means of self-defense. Turn to economic sanctions first, then the military if necessary. However, to use military forces for self-defense, must get approved by UN

⁸⁹ United States. Department of Defense. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Washington, D.C.: U.S. Dept. of Defense, November, 2011. 2.

⁹⁰ Ibid.

United Nations and the International Community

In recent years, cyber warfare has afflicted the international community. Iran has grown especially threatening as it continues to develop its cyber arsenal. International organizations have failed to resolve and sufficiently analyze many cyberattacks, never truly establishing a precedent for future conflicts. Due to the lack of a consultative framework and the extensive spectrum of cyber warfare, there is a need for precise policy initiatives and regulations. To create this policy, we have specifically looked to NATO's response to the Russian cyberattack of Estonia's infrastructure in 2007, the Stuxnet virus that infiltrated Iranian nuclear facilities in 2009, and the hack of Saudi Arabia's Aramco oil company in 2012. Each of these global conflicts highlights both the shortcomings and the success of the international community's response to cyber warfare and provides possible solutions for the situation in Iran.

Cases: Russia, Estonia, and NATO

In 2007, Estonia experienced "denial-of-service" attacks by Russia as a protest against the Estonian government's removal of the Bronze Soldier monument, a Soviet war monument erected in 1947. Targeted websites received over 4 million incoming packets of information per second. According to the European Institute, "it was the first time that a sustained, wholesale and politically motivated e-assault was launched to wreak havoc on a country's entire digital infrastructure."⁹¹ One NATO senior official commented, "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?"⁹² NATO assisted the Estonian government in diminishing the damage caused by the cyber attack. Additionally, NATO passed legislation to create the Co-operative Cyber Defense Center of Excellence (CCD COE) in Tallinn, the capital. The purpose of this Center was to provide a "standard protocol for responding to a cyberattack" and guide cyberwar response research.⁹³

The cyberattack on Estonia provides important insight on how to deal with Iranian cyber warfare. In the aftermath of the attack, NATO responded effectively and immediately, helping to restore Estonia's critical infrastructure. If Iran carries out an attack of the same caliber as the Russian attack, NATO should respond with similar support. NATO's introduction of legislation as a response to the attack was an effective decision. To respond to any future instances of Iranian cyber warfare, specific legislation should be created to deal with particular threats. Furthermore, NATO's denunciation of Russia was another successful deterrent of further cyberattacks. Should Iran initiate cyber warfare with any country in NATO, we would encourage NATO to make a similar denunciation of Iran. Yet, if the cyberattacks continue and become more destructive, we would ask NATO members to impose economic sanctions and possibly take military action. While the international community responded adequately to the attacks in Estonia, conversations about cyber warfare between Estonia and Russia should have occurred more often, both before and during the attacks on Estonia. Thus, we propose that both the United Nations and NATO establish direct lines of communication with Iran concerning cyber warfare issues.

⁹¹ Ruus, Kertu, "Cyber War I: Estonia Attacked from Russia." *The European Institute*, Last modified 2007. <http://bit.ly/2aetUzC>.

⁹² Anonymous post to The Economist newsgroup, "Cyber-riot," May 10, 2007. Accessed. July 26, 2016. <http://www.economist.com/node/9163598>.

⁹³ Ibid.

Stuxnet

In 2009, Israeli and United States intelligence joined forces to launch the Stuxnet virus to target Iranian nuclear facilities. The virus, which corrupted thousands of centrifuges in Iranian nuclear reactors, covered up its tracks so that Iranian authorities were unable to identify anything out of the ordinary. Although the Stuxnet attack illustrated the advantages of collaboration among global cyber powers (see Appendix A) like the United States and Israel, the attack also initiated a worldwide escalation of cyber programming. In fact, twenty nations have introduced cyber warfare programs since the uncovering of Stuxnet.⁹⁴ According to Kim Zetter, author of *Countdown to Zero Day*, the Stuxnet virus has set off a mass espionage network around the world as 100,000 systems were corrupted.⁹⁵ Furthermore, the attacks signified the cyberpower's loss of any sort of "moral ground for demanding other countries not [to] use cyber warfare techniques."⁹⁶ Christopher Dickey, author of "The Shadow War," claimed that the virus was not intended to reach beyond those computers it directly affected and that it was meant to expire, or "self-destruct," within a limited period of time.⁹⁷ The Stuxnet virus failed to do either, it appears, and thus highlights the importance of regulating more strictly the dissemination of cyber warfare techniques. Indeed, Stuxnet was the "start of a new era," said Stewart Baker, former general counsel of the U.S. National Security Agency,⁹⁸ and Iran may very well be considered "the first true victim of cyber warfare."⁹⁹

By examining the consequences of the Stuxnet attack, the international community can learn from its mistakes and its successes. First, it is important to understand the critical role that Stuxnet played in delaying the emergence of Iran as a veritable nuclear threat—at which point Israel would have most likely launched a military strike on Iran.¹⁰⁰ Indeed, then-Secretary of State Hillary Clinton acknowledged that the attack set Iran's nuclear program back "several years."¹⁰¹ In this way, cyber warfare, when waged strategically and collaboratively, can act as a vehicle for sustaining world peace and security—as is the goal of the United Nations Security Council—by delaying armed conflict and indirectly promoting diplomacy. On the other hand, Stuxnet served as a catalyst for Iran's build-up of its cyber arsenal. In fact, Iran increased its budget for cyber weapons 1,200 percent in the three years following the Stuxnet attack.¹⁰² Barbara Slavin, a Senior Fellow in the Atlantic Council's South Asia Center, acknowledged that "we have learned from Stuxnet that there are consequences to our actions and that we should be very careful before we attack the infrastructure of other countries because they have an ability to respond...Iran's response to Stuxnet cost millions of dollars to our financial sector and presumably they could wreak worse havoc if provoked."¹⁰³

⁹⁴ "Phil's Stock World: Cyberwarfare Threat To Nuclear, Banking and Financial System," *Phil's Stock World* (blog), entry posted June 13, 2015, accessed July 25, 2016, <http://bit.ly/2a9Tb8D>.

⁹⁵ Ibid.

⁹⁶ Ibid.

⁹⁷ Christopher Dickey, "The Shadow War," *Newsweek*, December 20, 2010, accessed July 25, 2016, <http://proxygw.wrlc.org/login?url=http://search.proquest.com/docview/817285670?accountid=11243>.

⁹⁸ Ibid.

⁹⁹ Nicholas C. Reuter, "The Cybersecurity Dilemma" (master's thesis, Duke University, 2011), 19, accessed July 25, 2016, ProQuest.

¹⁰⁰ Ibid.

¹⁰¹ "Israel's Dimona Nuclear Facility Splits Time as Cyberweapon Testing Ground CyberWarfare," *Gizmodo* (blog), entry posted January 16, 2011, accessed July 25, 2016, <http://bit.ly/2a92Mz8>.

¹⁰² Ashish Kumar Sen, "Iran's Growing Cyber Capabilities in a Post-Stuxnet Era," Atlantic Council, April 10 2015 <http://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era>.

¹⁰³ Ibid.

Ultimately, what makes the Iranian case so threatening is that its cyber program is inextricably bound to its nuclear program. Given the consequences of the Stuxnet attack, we suggest that global cyber powers like Israel and the United States communicate first with other cyber nations to ensure that the attack is as targeted as possible in order to minimize the negative repercussions to unintended parties. Furthermore, we would've encouraged and continue to encourage--that global powers like the US and Israel deliver a threat before acting according to our three step plan.

Attacks on Saudi Aramco

In 2012, the hackers "Cutting Sword of Justice" attacked Saudi Aramco, supplier of 10% of the world's oil, when a member of Aramco's technology team opened a scam message, leaking the Shamoon virus into their network. The group forced Saudi Aramco into complete turmoil, severely hindering its productivity and basic technological use. The company was forced to use aged equipment, withhold the sale of oil to domestic gas trucks, and struggled to maintain success within its subsidiary offices in neighboring countries.¹⁰⁴ Fortunately, the cyberattack did not affect the systems that drive the technical operations of Aramco and its oil output; however, 30,000 office computers were infiltrated.¹⁰⁵ Although there were no serious threats to the infrastructure of Saudi Arabia and its neighboring countries, the incident convinced Aramco to impose stricter security measures on different services worldwide. Because Iran poses evident threats towards Saudi Arabian petroleum, global nations must be knowledgeable of cyber warfare capabilities and propose stricter cybersecurity policies, knowing that Iran has the capabilities and cyber resources to severely damage other societies.¹⁰⁶ Due to present tensions between the two nations today, Iran may continue to wage cyberattacks on Saudi Arabia. Only by monitoring Iranian cyber activity will the international community ensure that another Shamoon will not corrupt a corporation in the near future.

Unlike the Saudi's limited communication with global cyber powers during their investigation of the Aramco attack, the international community ought to promote transparency when dealing with Iranian cyber warfare. Following the hack, Saudi Aramco and the Saudi Ministry of Interior worked together to investigate the causes and the consequences of the attack. However, perhaps in an attempt to preserve Aramco's reputation and to "prevent any potential further escalation" by the cyber attacker, the investigation was kept private and the findings were not released to the international community. Furthermore, the incident was handled as a domestic affair despite the fact that the ministry claimed the hack "originated from several other countries."¹⁰⁷ In this way, the Saudi's response to the cyberattack limited crucial communication between global cyber powers that could have helped in the investigation as well as in establishing a stronger defense against cyberattacks in the future. By establishing channels between computer emergency response teams (CERTs), the international community can better respond to crises concerning Iran in the future. Transparency will speed up the process of attribution and reduce the risk of blaming the wrong group or individual, thus avoiding a potential escalation. In both the case of Saudi Aramco and the

¹⁰⁴ Jose Pagliery, "The Inside Story of the Biggest Hack in History," CNNMoney, last modified August 5, 2015, accessed July 27, 2016, <http://money.cnn.com/2015/08/05/technology/aramco-hack/>.

¹⁰⁵ Sico Van der Meer, *Foreign Policy Responses to International Cyber-attacks: Some Lessons Learned*, September 2015, accessed July 27, 2016, <http://bit.ly/2avW6My>.

¹⁰⁶ Christopher Bronk and Eneken Tikk-Ringas, *Hack or Attack? Shamoon and the Evolution of Cyber Conflict*, February 1, 2013, accessed July 27, 2016, <http://bit.ly/1jtKh3o>.

¹⁰⁷ Van der Meer, *Foreign Policy Responses to International*.

Stuxnet virus, neither Iran nor the United States formally claimed responsibility for the attack. This fact brings into light the difficult question of attribution. In response to a cyberattack, the first responsibility of the international community is to determine the perpetrator. By reducing the risk of wrongfully accusing a nation of waging cyber attack, we limit conflict and tension and the possibility of small cyberattacks escalating into cyber warfare.¹⁰⁸ With the escalating arms race between Israel and Iran emerging as a “cold war of cyber,”¹⁰⁹ the international community must keep a very close eye on both sides, with Israeli allies communicating as much as possible with the Israeli cyber team. The United Nations agency, International Telecommunication Union, has worked to forge global partnerships and encourage projects that strive to “create a safe and secure cyber environment for everyone.”¹¹⁰

Criteria

Based on these three cases, we have determined that, in order to protect the international community from cyber warfare, individual nations should respond to Iranian cyber warfare by collaborating with the United Nations and NATO. The response of these international organizations to Iranian cyber warfare should follow a three-step procedure. This strategy speaks to two main ideas, one based upon expanding communication and the other built to deter severe damage from these attacks. The first step in our three-step international action plan is to “Talk”. Allies such as Israel and the United States should enhance and expand existing lines of communication as well as establish new ones when dealing with Iranian cyber warfare. In addition, we encourage Iran to develop similar channels of communication, such as direct conversation with international organizations such as the United Nations and NATO. Finally, we encourage developing even more channels to connect governments and state-sponsored private entities in the case that government cyber capabilities are compromised. The next step in our action plan is to “Threat.” The U.N. and NATO should threaten Iran with economic sanctions and military action if Iran continues to wage cyber warfare that is detrimental to the targeted nation’s national security. Our final step is to “Act”. If Iran continues to wage cyber warfare, the U.N. should first impose economic sanctions, to be determined by the severity of the attacks, as mentioned in the “Threat” phase. The economic sanctions are to be set by the United Nations members. However, if the attacks destroy infrastructure in any nation belonging to the U.N., the targeted nation is allowed to declare war on the country or organization who initiated the attacks. The Tallinn Manual claimed that the infrastructure of any nation is that nation’s sovereign land. Destroying a nation’s sovereign land, even by cyber warfare, classifies as an act of war.¹¹¹ While the attacked country is by no means obligated to declare war, they would not be persecuted by the international community for doing so. Additionally, should the targeted nation declare war, no other U.N. nations are required to join a coalition with the targeted nation.

¹⁰⁸ Detlev Wolter, "The UN Takes a Big Step Forward on Cybersecurity," Arms Control Association, accessed July 27, 2016, <http://bit.ly/2ao8ajn>.

¹⁰⁹ Cory Bennett, "Israel, Iran Locked in Escalating Cyber War," The Hill, last modified March 4, 2015, accessed July 27, 2016, <http://bit.ly/2ad3LRT>.

¹¹⁰ Hamadoun I. Touré, "International Telecommunication Union Cybersecurity Overview," United Nations, accessed July 27, 2016, http://www.un.org/en/ecosoc/cybersecurity/itu_cybersecurity_overview.pdf.

¹¹¹ Wolff Heintschel von Heinegg, "The Tallinn Manual and International Cyber Security Law" *Yearbook of International Humanitarian Law* (2012): 16

Rebuttal

Some would argue that our three-step action plan will not effectively diffuse future cyber warfare conflicts. It could be said that our first step, setting up lines of communication between cyber warring nations, will be impossible in some cases. For example, it could be argued that Israel and Iran will never collaborate on such an intimate level. While it might be hard to convince nations with strained relations to work together, there are methods that the international community could employ to establish discussion as the primary means of dealing with cyber warfare. To deal with these challenges to diplomacy, the international community should present the consequences of not working together on cyber issues in a very specific way. Similar to the detente of nuclear tensions between Russia and the United States in the 1960s and '70s, we hope to persuade cyber warring nations to make peace by warning them that their activities could escalate and lead to mutual destruction. Many analysts have recognized the benefits that this method of deterrence could have for the international community.¹¹² Building off of this idea of mutually-assured destruction, Matthew D. Crosston of Bellevue University noted that “it is logically more stable and potentially peaceful to have a system of deterrence that is structured mutually across major powers, giving no one state the ability to disrupt cyber equilibrium.”¹¹³ Iran’s fear of losing critical infrastructure to cyber warfare will hopefully convince them to set up direct lines of communication to establish peace and to accept the help of the international community.

Other people might also argue that the second step in our three-pronged action plan, to threaten the aggressor nation with economic sanctions regulated by the United Nations and a military coalition force response, will only heighten tensions. Yet, following the cyberattacks on Estonia’s infrastructure in 2007, top NATO officials used aggressive language, some questioning if Russia’s attacks were an act of war. This forceful response terminated Russia’s cyberactivities and prevented Estonia from suffering further damage. When organizations that represent the international community denounce the acts of certain nations’ use of cyber warfare, their words hold incredible weight. The aggressor’s fear that it might face a coalition force is usually enough to prevent them from launching more cyber warfare attacks.

Finally, it could be said that the final step in our international response plan, to act on the threats articulated in step two, would be a severe overreaction. Yet, in recent years, when countries have experienced major attacks on critical infrastructure, the international community has never responded with enough force to discourage attacks in the future. In 2011, Gordon M. Snow, Assistant Director of the Cyber Division of the FBI, stated before the Senate Judiciary Committee, “The FBI’s statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation-states, and terrorists”.¹¹⁴ In 2015, however, the United States government alone experienced 77,000 cyberattacks, clearly showing that the FBI’s policy of

¹¹² Lenny Zeltser, "Mutually-Assured Destruction as a Factor in Cyber Warfare," Lenny Zeltser, last modified February 20, 2015, accessed July 27, 2016, <https://zeltser.com/mutually-assured-destruction-in-cyberspace/>.

¹¹³ Matthew D. Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly*, Spring 2011, accessed July 27, 2016, <http://bit.ly/2a10BQ1>.

¹¹⁴ *Crime and Terrorism: Hearings Before the Judiciary Committee*, 112th Cong., 1st Sess. (2011) (statement of Gordon M. Snow). Accessed July 27, 2016. <http://bit.ly/2arMSQg>.

investigation, collection, and dissemination of intelligence was proving ineffective.¹¹⁵ This lesson can be applied to the broader narrative to understand that severe threats and decisive action are the only ways to deter the most determined cyber-attackers.

Recommendations

- Individual nations should respond to Iranian cyber warfare by working with organizations like the United Nations and NATO
- The United Nations and NATO's responses to specific instances of Iranian cyber warfare should adhere to a three-step policy
 - Talk - Allies such as Israel and the United States should enhance and expand existing lines of communication as well as establish new ones when dealing with Iranian cyber warfare. In addition, we encourage Iran to develop similar channels of communication with international organizations such as the U.N. and NATO. Finally, we encourage developing even more channels to connect governments and state-sponsored private entities in the case that government cyber capabilities are compromised.
 - Threat - The U.N and NATO should threaten Iran with economic sanctions and military action if Iran continues to wage cyber warfare.
 - Act - If dramatic Iranian cyberattacks persist, the U.N. should impose economic sanctions as threatened in Step Two. If the attacks destroy infrastructure in any nation belonging to the U.N., a declaration of war is justifiable.
 - In the case where military action is needed, no other U.N. nations are required to join a coalition with the targeted nation
 - According to the Wall Street Journal, the Pentagon does consider cyber threats "acts of war" and allows the use of "military force" when the attack causes the "death, damage, destruction, or high-level disruption that a typical military attack would cause."¹¹⁶

¹¹⁵ Alistair Bell, ed., "Number of U.S. Government 'Cyber Incidents' Jumps in 2015," Reuters, last modified March 21, 2016, accessed July 27, 2016, <http://www.reuters.com/article/us-usa-cyber-idUSKCN0WN263>.

¹¹⁶ Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal* (New York, NY), May 31, 2011, accessed July 27, 2016, <http://on.wsj.com/1OYTjaR>.

US Government State and Defense

Obama Administration

In 2015, the Department of Defense (DoD) released a cyber strategy which explicitly lays out five strategic goals.

Strategic Goal I is to “build and maintain ready forces and capabilities to conduct cyberspace operations.”¹¹⁷ The DoD says in order to do this we must first create a “cyber mission force”¹¹⁸ and a cyber workforce. Within this workforce they are focused on recruiting civilian and military agents. They are focused on enhancing cybersecurity and cyberspace education in addition to training.¹¹⁹ Through this they aim to foster career paths towards cyber operations. The DoD also says that we must have larger technical capabilities in order to carry out cyber operations. To do this, we must speed up the development and research process to create a “unified platform”¹²⁰ Under this goal they acknowledge and state the need to refine their command and control their policy to establish regular effectiveness.

Strategic Goal II is to “defend the DoD information network, secure DoD data and mitigate risks to DoD missions.”¹²¹ In order to fulfill this goal, the DoD is looking to “build the joint information environment (JIE) single security architecture”¹²² and continuously assess the Joint Force Headquarters and our current DoD Computer Network Defense Service Provider (CNDSP) for effectiveness. In addition they will assess our defensive cyber forces. In order to secure data, the DoD says they need to “mitigate known vulnerabilities” and plan for a defense and resilience plan, and that every action should encompass a cyber red team.¹²³ The red team tests systems in order to figure out their vulnerabilities and weaknesses. The DoD authorizes the use of counterintelligence to defend our nation against intrusions and to counter “intellectual property theft.”¹²⁴

Strategic Goal III is to “be prepared to defend the U.S Homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence.”¹²⁵ In order to achieve this goal, the DoD recommends intervention before the cyberattacks happen. They will prepare to carry out cyber operations in order to defend our nation and in addition will practice emergency actions. In order to defend the nation from serious consequence the DoD will work with other organizations to achieve nation wide safety from cyber threats. In addition they promise to create creative ways to

¹¹⁷ Department of Defense, *The Department of Defense Cyber Strategy*, by Ashton Carter (Washington, DC: GPO, 2015), 15 accessed July 27, 2016, <http://bit.ly/2aa6Spz>.

¹¹⁸ Ibid.

¹¹⁹ Ibid.

¹²⁰ Ibid.

¹²¹ Ibid.

¹²² Ibid.

¹²³ Ibid.

¹²⁴ Ibid.

¹²⁵ Ibid.

defend our critical infrastructure and develop ways to share information between private sectors and the US government. The DoD will assess their strategy and cyber prevention policy.

Strategic Goal IV is to “build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.”¹²⁶ To do this the DoD has to include cyber choices in combatant.

Strategic goal V is “build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.”¹²⁷ A more detailed description of the US’s policy relating to international alliances in combating cyber warfare is included in the international section.

Though this cyber strategy under Obama’s administration is intricate, they do not address some of the key aspects that will protect our nation, therefore we are suggesting to expand these. Cyber hacking skill sets are scarce and the DoD does not have an explicit plan to encourage more people to develop these skill sets, so we will suggest ways to tack this.¹²⁸ In addition the interconnected world of today presents both great promise and great danger. How the U.S. government responds to cyber warfare attacks is vital to security and the lasting prosperity of our digital infrastructure. Our current US initiatives have promised a response, and more specifically we are suggesting to refine and lay out policies to protect America’s national economic and public safety. On a non-federal level, certain states have specific cyber strategy plans but most don’t. We suggest a federal mandate that brings all the states to a baseline in plans, in case of attack.

Public School Proposal: Making CS a Core Requirement

Since 2005, the number AP Computer Science classes have fallen by 33% in a time when business’ and government are calling for a more advanced understanding of coding.¹²⁹ In 2011, data showed that out of the 42,000 high schools in the US, only 2,100 schools were certified to teach this advanced course, and roughly 21,139 students physically took the AP exam. The public schooling systems such as those in Chicago have now made it a core requirement of high school students to take Computer Science.¹³⁰ Since the 1990s, student participation in all STEM (science, technology, engineering, and math) courses have increased except for computer science, which has dropped 25% to 19%.¹³¹

In order to make this essential course mandatory, the United States government must implement law stressing its importance and work to build it into the core curriculum in the US public school

¹²⁶ Ibid.

¹²⁷ Ibid.

¹²⁸ Lara Schmidt, “Perspective on 2015 DoD Cyber Strategy”, Rand Corporation, September 29 2015 Schmidt

¹²⁹ “Code.org Advocacy Coalition,” Code.org, accessed July 27, 2016, <https://code.org/advocacy>.

¹³⁰ Jeff Meisner, *A National Talent Strategy*, December 3, 2012, accessed July 27, 2016, <https://news.microsoft.com/download/presskits/citizenship/MSNTS.pdf>.

¹³¹ Nord, C., Hicks, L., Hoover, K., Jones, M., Lin, A., Lyons, M., Perkins, R., Roey, S., Rust, K., and Sickles, D. (2011). *The 2009 High School Transcript Study User’s Guide* (NCES 2011–465). U.S. Department of Education, National Center for Education Statistics. Washington, DC: U.S. Government Printing Office.

system. Core science classes include Biology, Chemistry, and Physics, but since there are four years of high school, implementing a fourth requirement to the sciences works logistically and would allow students to broaden their future job opportunities.

Not only do we stress the implementation of computer science in public schools, we also stress the importance to get more women and people of color pursuing computer science. According to NPR as of 2012 only 17% of women majored in a field of computer science.¹³² By 2020, there will be 1.4 million jobs available in computing related fields, but women are on track to fill only 3% of them. The gap becomes even bigger when race is factored in. Top universities report that black and hispanic computer science majors graduate at twice the rate that top technology companies hire them,¹³³ which causes a significant amount of underrepresentation of women and people of color in computer science. And if a significant amount of our population does not want to join the computer science industry, then the government's cyber hacking and cybersecurity industry will be missing out on a large portion of potential workers. Furthermore we suggest the government encourage more representation of the American people and narrow the gender and racial gap through subsidizing non profit programs. For example some of these programs include Girls Who Code, Code For Progress, and other programs who promote this representation will also receive subsidizing. In addition to subsidizing these programs, they should be included in the creation of the basic computer science curriculum to ensure coding is built to support all people. The White House released a Cybersecurity Research and Development plan in February of 2016 making this same request. Their 5th recommendation was to expand diversity in the cybersecurity workplace; making it a priority in the development of cybersecurity in the United States. The report claimed that “reframing the image of a cyber professional to be a more inclusive one would increase the talent pool, foster critical cyber skills among a wider swath of individuals, promote a healthier, more culturally-sensitive workplace”, and create “a more diverse workforce can provide a richer set of perspectives and innovative solutions to problems.”¹³⁴ We believe more resources and attention should be placed on this important issue.

United States Government Response to Cyberattacks

A response from the U.S. government to any malicious cyber attack will consist of three initiatives. Firstly, the U.S. government departments should increase budgetary spending towards cyber security by cutting indiscretionary spending. Secondly, the U.S. government will not tolerate cyber attacks nor be a bystander, and if attacked there will be direct retaliation. Finally, the U.S. would institute economic sanctions on countries who directly sponsor a cyber attack. The purpose of these initiatives is to plan, develop, and use U.S. capabilities effectively to ensure that cyber operations occur in a manner consistent with the values that the United States promotes domestically and internationally.¹³⁵

¹³² "Code.org Advocacy Coalition," Code.org, accessed July 27, 2016, <https://code.org/advocacy>.

¹³³ Elizabeth Weise and Jessica Guynn, "Tech Jobs: Minorities Have Degrees, but Don't Get Hired," *USA Today*, last modified October 13, 2014, accessed July 27, 2016, <http://usat.ly/1nikhzzq>.

¹³⁴ Networking and Information Technology Research and Development Program (U.S.), Federal Cybersecurity Research and Development Strategic Plan. Washington, D.C.: Executive Office of the President, 2016.

¹³⁵ Department of Defense, *The Department of Defense*.

U.S. government departments are inherently vulnerable to cyberattacks from anyone, due to disproportionate funding for cybersecurity. "In fact, only the Department of Homeland Security spent more than 3% of its 2014 budget on cybersecurity," said the Business Insider.¹³⁶ The Office of Personnel Management (OPM) invested the least amount of its budget towards cybersecurity compared to other executive departments. Since then, it has suffered the biggest US agency breach to date. Today, only 11 out of 15 federal departments are invested in cybersecurity, but a majority of those 11 companies investment only 1% of their budget to cybersecurity.¹³⁷ We propose that the U.S. government emphasizes a shift from the indiscretionary spending to cybersecurity. Ryan Alexander of Taxpayers for Common Sense reported that "we could save more than \$3 billion by permanently cancelling the expansion of the chemistry and metallurgy research replacement facility in New Mexico."¹³⁸ Additionally, the department of defense continues to invest in fighter jets, an outdated practice that could be modernized towards cybersecurity. Recent research by the department of defense has estimated the amount of money saved by these cutbacks over 10 years to be around \$89 billion.¹³⁹ The money saved in canceling these operations should be used for cybersecurity funding as the result of underfunding cybersecurity could result in an opportunity for a cyberattack.

Second, the DoD must be capable of adapting to challenging environments where cyberspace is contested and retaliatory.¹⁴⁰ Cyberattacks are assessed on a case-by-case and fact specific basis by the President and the U.S. national security team. If the Secretary of Defense approves of a preventive attack or another defensive maneuver, the U.S. military is authorized to conduct cyber operations with counterintelligence to protect the American people. If the President and the Secretary of Defense approve of an attack, the U.S. military is authorized to conduct cyber operations to counter an imminent or ongoing attack against the U.S. homeland or U.S. interests in cyberspace.

The final recommendation for the U.S. government is for the ratification of the usage of economic sanctions on state perpetrated cyber warfare. Currently the UN guidelines for economic sanctions are attacks that: "Harm or compromise a critical infrastructure sector, disrupt the availability of a computer or network or computers," cause "significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain."¹⁴¹ Sanctions may also be imposed on anyone who knowingly receives or uses trade secrets acquired via cyber theft, when the theft is "reasonably likely to result" in a threat to the nation's security or economic health.¹⁴² These guidelines should be used within the United States to determine sanctions. Sanctions will only be enforced on sovereign nations, as that is the most effective use of this specific technique outside of UN channels.

¹³⁶ Bob Bryan, "The US Government is not Spending Enough on Cybersecurity," Business Insider, last modified September 3, 2015, accessed July 27, 2016, <http://read.bi/2a03DE1>.

¹³⁷ Ibid.

¹³⁸ Ryan Alexander, "Start Cutting Government Spending with the Defense Budget," last modified January 6, 2013, accessed July 27, 2016, <http://bit.ly/2ak3lX7>.

¹³⁹ Friedman, Benjamin, and Christopher Preble. "A Plan to Cut Military Spending." Downsizing the Federal Government. Accessed July 29, 2016. <http://www.downsizinggovernment.org/defense/plan-cut-military-spending>.

¹⁴⁰ Department of Defense, *The Department of Defense*.

¹⁴¹ Justin Volz, "Obama Expands the US Response to Cyber Attacks," editorial, Defense One, last modified April 1, 2015, accessed July 27, 2016, <http://bit.ly/2auPaiF>.

¹⁴² Ibid.

Economic sanctions will restrict the following:

- (1) Trade
 - (a) Prohibitions on Iranian exports of arms, dual-use goods, and/or goods that could be used in enrichment-related activities.
- (2) An asset freeze directly imposed on an entity/person employed by the state
- (3) The restriction of the financial sector
 - (a) Freezing the assets of the Central Bank of Iran, and dominant Iranian banks

The order allows for sanctions against actors, even if the cyberattack is not successful.

If an attack is conducted by a rogue group, terrorist organization, or a non-state actor, our response will be to hack back immediately. Imposing sanctions would require recognition of the actors as important and worthy of attention, and would legitimize their organization. Additionally, any identified parties will be banned from the United States, and a push will be made to force their countries of origin to persecute them.

Cyber Readiness Among States

Above, the actions for the federal government were described, but cyberattacks big and small are often first handled by the states. State governments are scattered in their cybersecurity, leaving many prone to attack. The federal government needs to impose a baseline readiness in order to protect the citizens of this country. Critical infrastructure is under fire domestically and internationally, as shown by the Iranian hack of a small dam in upstate New York. There have been reports of Iran hacking into electric grids in order to gather information that if utilized could inflict major damage.

Cybersecurity in most states has not kept up with advances in cyber threats. Because this and the growing threats to infrastructure in an unstable world with an increasing reliance on technology, the federal government must raise the standard of cybersecurity for each state.

The process of protecting state infrastructure has already begun in many states, providing guidelines for future action. A Pell Center report¹⁴³ found that California, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington are leaders in cybersecurity techniques. They identified 3 policies that have been beneficial in stopping cyberattacks— policies which we believe should be enforced on a national level. These policies are as follows:

1. Create a cybersecurity strategic plan
2. Give law enforcement the tools to deal with cyberattacks
3. Create an information sharing hub for each state concerning cybersecurity

A cybersecurity strategic plan should detail how each state will deal with different tiers of cyberattacks. The National Institute of Standards and Technology (NIST) has released a “Framework for Improving Critical Infrastructure Cybersecurity”¹⁴⁴ in response to President Obama’s Executive Order 13636. The latest handbook specifically concerning cybersecurity and infrastructure was released in 2014, but the President released another executive order in February

¹⁴³ Francesca Spidalieri, *State of the States on Cybersecurity*, November 2015, accessed July 27, 2016, <http://bit.ly/2ai87lz>.

¹⁴⁴ National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. February 12, 2014. Accessed July 27, 2016.

of 2016 to create a new framework on enhancing national cybersecurity.¹⁴⁵ The handbook details the necessary setup of a plan to respond to a cyber attack. A state must be able to identify the attack, protect their infrastructure, detect attacks, respond to attacks, and recover information. How to do these things are detailed in the framework, though each state can respond according to its needs and budget.

Law enforcement must have a greater grasp on cybersecurity to protect the people from cyber threats the same way they protect the people from threats in the non-virtual world. Much of this will be remedied by mandatory computer science courses, but there must also be specific training for law enforcement personnel. Since 2013, there have been cyberattacks on police departments in at least 7 states.¹⁴⁶ The Department of Homeland Security has released a document on cyber incident reporting, with a section for training resources, but these resources are obscure initiatives.¹⁴⁷ Dr. Andy Ozmant, the DHS assistant secretary for cybersecurity and communications, said "It's really important for people to know [that] we can help," implying that the state governments he was addressing don't know there are resources for them to use.¹⁴⁸ These resources should be an integral part of the police force. According to The International Securities Exchange (ISE) there are only 7 no-cost federally sponsored cyber crime training programs in the country.¹⁴⁹ This is not enough to

¹⁴⁵ The White House, "Commission on Enhancing National Cybersecurity," *Federal Register*, February 12, 2016, accessed July 27, 2016, <http://bit.ly/2afvPQu>.

¹⁴⁶ Francescani, Chria. "Ransomware Hackers Are Targeting US Police Departments." CNBC. April 26, 2016. Accessed July 28, 2016. <http://www.cnbc.com/2016/04/26/ransomware-hackers-blackmail-us-police-departments.html>.

¹⁴⁷ Department of Homeland Security, comp., *Law Enforcement Cyber Incident Reporting* (Washington, DC: Department of Homeland Security, 2015), accessed July 27, 2016, <http://bit.ly/2avaNjb>.

¹⁴⁸ Francescani, "Ransomware Hackers Are Targeting US Police Departments." CNBC.

¹⁴⁹ "Cybercrime Training for Law Enforcement," *A Call to Action: Equipping Law Enforcement With the Tools to Investigate Cybercrime*, accessed July 27, 2016, <http://bit.ly/2ansM7U>.

provide cybersecurity services to every police station in the country. Additionally, police computers in many areas are ancient, leaving the people meant to protect us open to be attacked themselves. We must increase training accessibility and provide grants for laptop upgrades within police departments.

There are a few aspects of an information hub that need to be created to increase the state's ability to communicate with constituents, in state agencies, and federal agencies, particularly the Department of Homeland Security.

To communicate with constituents, each state should have an official website that lays out the latest cyber threats and ways to keep cyber-secure. The state of California has started to make this information available through the California Department of Technology website, and though there is room for improvement in terms of display, the base exists for other states to follow their example. They have moved forward with the help of a non-profit called the Center for Internet Security. This site is being used in some way by all 50 states and the District of Columbia, so the infrastructure is all there.¹⁵⁰ Within the Department of Homeland Security there is a department called the National

¹⁵⁰ "MS-ISAC MEMBERS," Center for Internet Security, accessed July 27, 2016, <https://msisac.cisecurity.org/members/index.cfm>.

Cybersecurity and Communications Integration Center (NCCIC), which aims to create a place with shared information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations.¹⁵¹ More information on the NCCIC is in the business section. This should continue to be utilized and should be provided with more funding to help state to federal government communication.

Additionally, all states should have Fusion Centers. There are states with fusion centers, but their expansion is vital to information sharing with the federal government. Fusion centers “operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners.”¹⁵² Once all states have these centers specifically relating to cybersecurity, the National Network of Fusion Centers (National Network) can take all the information and use it to protect more accurately against cyber warfare from Iran and other countries. These sharing mechanisms can all be supported by the federal government under sections 2 through 6 of Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing, which are dedicated to Information Sharing and Analysis Organizations (ISAO’s), an ISAO Standards Organization, Privacy and Civil Liberties Protections, and amendments to the National Industrial Security Program.¹⁵³

Recommendations

- The United States Government must make a commitment to increasing awareness and better educating the younger generation to pursue advanced degrees in Computer Science. by making it a mandatory course in public schools. In addition we will have non-profits who encourage diversity among the computer science field help in creating the core curriculum.
- U.S. government departments should increase budgetary spending towards cyber security by cutting indiscretionary spending, create a discreet policy for offensive and defensive cyberattacks, and institute economic sanctions on countries who directly sponsor a cyber attack.
- Federally mandate that all states have a strategic plan in response to cyberattacks, provide cybersecurity training resources and funding for newer computing technology to police departments, and build or maintain a cybersecurity fusion center for state to state and state to federal communication

¹⁵¹ Department of Homeland Security, "State and Major Urban Area Fusion Centers," dhs.gov, last modified June 17, 2016, accessed July 27, 2016, <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>.

¹⁵² Ibid.

¹⁵³ Office of the Press Secretary, "Executive Order -- Promoting Private Sector Cybersecurity Information Sharing," The White House, last modified February 13, 2016, accessed July 27, 2016, <http://bit.ly/1f78bqf>.

Cybersecurity in the Business Community

Introduction

Hostile Iranian cyber-crime groups, often either directly or indirectly affiliated with the Islamic Republic of Iran, have caused harm to the private sector by repeatedly attacking American corporations. These attacks have threatened the monetary and infrastructural stability of countless businesses, not to mention the harmful ramifications of these attacks on consumers. On several occasions, Iran and its associates have compromised sensitive information, overloaded networks, and hindered the functionality of companies.¹⁵⁴

In a series of incidents beginning in December 2011 and lasting until May 2013, private security companies that were linked to the Iranian government performed scattered attacks, disabling online banking platforms. These hacks prevented bank clientele from accessing their accounts, costing 46 financial institutions millions of dollars in remediation efforts.¹⁵⁵ Arguably more catastrophic, Iranian hackers targeted the Las Vegas Sands Casino in early 2014 and managed to steal credit card information, driver's licenses, and even social security numbers of the company's customers.¹⁵⁶ In November of 2014, Sony Pictures experienced one of the most crippling cyberattacks on record, when North Korea (a strong military ally of Iran) infiltrated the company's computer systems. Hackers wiped out half of Sony's global network and leaked four unreleased movies, costing the company between \$35 million¹⁵⁷ and \$100 million dollars¹⁵⁸, while ultimately rendering thousands of machines completely useless.¹⁵⁹ These troubling incidents are just a glimpse of the danger that international, and more specifically Iranian, cyberattacks pose to America's economy.

Iran, in addition to other countries like China and Russia, continues to bombard U.S. businesses with cyberattacks and the continued risk posed by these nations makes it imperative that we reduce America's vulnerability to these highly-coordinated, damaging attacks.

Current Efforts

With the passage of legislative measures like the Homeland Security Act of 2002, the Cybersecurity Act of 2015, and Executive Orders 13636 and 13691, there now exists a voluntary dialogue for information regarding cyber attacks that facilitates cooperation between private corporations and the federal government.¹⁶⁰ This data sharing is crucial for more comprehensive cyber defense framework for the betterment of business and government.

¹⁵⁴ Aitel, Dave, "Iran Is Emerging as One of the Most Dangerous Cyber Threats to the US." Business Insider, December 02, 2015.

¹⁵⁵ Larson, Erik, Patricia Hurtado, and Chris Strohm. "Iranians Hacked From Wall Street to New York Dam, U.S. Says." Bloomberg Technology. March 24, 2016.

¹⁵⁶ Pagliery, Jose. "Iran Hacked an American Casino, U.S. Intel Director Says." CNNMoney. February 27, 2015.

¹⁵⁷ "Hack Will Cost Sony Upwards of \$35 Million." RT International. February 4, 2015.

¹⁵⁸ Whittaker, Zach. "Sony Takes \$15M Hit after North Korea Cyberattack." ZDNet. Accessed February 4, 2015.

¹⁵⁹ Elkind, Peter. "Sony Pictures: Inside the Hack of the Century." Fortune. July 1, 2015.

¹⁶⁰ "Cybersecurity Legislation Watch." Cybersecurity Legislation Watch. July 24, 2016.

One of the pioneering programs for the purpose of inter-sector sharing is the Homeland Security Act of 2002. Under section 226(b) of this act, the National Cybersecurity and Communications Integration Center (NCCIC) was established by the Department of Homeland Security (DHS).¹⁶¹ The NCCIC was created to be a central information hub that allows bidirectional sharing to create awareness regarding cyber defense vulnerabilities and incidents.¹⁶² Within the NCCIC is the Cyber Information Sharing and Collaboration Program (CISCP),¹⁶³ which fortifies cyberdefenses by rapidly exchanging data through AISs (Automatic Indicator Sharing).¹⁶⁴ AISs, established by the Cybersecurity Act of 2015, quickly exchanges information regarding possible threats, such as malicious IP addresses or phishing emails so network defenders are able to block cyberattacks before damage is done.¹⁶⁵ This program works by highlighting new threats, making more in-depth analyses of intruders, focusing on small intrusions before their impact, and creating course of action recommendations.¹⁶⁶ The CISCP encourages sector sharing by being free of charge, redacting personal or proprietary information in order to protect civil liberties, and deleting information that is not directly relevant to cyber threats under the Protected Critical Infrastructure Information (PCII) Program.¹⁶⁷

Executive Order 13636 clarifies and expands framework for information sharing between the public and private sectors for the protection of critical infrastructure (CI).¹⁶⁸ The protection of CI is imperative for national security and the functionality of the economy. The Executive Order identifies crucial CI—to prioritize its protection—, orders the DHS’s Critical Infrastructure Partnership Advisory Council to facilitate protection activities of State, local, territorial, and tribal governments, and requires the National Institute of Standards and Technology (NIST) to develop cybersecurity framework and standards for best practices.¹⁶⁹ Executive Order 13691 expands on Executive Order 13636 designates the NCCIC as a CI protection program, and establishes non-sector affiliated Information Sharing and Analysis Organizations (ISAOs).¹⁷⁰ ISAOs are for the promotion of voluntary organizations to encourage interaction with other organizations and the Federal Government on a voluntary basis.¹⁷¹

Moving Forward

Despite recent efforts on behalf of the U.S. government to improve our current standing, there remains a series of necessary measures in order to strengthen economic cybersecurity. The United States can protect its businesses and overall economic stability by implementing cybersecurity standards and providing cybersecurity education opportunities.

¹⁶¹ Homeland Security Act 2002, 6 U.S.C. § 226(b) (2002).

¹⁶² National Cybersecurity and Communications Integration Center. January 19, 2016.

¹⁶³ Cyber Information Sharing and Collaboration Program (CISCP). May 4, 2016.

¹⁶⁴ Executive Department of Homeland Security. Automated Indicator Sharing (AIS).

¹⁶⁵ *Ibid.*

¹⁶⁶ Cyber Information Sharing and Collaboration Program (CISCP).

¹⁶⁷ Protected Critical Infrastructure Information (PCII) Program. July 21, 2016.

¹⁶⁸ Exec. Order No. 13636 Fed. Reg. 1 Feb. 12, 2013)

¹⁶⁹ Eric A. Fischer. Federal Laws Relating to Cybersecurity:. Issue brief no. R42114. December 12, 2014.

¹⁷⁰ Exec. Order No. 13691 Fed. Reg.

¹⁷¹ *Ibid.*

In order to develop a concise system for responding to cyberattacks on businesses, both in America and abroad, a system for analyzing the severity of an attack and the appropriate response measures must be instituted. An international standard of cybersecurity must be put forth to ensure that businesses adhere to best practices. It is essential that this standard explicitly defines the levels of cyber threats. An attempt was made to create international guidelines for defining the severity of cyberattacks, through the composition of the Tallinn Manual which focused on responses to these attacks on a state level.¹⁷² To appropriately facilitate responses to cyberattacks by international businesses, a similar document must be created that defines a set group of responses. This document is a necessity because cybersecurity is a developing industry and is evolving from what used to be a reactionary, passive measure to active defense.

Standardization will guarantee that businesses do not violate laws in retaliation to cyberattacks. The guidelines for cybersecurity must define what level of active cyber security is viable before it is labeled as a retaliatory cyber attack. With the increasing popularity of “hackbacks” as a response, it is necessary to define the extent of legal and ethical boundaries when it comes to retaliatory attacks.¹⁷³ One effective way to define the appropriate response levels would be to tier the severity of cyberattacks. For example, in a situation where the hacker is solely targeting intellectual capital, the response from the victim should be much less than when the hacker targets the identity and finances of employees or clientele. The most strategic way to address the varying levels of cyber threats would be to create a group of cybersecurity experts that would create a detailed analysis of the levels and degrees of cyber crimes and develop a structure that discussed appropriate responses. Once a standard level is created, it must be introduced to the international business community through an international business forum that allows for open discussions about the new policies being suggested. The ideal outcome of this forum would be a unanimous adoption of the policy, that would allow international businesses to cooperate only if all businesses upheld the standards introduced by the new cybersecurity document. This would allow businesses to operate with minimal government involvement but still have a standard agreement on what constitutes cyber security.¹⁷⁴

Another important facet of policy moving forward is a thoughtful approach to educating small business owners. In Symantec’s 2016 report, 43% of all cyberattacks targeted small businesses, a 25% increase from just four years ago.¹⁷⁵ These businesses have smaller IT budgets and, consequently, less capital to expend towards protecting from cyber threats.¹⁷⁶ This growing issue has garnered attention in Congress and the resulting legislative efforts have made some headway: Senate Bill 3024, entitled “Small Business Cybersecurity Improvements Act of 2016,” seeks to provide Small Business Development Centers (SBDCs) with the means to increase knowledge and protection of cyberspace among the small business community. By giving grants to SBDCs, they will have the ability to connect business owners with external cybersecurity specialists.¹⁷⁷ It is essential to

¹⁷² "Research." CCDCOE. 2014.

¹⁷³ Irving Lachow, "Cyber Defense," *AccessScience*, pag. Web.

¹⁷⁴ Ibid.

¹⁷⁵ Symantec, *2016 International Security Threat Report*, April 2016, 44.

¹⁷⁶ Ibid, 46.

¹⁷⁷ "S.3024 - 114th Congress (2015-2016): Small Business Cyber Security Improvements Act of 2016." *Congress.gov*, June 9, 2016.

the economic interests of our nation that legislation be signed into law. This ground-up approach, focusing on those smaller businesses that are more vulnerable to attack and face security threats that are often easier to remediate, can be applied to the international economic community also. After successful implementation of the measures outlined in SB 3024, the U.S. should collaborate with foreign nations to similarly legislate and protect their own growing businesses.

Recommendations

- Develop an international standard for responding to cyber attacks on businesses. The standard should clearly outline the proper method for analyzing the severity of an attack and appropriate response measures.
- Advocate for legislation (like SB 3024) that promotes the cyber security of small businesses by providing educational resources to small business owners.

Bibliography

- Aitel, Dave, "Iran is emerging as one of the most dangerous cyber threats to the US" *Business Insider*, 2 December 2015.
- Alexander, Ryan, "Start Cutting Government Spending with the Defense Budget" *US News*, January 2013.
<http://www.usnews.com/opinion/blogs/economic-intelligence/2013/01/16/start-cutting-government-spending-with-the-defense-budget>.
- "America Built A Cyber Weapon To Preempt Nuclear War With Iran." *Popular Science*. February 17, 2016.
- Anonymous post to The Economist newsgroup, "Cyber-riot," May 10, 2007. Accessed July 26, 2016.
<http://www.economist.com/node/9163598>.
- Art. 8, Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), 1907.
- Atherton, Kelsey D. "Cyber Attacks are America's Top Security Threat. That's Better News Than It Sounds" *Popular Science*, March 13, 2013.
- Barnes, Julian E. and Siobahn Gorman. "U.S. Says Iran Hacked Navy Computers." *The Wall Street Journal*, September 27, 2013. <http://www.wsj.com/articles/SB10001424052702304526204579101602356751772>.
- Bell, Alistair, ed. "Number of U.S. Government 'Cyber Incidents' Jumps in 2015." *Reuters*. Last modified March 21, 2016. Accessed July 27, 2016. <http://reut.rs/2ajuSZa>
- Bender, David J. "Congress Passes the Cybersecurity Act of 2015." *The National Law Review*, December 20, 2015.
<http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015>.
- Bennett, Cory. "Israel, Iran Locked in Escalating Cyber War." *The Hill*. Last modified March 4, 2015. Accessed July 27, 2016. <http://bit.ly/2ad3LRT>.
- Bertrand, Natasha. "Iran is building a non-nuclear threat faster that experts 'would have ever imagined.'" *Business Insider*, March 27, 2015.
- Blas, Javier. "Too Big to Value: Why Saudi Aramco Is in a League of Its Own." *Bloomberg*, January 7, 2016.
www.bloomberg.com/news/articles/2016-01-07/too-big-to-value-why-saudi-aramco-is-in-a-league-of-its-own.
- Bronk, Christopher, and Eneken Tikk-Ringas. *Hack or Attack? Shamoon and the Evolution of Cyber Conflict*. February 1, 2013. Accessed July 27, 2016. <http://bit.ly/1jtKh3o>.

Bryan, Bob. "The US Government is not Spending Enough on Cybersecurity" Business Insider, September 3, 2015. <http://read.bi/2a03DE1>.

Bush, George W. "The National Strategy to Secure Cyberspace." The White House, February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Carter, Ashton. "The Department of Defense Cyber Strategy" Washington, DC: GPO, July 27, 2016. <http://bit.ly/2aa6Spz>

Carter, Ashton. "The Department of Defense Cyber Strategy" Washington, DC: GPO, 2015. <http://bit.ly/2aa6Spz>.

Center for Internet Security. "MS-ISAC MEMBERS" <https://msisac.cisecurity.org/members/index.cfm>.

Chien, Eric, Liam Murchu, and Nicolas Falliere. "W.32 Stuxnet Dossier." *Symantec*, version 1.4 (2011): 5-7.

Clinton, Bill. "Presidential Decision Directives/NSC-63." The White House, May 22, 1998, <http://fas.org/irp/offdocs/pdd/pdd-63.htm>.

"Code.org Advocacy Coalition." July 27, 2016. <https://code.org/advocacy>.

Crime and Terrorism: Hearings Before the Judiciary Committee, 112th Cong., 1st Sess. (2011) (statement of Gordon M. Snow). Accessed July 27, 2016. <http://bit.ly/2arMSQg>.

Crosston, Matthew D. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly*, Spring 2011. Accessed July 27, 2016. <http://bit.ly/2a10BQ1>.

"Cyber Defence Training." CCDCOE. 2014.

Cybersecurity Legislation | Cybercrime Laws | Cyber Security News - ISACA." *Cybersecurity Legislation | Cybercrime Laws | Cyber Security News - ISACA*, January 6, 2016.

"Cybersecurity Legislation Watch." Cybersecurity Legislation Watch. July 24, 2016.

Cyber Information Sharing and Collaboration Program (CISCP). May 4, 2016. <https://www.dhs.gov/ciscp>.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. <http://www.wired.com/2007/08/ff-estonia/>.

Department of Defense. "Department of Defense Strategy for Operating in Cyberspace," July 2011,

Department of Homeland Security. "Law Enforcement Cyber Incident Reporting (Washington, DC: Department of Homeland Security, 2015)" <http://bit.ly/2avaNjb>.

Department of Homeland Security. "State and Major Urban Area Fusion Centers" June 17, 2016. <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>.

Dickey, Christopher. "The Shadow War." *Newsweek*, December 20, 2010. Accessed July 25, 2016. <http://bit.ly/2ayG0mW>.

Dillow, Clay. "Stuxnet Worm Is A 'Game Changer' For Global Cybersecurity," *Popular Science*, November 2010.

Elkind, Peter. "Sony Pictures: Inside the Hack of the Century." *Fortune*. July 1, 2015.

Executive Department of Homeland Security. Automated Indicator Sharing (AIS). 2016. <https://www.dhs.gov/ais>. "Automated Indicator Sharing (AIS)." US-CERT.

Executive Department of Homeland Security. Automated Indicator Sharing (AIS). 2016. <https://www.dhs.gov/ais>. "Automated Indicator Sharing (AIS)." US-CERT.

Exec. Order No. 13636 Fed. Reg. 1 (Feb. 12, 2013). <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636>.

Exec. Order No. 13691 Fed. Reg. 1 (Feb. 15, 2015). <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

Filshinskiy, Stas. "Privacy and Security Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air?" *Viewpoints* 56, (June 2013): 28-30.

Fischer, Eric A. Federal Laws Relating to Cybersecurity:. Issue brief no. R42114. December 12, 2014.

Golnaz Esfandiari. "Basij Members Trained to Conquer Virtual World." *Payvand Iran News*, August 21, 2010.

Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." *Wall Street Journal* (New York, NY), May 31, 2011. Accessed July 27, 2016. <http://on.wsj.com/1OYTjaR>.

"Hack Will Cost Sony Upwards of \$35 Million." RT International. February 4, 2015.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aliien Nowlan, William Perdue, Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (August 2012): 817-85.

Homeland Security Act 2002, 6 U.S.C. § 226(b) (2002).

International Securities Exchange. "A Call to Action: Equipping Law Enforcement With the Tools to Investigate Cybercrime"
<https://www.ise.gov/sites/default/files/cyber%20awareness%20call%20to%20action%203-2016.pdf>.

Irving Lachhow, "Cyber Defense," *AccessScience*, pag. Web.

"Israel's Dimona Nuclear Facility Splits Time as Cyberweapon Testing Ground CyberWarfare."
Gizmodo (blog). Entry posted January 16, 2011. Accessed July 25, 2016. <http://bit.ly/2ag9GQ7>.

Journal of International Commercial Law & Technology. 2013, Vol. 8 Issue 3, p179-189. 11p.

Katz, Yaakov. "Iran embarks on #1b. Cyber-warfare program." *The Jerusalem Post*, December 18, 2011.

Kumar Sen, Ashish. "Iran's Growing Cyber Capabilities in a Post-Stuxnet Era: Cyber attack on Iran served as an 'awakening' for Tehran." Atlantic Council. Last modified April 10, 2015. Accessed July 28, 2016. <http://bit.ly/2azJ560>.

Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Software Magazine*, May 2011, 49-51.

Larson, Erik, Patricia Hurtado, and Chris Strohm. "Iranians Hacked From Wall Street to New York Dam, U.S. Says." Bloomberg Technology. March 24, 2016.

Marks, Joseph. "Iran Launched Major Cyberattacks on the Israeli Internet - German Intelligence Snooped On Kerry and Clinton - Seleznev Gets No Bail." *Politico*, August 8, 2014.

Meisner, Jeff. "A National Talent Strategy." Microsoft. December 3, 2012.
<http://blogs.microsoft.com/on-the-issues/tag/national-talent-strategy/#sm.000006g2phtjnelivncskc6p39fv>

Melzer, Nilz. United Nations Institute for Disarmament Research. *Cyberwarfare and International Law*.

National Cybersecurity and Communications Integration Center. January 19, 2016.
<https://www.dhs.gov/national-cybersecurity-and-communications-integration-center>.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity" February 12, 2014.

- Nord, C., Hicks, L., Hoover, K., Jones, M., Lin, A., Lyons, M., Perkins, R., Roey, S., Rust, K., and Sickles, D. "The 2009 High School Transcript Study User's Guide (NCES 2011-465)" U.S. Department of Education, National Center for Education Statistics.
- Office of the Press Secretary. "Executive Order -- Promoting Private Sector Cybersecurity Information Sharing" The White House. February 13, 2016.
<https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.
- Oliver Kessler and Wouter Werner, "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare" *Leiden Journal of International Law* (2013): 799-801 Schmitt, Michael N. "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law & Policy Review* 25:269-300.
- Pagliery, Jose. "The Inside Story of the Biggest Hack in History." *CNN Money*, August 5, 2012.
money.cnn.com/2015/08/05/technology/aramco-hack/.
- Pagliery, Jose. "Iran Hacked an American Casino, U.S. Intel Director Says." *CNNMoney*. February 27, 2015.
- Perloth, Nicole. "In Cyberattack on Saudi Firm, U.S. sees Iran Firing Back." *The New York Times*, October 23, 2012.
- "Phil's Stock World: Cyberwarfare Threat To Nuclear, Banking and Financial System." *Phil's Stock World* (blog). Entry posted June 13, 2015. Accessed July 25, 2016. <http://bit.ly/2aetUzC>.
- Protected Critical Infrastructure Information (PCII) Program. July 21, 2016.
<https://www.dhs.gov/pcii-program>.
- "Research." CCDCOE. 2014.
- "Research." CCDCOE. 2014. Accessed July 26, 2016.
- Reuter, Nicholas C. "The Cybersecurity Dilemma." Master's thesis, Duke University, 2011. Accessed July 25, 2016. ProQuest.
- Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." *International Affairs Review*, April 4, 2009. www.iar-gwu.org/node/65.
- Rogin, Josh. "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History.'" *The Foreign Policy Group*, July 9, 2012.
- Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia." *The European Institute*. Last modified 2007.
<http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia>.

- Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times*, June 1, 2012.
- Sanger, David E., and Mark Mazzetti. "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." *The New York Times*. 2016.
- Shafa, Eric K. "Iran's Emergence as a Cyber Power." Strategic Studies Institute, August 20, 2014.
- Siboni, Gabi and Sami Kronenfeld. "Developments in Iranian Cyber Warfare." *Military and Strategic Affairs*, August, 2014.
- Spidalieri, Francesca. "State of the States on Cybersecurity" November 2015. <http://bit.ly/2ai87lz>.
- Sternstein, Aliya. "Pentagon Contractors Developing Lethal Cyber Weapons." *NextGov.com*. November 4, 2015. 39-40
- Symantec, *2016 International Security Threat Report*, April 2016.
- "S.3024 - 114th Congress (2015-2016): Small Business Cyber Security Improvements Act of 2016." *Congress.gov* June 9, 2016.
- Touré, Hamadoun I. "International Telecommunication Union Cybersecurity Overview." *United Nations*. Accessed July 27, 2016. <http://bit.ly/2agaX9E>.
- United States. Department of Defense. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Washington, D.C.: U.S. Dept. of Defense, November, 2011. 2. United Nations, Charter of the United Nations, 24 October 1945
- Van der Meer, Sico. *Foreign Policy Responses to International Cyber-attacks: Some Lessons Learned*. September 2015. Accessed July 27, 2016. <http://bit.ly/2avW6My>.
- Volz, Justin. "Obama Expands the US Response to Cyber Attacks" *Defense One*. April 1, 2015. <http://bit.ly/2auPaiF>.
- Weinberger, Sharon. "Is this the start of Cyberwarfare?" *Feature News 474*, (June 2011) : 142-145, *The IEEE Computer and Reliability Societies*, "Cyberwarfare" Guest Editors' Introduction, (August 2011): 13-15.
- Weise, Elizabeth, and Jessica Guynn. "Tech Jobs: Minorities Have Degrees, but Don't Get Hired." *USA Today*. Last modified October 13, 2014. Accessed July 27, 2016. <http://usat.ly/1nikhzq>.

"What Limits Does the Law of War Impose on Cyber Attacks?" - ICRC. June 28, 2013. Wolff Heintschel von Heinegg, "The Tallinn Manual and International Cyber Security Law" Yearbook of International Humanitarian Law (2012): 1-10

The White House. "Commission on Enhancing National Cybersecurity" Federal Register. February 12, 2016.

<https://www.federalregister.gov/articles/2016/02/12/2016-03038/commission-on-enhancing-national-cybersecurity>.

Whittaker, Zach. "Sony Takes \$15M Hit after North Korea Cyberattack." ZDNet. Accessed February 4, 2015.

Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity." Arms Control Association. Accessed July 27, 2016. <http://bit.ly/2ao8ajn>.

Zeltser, Lenny. "Mutually-Assured Destruction as a Factor in Cyber Warfare." Lenny Zeltser. Last modified February 20, 2015. Accessed July 27, 2016. <http://bit.ly/2aAG8zi>

Appendix A

Armed Attack: an attack made by a weapon that includes computers.

Computer virus: Piece of code that is capable of copying itself and has a detrimental effect such as corrupting systems or destroying data

Cyberattack: Any attack on the infrastructure of the United States of America

Cyber Powers: Global powers with strong cyber capabilities

Cybersecurity: measures taken to protect infrastructure, corporations, and information systems from a cyber attack

Cyberspace: an area in which computer networks are able to communicate

Cyber warfare: the conflict that results from the use of malware, an assortment of software capable of intruding a technological system, to disarm a nation's security network or infrastructure.

Denial-of-Service attacks: An incident when the attacker suspends the ability of users to access services or information

Infrastructure: systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have an impact on security, national economic security, national public health or safety, or any combination of those matters.

Intentional cyber harm (cyberattacks): a type of attack that targets a system's ability to manage infrastructure

Malware: Software that damages computers and computer systems. Blend of malicious/software
Phishing: An attempt to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Seculert: (a cloud-based cyber security technology company based in Israel. The company's technology is designed to detect breaches and Advanced Persistent Threats (APTs), attacking networks. Seculert business is based on malware research and the ability to uncover malware that has gone undetected by other traditional measures)

Self-Defense: An action or set of actions that one country makes against another after the other has made an attack or set of attacks against that country.

Worm: Standalone malware that replicates itself to spread to other computers that (unlike viruses) do not need to attach themselves to programs. They always cause harm and can use bandwidth or create backdoors for hackers to gain total control of computers.