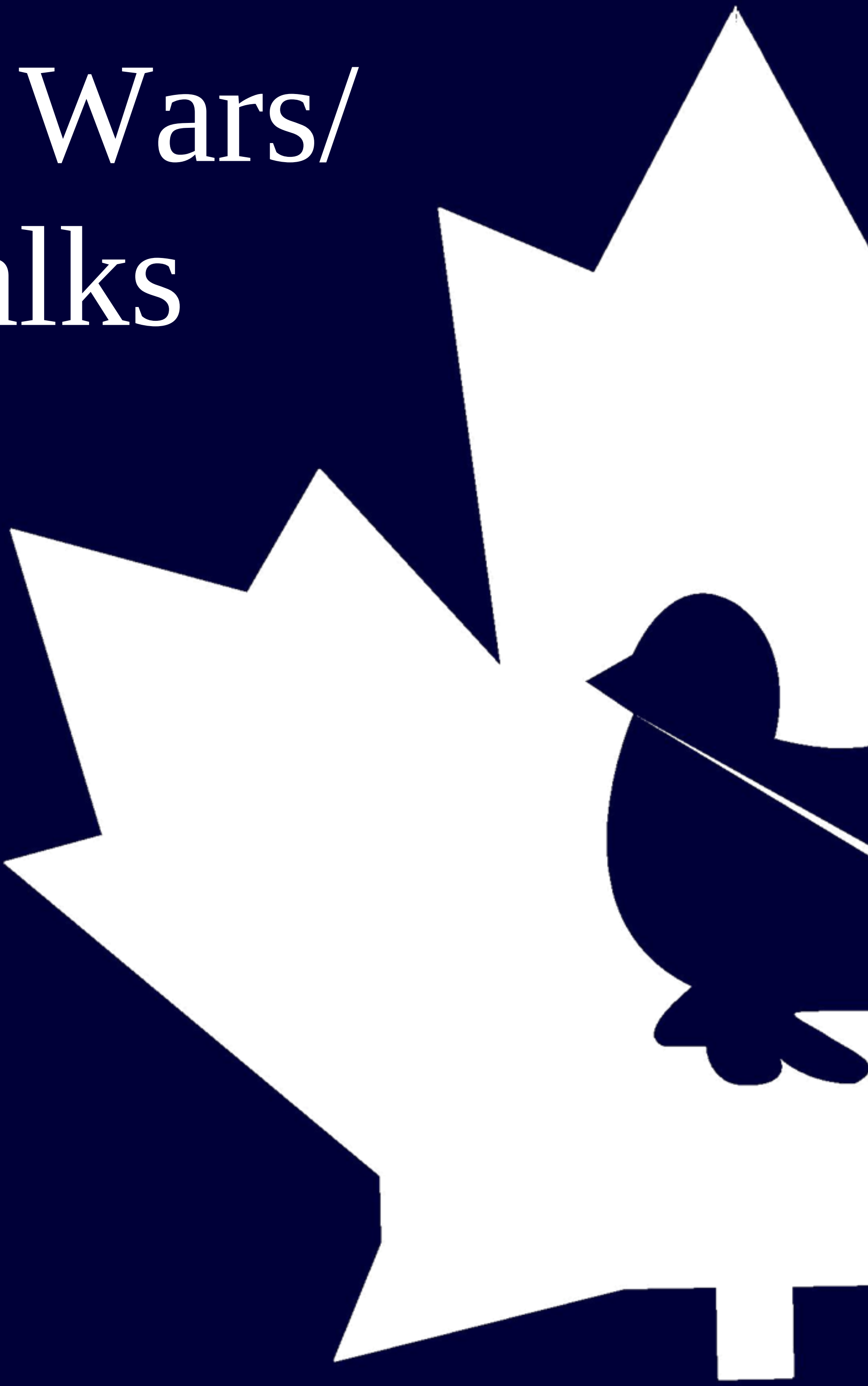
SECONDARY SCHOOLS' UNITED NATIONS SYMPOSIUM 2015

Hacking Wars/ Peace Talks



Chair:
Nick Nasirpour

Vice Chairs:
Caroline Wesley
Hana Bell
Arun Rawlani

NOVEMBER 12-15, 2015 | MONTRÉAL, QUÉBEC

Hacking Wars/Peace Talks Committee

Dear Delegates,

My name is Nick Nasirpour, and I will be your Chair for Hacking Wars and Peace Talks at this iteration of the Secondary Schools' United Nations Symposium in Montréal. I'm currently a third year student studying Software Engineering and aim to bring my knowledge of computer systems and development to good use during this committee. I was born in Vancouver, but I'd lived in San Diego for most of my life before making my way over to Montréal and McGill. On top of being on this dais for SSUNS, I'm also a member of the McGill Model United Nations Assembly Secretariat for the upcoming conference.

Throughout the weekend, we will be discussing a wide variety of topics ranging from ways of improving cyber-security to the impacts of cyber-warfare. We'll also be having a small Hacking 101 session, where we'll demonstrate various hacking techniques in order to give you a better understanding of the topic at hand. Accompanying me on this adventure will be my three lovely vice-chairs:

Caroline Wesley is a U1 double major in Political Science and International Development Studies, minoring in East Asian Language and Literature. Working as the Head Delegate of her high school's MUN Team and as a staff member of McMUN2015, Caroline developed a passion for everything United Nations. She looks forward to meeting the SSUNS2015 delegates and is always looking to practice her French, Spanish, or Chinese!

Hana loves to travel- she was born in Vancouver, raised in Toronto, and now lives in Manhattan when she is not working on her McGill degree here in Montreal. She also hopes to attend law school in California in the fall of 2016. She is now in her fourth and final year as an English Literature major with a double minor in Communications and East Asian Studies. This is her second year working on MUN at McGill and she is excited to be working for her first time as a vice chair! Hana is fluent in Japanese and has danced professionally for most for of her life. Some other fun facts are that the royal antelope is her spirit animal and she loves raspberry cheesecake!

Arun is currently a U2 at McGill majoring in Computer Science. As a proficient debater since high school, MUNs have always intrigued him. They present us with a chance to find our feet in a world increasingly shaped by strategic negotiations, farsighted alliances and matters of diplomacy. They present us a great opportunity to learn and display our own skills in these areas. When he's not MUNing, He enjoys doing programming, product design, traveling, photography, sports and writing.

Our team will be working diligently to prepare a realistic and unforgettable experience for you! Please do not hesitate to contact us with any questions, comments, or concerns.

Nick Nasirpour

Chair,
Hacking Wars and Peace Talks
SSUNS 2015

Topic I: Defense against Cyber Attacks

Introduction

The computer security community uses the term APT (advanced persistent threats) in reference to a long-term pattern of sophisticated hacking attacks aimed at governments, companies, and political activists.[1] These threats have the ability to penetrate a standard security system and work underground while remaining undetected for months at a time[2]. From 2010 to 2011, PC World reported an 81 percent increase in APT attacks.[3] These statistics show how quickly APTs can proliferate. In order to mitigate the emergence and persistence of cyber hacking, protection against them must continuously improve.

The earliest published APT attack on a military research establishment was in the late 1980s. This attack raised awareness across intelligence and security communities, warning them of hacking capabilities and the vulnerability of their own security systems. It was a "portent for future attacks that would materialize in years to come."[4] An ongoing issue with APT attacks is the difficulty of determining the party responsible. With every notable cyber attack has come a group of experts, each with a different unsubstantiated rumor regarding who is responsible for the act.

Until Operation Aurora, victims of APT attacks chose not to disclose the details of their attacks out of fear that their client base would be upset or their attackers may be antagonized. In January 2010, Google, a victim of Operation Aurora, publicized the attack, promoting awareness of the risk and encouraging corporations susceptible to attacks to invest in improved security countermeasures. Many large companies are reluctant to disclose information regarding being victims of cyber attack, but as of recent, regulatory compliance requirements have coerced companies to open up about their hacking experiences.[5]

Figure 1 Google has left China since.
(src=http://www.baijingapp.com/question/3850)

[1] Angie Heise, "Understanding the Enemy: The Advanced Persistent Threat" *Lockheed Martin* (2015).
[2] Trend Micro, "Custom Defense Against Cyber Attacks" *A Trend Micro White Paper* (2014).
[3] Angie Heise, "Understanding the Enemy: The Advanced Persistent Threat" *Lockheed Martin* (2015).
[4] ISACA, "The Most Famous Advanced Persistent Threats in History" *IT Business Edge* (2013).
[5] Matthew J. Schwartz, "Google Aurora Hack Was Chinese Counterespionage Operation" *DARKReading* (2013).

Cyber defense techniques employed by the US

There are three varieties of cyber attacks that are responsible for most of the cybercrime costs and damages in the US. These categories given by Trend Micro are:

- *Social* – Targeting and attacking specific people with social engineering and advanced malware;
- *Sophisticated* – Exploiting vulnerabilities, using backdoor controls, stealing and using valid credentials;
- *Stealthy* – Executed in a series of low profile moves that are undetectable to standard security or buried among thousands of other event logs collected every day.[6]

The best defense mechanism companies can take against cyber attack is to invest in advanced technological software that will protect against security attacks. If the hacking party cannot infiltrate the security wall of a company, they will be unable to steal, compromise, or damage any information. Furthermore, if security walls are strengthened, the hacking virus/software will be unable to rest unseen, amalgamating into an APT and waiting for the opportune moment to attack.

History of Cyber Attacks on the U.S

The following link leads to Nato's Cyber Timeline.
http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

It briefly outlines the most serious cyber attacks and their consequences. Some notable cyber attacks in the US include Epsilon 2011, an attack that incurred $225 million to $4 billion dollars in damages; Moonlight Maze 1988, a supposed Russian attack on the US where hackers targeted military maps and troop configurations from the Pentagon; Titan Rain 2004, a series of Chinese government coordinated cyber raids against NASA that left American machines "zombified" and easier to infiltrate in the future; and the Original Logic Bomb 1982, in which the CIA used a portion of code to disrupt and explode a Siberian gas pipeline operation.

According to The New York Times, in its joint publication with an American computer security firm Mandiant, majority of cyber attacks on the US originates from China. The report argues that a significant portion of the cyber attacks on American entities originate from the People's Liberation Army base near Shanghai, China. Known as the "Comment Crew", it has allegedly broken into computer systems of US based companies such as Coca-Cola, and the government's critical infrastructure such as a computer security firm RSA which stores many corporate and government databases.[7]

[6] Trend Micro, "Cyber Attack Protection" *Trend Micro* (2014).

[7] http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Case Study: Operation Aurora

In 2009, Chinese groups tied to the People's Liberation Army, such as the Elderwood Group, conducted a series of cyber attacks aimed at American corporations such as Google, Adobe Systems, Yahoo, and Morgan Stanley. The primary goal of the attack was to gain access to and potentially modify source code repositories at high tech security companies.[8] Threat research at cyber-security company McAfee Labs discovered that "Aurora" was part of the file path on a machine associated with the attackers, and the attacks were thus named Operation Aurora.[9]

The resulting damage

Operation Aurora hackers infiltrated many companies, but the one most publicized is the attack against Google. The hackers penetrated Google's security wall and stole intellectual property, one of which was information from the Gmail accounts of human rights advocates in the US, Europe, and China. Google then threatened to shut down its operations in China.[10] Though experts say it is difficult to assess what the long term damages are, but one idea is that someone could build a competing product or find vulnerabilities to the product code and use it to leverage access elsewhere.[11] One of the worst damages an attack can cause is damage to a company's infrastructure, which could prohibit the ability of a company to run itself in the long term.

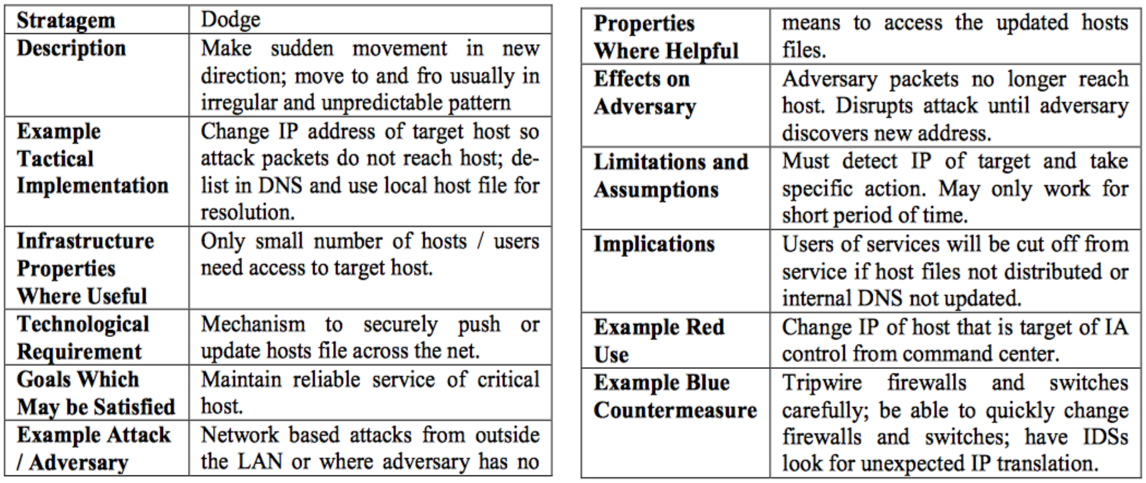
How it was dealt with

In a cyber attack, the attacked must decide which move to take. Figure 1 is an example of the steps an enterprise could carry out using a "dodge" defense technique.
This topic aims to show how cyber attacks develop based on action and reaction, and delegates will work to determine the right action for certain attacks based on in depth analysis.

According to Trend Micro, Operation Aurora was hit so Micro has software that can minimize attack damage in the future. This ideal software – Trend Micro's Custom Defense solution – not only detects attacks based on environment, attackers, and type of attack, but also engages and responds by fighting back against the attack. Google recommends that corporations should use reputable antimalware software, patch diligently, and update Web browsers on a regular basis.[12] These steps of action are some

[8] Éric Filiol and Adrien Erra, "Operation Aurora" *Proceedings of the 11th European Conference on Information warfare and security* (2012), 48.
[9] McAfee Labs and McAfee Foundstone Professional Services, "Protecting Your Critical Assets", *McAfee Inc.* (2010).
[10] John Seabrooke, "Network Insecurity" *The New Yorker* (2013).
[11] William Jackson, "How Google attacks changed the security game" *GCN* (2010).
[12] Nick Lewis, "Operation Aurora: Tips for thwarting zero-day attacks, unkown malware" *TechTarget* (2010).

examples of what will help mitigate attacks similar to Operation Aurora.



Stratagem	Dodge
Description	Make sudden movement in new direction; move to and fro usually in irregular and unpredictable pattern
Example Tactical Implementation	Change IP address of target host so attack packets do not reach host; de-list in DNS and use local host file for resolution.
Infrastructure Properties Where Useful	Only small number of hosts / users need access to target host.
Technological Requirement	Mechanism to securely push or update hosts file across the net.
Goals Which May be Satisfied	Maintain reliable service of critical host.
Example Attack / Adversary Properties Where Helpful	Network based attacks from outside the LAN or where adversary has no means to access the updated hosts files.
Effects on Adversary	Adversary packets no longer reach host. Disrupts attack until adversary discovers new address.
Limitations and Assumptions	Must detect IP of target and take specific action. May only work for short period of time.
Implications	Users of services will be cut off from service if host files not distributed or internal DNS not updated.
Example Red Use	Change IP of host that is target of IA control from command center.
Example Blue Countermeasure	Tripwire firewalls and switches carefully; be able to quickly change firewalls and switches; have IDSs look for unexpected IP translation.

Figure 2 src=http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf

Comments on the incident

Professionals in computer hacking advise corporations to increase skills, processes, and technology to their cyber security arsenals in order to decrease the chances of APT infiltration. Should American companies decide to invest in refurbishing their software, the chance of APTs looming in the shadows and preparing for attack will be exponentially lessened. Though increasing security hardware is important in defending against cyber attacks, hackers are simultaneously increasing their own hacking sophistication. Because of this, the focus of defending against cyber attacks should not be just on strengthening security walls, but on detecting and responding before an attack happens.

Conclusion

Delegates will analyze cyber attacks against the United States of America and make predictive judgments about whether to act, and how to act. Delegates should be mindful of long-term policy interests and make decisions while being mindful of potential reactions from the opposing side of the attack, as well as potential consequences such as loss of client base.

Questions to Consider:

1. Does a cyber attack ever warrant self-defense in the form of retaliation? If so, when? How can the US determine which techniques to use?
2. Should enterprises in the US create a playbook with a list of plays arranged for certain situations? What other steps can the US take to defend against cyber attacks?
3. With increasing APTs, what steps can be taken to ensure there are no covert cyber threats penetrating existing security walls?

Topic II: Cyber attacks

Introduction

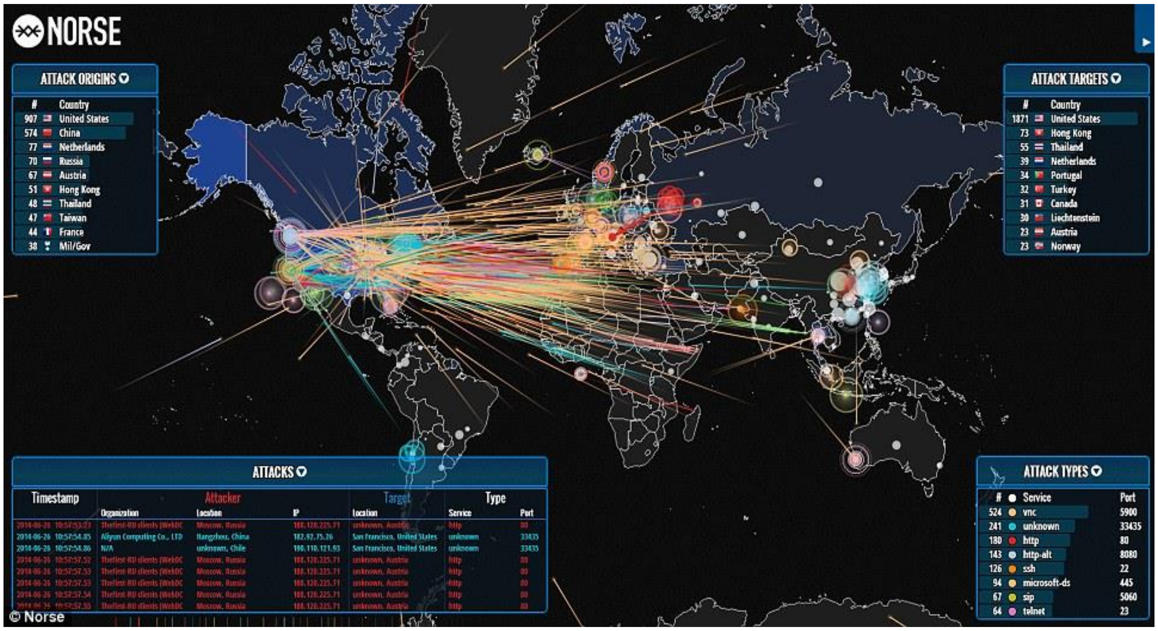
Following the terror attacks of September 11th, 2001, the United States has built one of the most heavily funded and comprehensive counterintelligence programs in the world. Former NSA contractor Edward Snowden revealed to The Washington Post that in 2013, The United States funded a **“**Black Budget**”** of $52.6-billion towards their National Intelligence Program. This program is composed of 16 spy agencies, with the majority of funding going to the fundamental 5: The Central Intelligence Agency (CIA); The National Security Agency (NSA); The National Reconnaissance Office; The National Geospatial-Intelligence Program; and The General Defense Intelligence Program.[13] This conglomeration employs a staggering number of 107,035 people, and the expenditure of these agencies can be divided into four main categories: “data collection, data analysis, management, facilities and support and data processing and exploitation.”[14]

Cyber-attack techniques employed by the U.S

Another startling revelation made by Snowden’s budget leak was that the CIA and the NSA have implemented a system of “offensive cyber operations”, which are comprised of “aggressive new efforts to hack into foreign computer networks to steal information or sabotage enemy systems”.[15] One method outlined within the “Black Budget” was through operation GENIE, which is a $652-million project that “placed “covert implants, sophisticated malware transmitted from far away, in computers, routers and firewalls on tens of thousands of machines every year, with plans to expand those numbers into the millions.” [16]

In addition to this covert hacking USA has employed, their more intrusive methods have also come to light. Snowden’s leaked documents reveal that of the **231 offensive operations** conducted in 2011, “nearly three-quarters were against top-priority targets, which former officials say includes adversaries such as Iran, Russia, China and North Korea and activities such as nuclear proliferation.”[17] Offensive operations such as these are defined by the U.S. agencies as activities intended to “to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves,” and these operations are most often immediately effective in compromising the functionality of a target’s machine. This is usually seen in “slowing its network connection, filling its screen with static or scrambling the results of basic calculations.”[18]

[13] "The Black Budget: Explore Top Secret U.S. Intelligence Funding." Washington Post. Accessed May 01, 2015.
[14] Ibid.
[15] Gellman, Barton, and Greg Miller. "'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives." Washington Post. August 29, 2013. Accessed June 06, 2015.
[16] Gellman, Barton, and Ellen Nakashima. "U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show." Washington Post. August 30, 2013. Accessed May 01, 2015.
[17] Ibid.
[18] Ibid.



ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 10:57:53.23	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.26	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.86	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.52	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.55	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	●	Service	Port
524	●	vnc	5900
241	●	unknown	33435
180	●	http	80
143	●	http-alt	8080
126	●	ssh	22
94	●	microsoft-ds	445
67	●	sip	5060
64	●	telnet	23

Figure 3 Cyber Attack Origins and Targets (src=Daily Mail UK)

According to a former NSA operator, the central location from which most state-funded hackers carry out cyber-attacks is “the ROC”, or the Remote Operations Center. These centers include the NSA’s Fort Meade headquarters and regional operations centers in Georgia, Texas, Colorado, and Hawaii. In a 570-page budget blueprint for what the United States government calls its Consolidated Crypologic Program, it states that once the hackers find a weak spot in a target’s defense, “[t]argeted systems are compromised electronically, typically providing access to system functions as well as data. System logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals,”[19] Within this program, units from the FBI, the CIA and U.S. Cyber Command work hand in hand with overlapping missions. The leaked budget report states that the ROCs aforementioned “breaking-and-entering” mission is supported by the GENIE program’s infrastructure, and aim for the exploitation of foreign systems. Such exploitation, according to the budget, entails “surreptitious virtual or physical access to create and sustain a presence inside targeted systems or facilities… System logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals.”[20]

History of U.S cyber-attacks and cyber security breaches by the U.S

In *The Guardian*’s comprehensive guide to decoding the leaked NSA files by the whistleblower Edward Snowden, the two main information-collecting programs are explained. Upstream (often known under its various codenames such as BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW) is the NSA’s own cable-interception

[19] Ibid.
[20] Ibid.

program that works in partnership with major US telecommunication and Internet companies. The NSA defines this program's objective: "Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routes throughout the world."[21] In addition to their access to fiber-optic cables within the US, the NSA extends its access to international territory through its partnership with Britain's GCHQ, which has its own program called Tempora to gather large quantities of phone and internet traffic through tapping into fiber-optic cables.[22] Working together, these programs allow the GCHQ and the NSA to look into the communications (such as recordings of phone calls, the content of emails, Facebook entries, and internet website access history) of huge quantities of people, in addition to targeted suspects.[23]

The Guardian reports that in addition to the NSA's "upstream" programs, they have Prism, which is shown in the leaked Snowden documents to be the biggest single contributor to its intelligence reports.[24] This program collects data from Google, Facebook, Apple, Yahoo, and other US internet giants through a "downstream" method, as the NSA has stated, in a completely legal fashion: "NSA works with a number of partners and allies in meeting its foreign-intelligence mission goals, and in every case those operations comply with US law and with the applicable laws under which those partners and allies operate."[25]

Finally, another classified document provided by Snowden has shown that the NSA has monitored the phone conversations of 35 world leaders, due to their encouragement of senior officials within "senior departments" (such as the White House) to share their contacts in order to add these foreign politicians to their monitoring system.[26]

Case Study: U.S cyber-attack on China (Snowden Documents)

Introduction to the incident

The NSA has already been revealed to have the power to monitor not only its own citizens, but also the citizens and leaders of foreign nations. Perhaps the most important nation for the NSA's hacking team is China, which has risen to be an economic superpower on the international stage. Due to the high level of secrecy maintained by the the government of the People's Republic of China , American surveillance agencies (most notably the NSA) have had a long history of targeting the

[21] Macaskill, Ewen, and Gabriel Dance. "NSA Files: Decoded- What the Revelations Mean for You." The Guardian. November 1, 2013. Accessed May 1, 2015.
[22] Macaskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications." The Guardian. June 21, 2013. Accessed June 6, 2015.
[23] Ibid.
[24] "NSA Files: Decoded- What the Revelations Mean for You."
[25] Ibid.
[26] Ball, James. "NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts." The Guardian. October 25, 2013.

communications networks that operate in China in order to gain intelligence on political intentions of the country, particularly for security concerns. Many have described this ongoing reciprocal hacking war as the “modern cold war” as the spending by the USA’s espionage empire has exceeded the level of espionage spending at the height of the Cold War.[27]

The resulting damage

In 2014, Edward Snowden leaked another set of crucial documents to both *The New York Times* as well as to Der Spiegel that revealed the NSA’s counterintelligence operations against the Chinese telecommunications company, Huawei. According to *The New York Times*, American officials consider the telecommunications giant to be a security threat against American corporate and governmental secrets. The United States has made an elaborate case against Huawei, and has blocked the company from business deals in the States due to the fear that they would place “back doors” in their equipment that could allow the Chinese military or government-supported hackers access to intelligence within The United States. [28]

However, Snowden revealed that the National Security Agency has been doing the same thing within Huawei’s networks: the documents show that the NSA gained access to Huawei’s tightly secured servers in Shenzhen, China. This has allowed them to acquire information concerning the workings of Huawei’s giant routers and their complicated digital switches that are claimed to connect a third of the world’s population. The communications of top executives of the company have also been were also monitored. This operation, codenamed “Shotgiant”, aimed to investigate possible links between Huawei and the People’s Liberation Army, and as is written in one of the documents that the NSA stated: “We want to make sure that we know how to exploit these products,” it added, to “gain access to networks of interest” around the world.[29] Additionally, the document revealed their further desire to collect counterintelligence on Huawei-allied countries with high-priority targets, such as Iran, Afghanistan, Pakistan, Kenya, and Cuba.[30] Der Spiegel reports that the NSA also spied on the “former Chinese President Hu Jintao, the Chinese Trade Ministry, banks, as well as telecommunications companies.”[31]

Additionally, Edward Snowden told South China Morning Post that the NSA has also been spying on Tsinghua University, which is one of China’s biggest research institutions and the home to the world’s largest national research hub, the China Education and Research Network (CERNET).[32] This gives the NSA the opportunity to mine the information of the hundreds of millions of people using the popular network.

[27] "'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives."

[28] Sanger, David E., and Nicole Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat." The New York Times. March 22, 2014.

[29] "N.S.A. Breached Chinese Servers Seen as Security Threat."

[30] Ibid.

[31] "Targeting Huawei: NSA Spied on Chinese Government and Networking Firm - SPIEGEL ONLINE." SPIEGEL ONLINE. March 22, 2014.

[32] Rapoza, Kenneth. "U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press." Forbes. June 22, 2013.

Aftermath

Presidents Obama and Xi Jinping have begun talks about limiting the cyber conflict, although the release of such sensitive NSA documents reveal that a growing cyber war is continuing to escalate between the two countries. *The New York Times* reports that the NSA is tracking "more than 20 Chinese hacking groups – more than half of them Chinese Army and Navy units – as they break into the networks of the United States government, companies including Google, and drone and nuclear-weapon part makers, according to a half-dozen current and former American officials."[33] Der Spiegel reports on the American response to the allegations: "NSA spokeswoman Caitlin Hayden said she should could not comment on specific collection activities or on the intelligence operations of specific foreign countries, "but … that [US's] intelligence activities are focused on the national security needs of our country." She also said, "We do not give intelligence we collect to US companies to enhance their international competitiveness or increase their bottom line."" Xi has also continued to deny all accusations related to cyber attacks and said, "cyber theft of commercial secrets and hacking attacks against government networks are both illegal; such acts are criminal offences and should be punished."[34]

Comments on the incident

As can be seen above, the conflict between these countries continues with increasingly elaborate cyber-attacks coming from both counterintelligence agencies of The United States and China. Both nations claim to be attempting to de-escalate this conflict, but revealed documents tell us otherwise. During the months of August and September there were talks of US weighing the option of sanctioning China as a response to its cyber attacks[35], which became possible after Obama administration passed an executive order early April. [36]

Conclusion

To conclude, it is clear that the United States have devoted a considerable part of their national budget to counterintelligence, with a focus on cyber-attacks and espionage against China. Programs veiled in secrecy such as GENIE, Upstream, Prism, and Shotgiant show us that relations between The United States and China are stressed.

Questions to Consider

1. Are counterintelligence measures facilitated through programs such as GENIE, Upstream, Prism, and Shotgiant a violation of international law?
2. What resolutions can be implemented to de-escalate the cyber-conflict between the United States and China?

[33] "N.S.A. Breached Chinese Servers Seen as Security Threat."

[34] http://www.theguardian.com/world/2015/sep/22/xi-jinping-says-china-is-not-guilty-of-cyber-attacks-as-he-prepares-for-us-visit

[35] https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html

[36] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

Topic III: Cyber Security Collaboration

Introduction

The growing importance of friendly relations between China and the United States has been an issue since China's emergence as a leader in global economy. Ahead of these two countries lies an unprecedented opportunity to collaborate in maintaining world peace and reshaping global norms for the future. To do so, the two states will need to overcome various conflicts, which usually arise due to fundamentally different views on ethics.

Cyber security has been a matter of concern that has significantly affected US-China ties and international relations. Though commonly gestated as a strategic geo-political issue, the backbone of this issue is comprised of a series of ethical considerations. Additionally, it is widely believed that filling in some of the differences in the socio-political fabric can prove to be crucial in easing bilateral tensions and promoting cooperation than stringent negotiations between the two states.

These differences have led to growing suspicions between technology companies in the United States and China. Chinese critical sectors have asked for "De-Americanization" of the various ICT products as a part of the solution to improve infrastructure security and protection. Such a situation can severely hamper global innovation and trade and can lead to long-term losses for both countries. China and the United States must strive to come up with a pragmatic solution in order to address these issues relating to cyber security and identify common concerns to promote growth in the technology sector.[37]

Current measures employed by the US

John Kerry, U.S. Secretary of State, visited Beijing, China in June 2013 to negotiate a deal between the United States and China. According to the article that was published during his stay in Beijing, "An agreement on the establishment of a cyber-security initiative was foremost for Kerry who acknowledged that this issue was of a national security concern."[38] Hagel hinted that recent cyber attacks on US technology infrastructure has harmed the industry and imposed security concerns. He further stated that the attacks seem to be tied to the Chinese military and government, which has instigated the US government and technology industry to grow skeptical about businesses affiliated with China.

Cyber attacks on US defense contractors such as Lockheed Martin and Raytheon have raised questions about the possibility of remotely activating an overseas US military installation to attack potential US targets. However, Kerry then pointed out that

[37] Robert D O'Brien, "The U.S., China, and Cyber Security: The Ethical Underpinnings of a Controversial Geopolitical Issue," *Carnegie Council (2014)*

[38] Sussane Poel, "Hagel: US & China to Collaborate on Cyber Security Working Group", *Sussane Posel*

recognizing the value of eased bilateral relations between the two major economies, US is determined to collaboratively work with China and affiliated businesses to introduce international norms regarding security and protection.

How is America dealing with the issue of cyber security?

Scope

The current focus is on improving critical infrastructure including government services and systems of predefined sectors largely managed by private sector. The federal and state government information systems may be subject to different security requirements based on risk assessment.

Enforcement methods

The government is trying to enforce the improvement through laws, presidential and executive orders. These were some of the measures the U.S. government has taken to deal with the situation:

1. International and domestic security measures are exercised to ensure higher Internet information security.
2. Voluntary compliance for most government sectors and large private sectors under the Critical Infrastructure Cybersecurity program.
3. Potentially mandatory for related entities, but values industry self-regulation.
4. Mandates security compliance for configuring desktops and procuring out services for the federal government
5. Encourages public-private partnership for meaningful information sharing
6. Values industry self-regulation and timely incident response
7. The U.S. does not have any cyber security legislations as of now, but do have the White House Cybersecurity Directives as an effort to ensure higher security.

As briefly aforementioned, In April this year, President Obama signed an executive order which defines foreign cyber attacks on US entities “a national emergency” and “an unusual and extraordinary threat.”[39] It is grounded in the International Emergency Economic Powers Act which was passed in 1977 allows the president to declare “national emergency” on “any unusual and extraordinary threat” to national security, foreign policy or economy

Figure 4 White House

[39] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

of the United States that originates from outside of the country.[40] The executive order expands the legal scope of actions to be taken by the US government as a response to cyber terrorism. It allows the US Treasury Department to freeze financial assets of and bar commercial transactions with individuals and entities overseas that allegedly take part in cyber crimes. Acting on the directive requires consultation with the Justice and State Departments as well as evidence to withstand a court challenge. Such evidence must prove the crime falls under one of these four “harms”: it harms computer networks of a major infrastructure sector; disrupts provision of services by US entities; limits availability of computer networks; or allows parties to benefits from the gains of a cyber attack.[41] If the administration decides to advance on the sanctions, it would mark the first time this executive order comes into effect. (Following North Korea’s cyber attack on Sony Pictures in January, Obama issued an executive order to impose financial sanctions on certain officials and government entities.[42] However, the order claimed that the sanctions authority was not specific to cyber activity and the individuals were not targeted solely for their involvement in the cyber espionage.[43])

Current measures employed by China

China’s National Computer Emergency Response Team (CNERT/CC), answerable for any cyber attacks or security breaches in China, recognized the growth of domestic hacking in China and advised on taking actions to avoid such malpractice. They called for stronger data security measures on Internet and conduct awareness programs regarding cyber security among the youth. Furthermore, they asked to further strengthen the technology used by network security agencies to discover vulnerabilities in software that can lead to exploitation of data crucial to national security.[44]

PHOTO: GOH CHAI HIN/AFP/GETTY IMAGES

Then in August 2013, the Ministry of Industry and Information Technology introduced a plan, “Prevent and Combat the Hacker Underground Supply Chain,”, which advocated an extensive and pragmatic solution to mitigate damages that are a consequence of cyber security breaches and to introduce robust data security measures.

[40] http://www.treasury.gov/resource-center/sanctions/Documents/ieepa.pdf

[41] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

[42] https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea

[43] https://www.washingtonpost.com/world/national-security/us-to-establish-sanctions-program-to-combat-cyberattacks-cyberspying/2015/03/31/7f563474-d7dc-11e4-ba28-f2a685dc7f89_story.html?wpmk=MK0000203

[44] Paul Mozur, “ New Rules in China Upset Western Tech Companies,” *New York Times (2015)*

In early 2015, Chinese government required US-affiliated software companies to handover their software details, and instead use encryption algorithms provided by Beijing. Moreover, US technology corporations, including Cisco and Microsoft, were pressurized by China to undergo rigorous security checks before their products are integrated with machines used by Chinese financial institutions. These actions were a consequence of the revelations by former National Security agency contractor, Edward Snowden. He reported that US spying agencies planted code in software, to extract valuable information on overseas targets.[45]

How is China dealing with the issue of cyber security?

Scope

Figure 5 src=shutterstock

Current measures classify the government systems meeting the requirement of Level 3 under the Multi-level Protection Scheme as critical infrastructure. Eight industry sectors that are state-owned and operated such as banking, financial services, transportation, energy, etc. are now regarded as critical infrastructure.

Internet information security has become a key element of critical infrastructure protection with nine types of content defined as illegal. As a result, it now requires “Real Name Registration” for all Internet users.

Enforcement methods

The Chinese government is handling the situation by introducing various laws, policies, regulations, standards, licensing schemes, certification schemes and Five Year plans.

The enforcement methods are being exercised through the following actions:

1. Based on domestic security standards and adopted standards based on ISO/IEC and ITU. Developed largely by domestic entities with limited public comment period (30 days)
2. National security strategy, including focus on creating cyber security legal framework
3. Mandates compliance with Internet information security laws and regulations by the Internet industry and the public.
4. Mandates compliance of Multi-level Protection Scheme for government systems nationwide and for significant Internet services. 5. Mandates compliance of multi-level protection scheme for government systems nationwide and for significant Internet services
5. Limits any use of security products for MLPS Level 3 systems and higher to only those listed in the certified security product catalog

[45] Jing De Jong-Chen, “U.S.-China Cyber Security Relations : Understanding China’s Current Environment,” Georgetown Journal of International Affairs (2014)

6. Requires mandatory security product certification (China compulsive compliance) for government procurement (MLP S Level 3 systems and higher)
7. Mandatory encryption regulation requires support for Chinese cryptography algorithms at all levels
8. Requires mandatory reporting by Internet Service Providers (ISPs) to law enforcement agencies for any information system that connects to an overseas network.
9. Mandates Internet Service Providers (ISPs) notify customers of security breaches in less than 15 days

Conclusion

As a result of fundamentally different views on security and foreign policy, it is difficult the United States and China to collaborate on cyber security and data protection. However, acknowledging the importance of eased relations between these two states to maintain global peace, it is imperative that negotiations are done to protect cyber sovereignty.[46]

Political imperatives are unique to political issues. Progressive relationship between the citizens of US and China can get severely damaged if the issue of cyber security is not handled immediately. [47]As a result, it can impede the capacity of global collaboration to combat cybercrimes and can weaken the interdependencies in the social, political and economic fabric of the two states.

Questions to Consider

1. How do the United States and China move away from the mistrust that currently governs the relationship?
2. How could the U.S. and China find common ground on cyber sovereignty despite their current disagreement?
3. With fundamentally different political and social systems, how would the U.S. and China align their national security interests with global benefits to protect cyber infrastructure and trade?
4. What security policies and legal frameworks are needed to promote global collaboration and supply chain trust?
5. What are the key roadblocks in creating effective policies for cyber security in the United States and China?

[46] Executive Yuan, "ROC calls for cyber security collaboration with the U.S." *Department of Information Services (2015)*

[47] Christopher Bodeen, "New Chinese Law enforces reinforces government control of cyberspace" *Yahoo News! (2015*)

Helpful Links

"Google Aurora Hack Was Chinese Counterespionage Operation." Dark Reading. N.p., n.d. Web. 16 Apr. 2015. <http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060>
This website briefly outlines Operation Aurora's attack against Google in late 2009. It gives high-profile information from Symantec that the operation was still at work as of 2012, and gives names of a few other American corporations targeted during the operation.

"Google Hack Attack Was Ultra Sophisticated, New Details Show | WIRED." Wired.com. Conde Nast Digital, n.d. Web. 16 Apr. 2015. <http://www.wired.com/2010/01/operation-aurora/>
This site explains the origins of the name of operation Aurora, as well as details elaborating how the attacks were performed. It also details some protection methods, such as McAfee enhancing their products to detect malware used in attacks. Additionally, it gives testimony from iDefense that explains some of the reasons why the corporations were vulnerable to attacks.

"In Google Attack Aftermath, Operation Aurora Keeps on Hacking." In Google Attack Aftermath, Operation Aurora Keeps on Hacking. N.p., n.d. Web. <http://www.technewsworld.com/story/76109.html 16 Apr. 2015.>
This site outlines how the operation is government-sponsored. It gives an overview of the attacks, the flaws that were exploited, explains spearphishing, and describes how the hacker group Anonymous was likely not involved in the attacks.

"'Aurora' Cyber Attackers Were Really Running Counter-Intelligence." CIO. N.p., n.d. Web. 16 Apr. 2015. <http://www.cio.com/article/2386547/government/-aurora--cyber-attackers-were-really-running-counter-intelligence.html>
This site details some conspiracy theories about Chinese hackers – it gives a new, foreign perspective of the attack on Google. The argument in this article seeks to reveal how the hackers were actually attempting to determine the types of surveillance U.S. authorities were conducting on undercover operatives.

"Lessons Learned from Investigating the Google Attacks -- GCN." Lessons Learned from Investigating the Google Attacks -- GCN. N.p., n.d. Web. 16 Apr. 2015. <http://gcn.com/articles/2010/09/06/interview-george-kurtz-mcafee-google-attacks.aspx>
This site gives a detailed explanation of what exactly Operation Aurora is. It showcases why the attacks got so much publicity in the security community, what lessons have been learned, some long-term damage, and some of the threats we face today.

"Lessons from Google Attacks Could Help US Bolster Cyber Defense -- GCN." Lessons from Google Attacks Could Help US Bolster Cyber Defense -- GCN. N.p., n.d.

Web. 16 Apr. 2015. <http://gcn.com/articles/2010/04/16/dewalt-on-cybersecurity-041510.aspx>
This website is a great source for learning about how to mitigate future attacks. It reveals that real-time intelligence gathering and response is the key to being a step ahead of the attackers.

"Hackers Attack Google Using Microsoft Security Hole -- GCN." Hackers Attack Google Using Microsoft Security Hole -- GCN. N.p., n.d. Web. 16 Apr. 2015.
<http://gcn.com/articles/2010/01/15/zero-day-bug-internet-explorer-google-attack.aspx>
This website gives a few details on how Operation Aurora happens, and elaborates on the security hole that allowed Chinese hackers to infiltrate American corporations.

"What You Need to Know (and Don't) About the AURORA Vulnerability - POWER Magazine." POWER Magazine. N.p., n.d. Web. 16 Apr. 2015.
<http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/>
This site demonstrates how the operation was widespread – it planted a seed that would keep growing long after the attack was supposedly "over" in 2007. It outlines that the cost to mitigate future attacks is relatively low, but how almost nothing has been done to help protect the grid from future "potentially devastating consequences".

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Amsterdam [Netherlands: Morgan Kaufmann Publishers, an imprint of Elsevier, 2013. Internet resource.
<http://www.sciencedirect.com.proxy3.library.mcgill.ca/science/book/9780124078147>
This book has information relating to the thinking of Chinese military thinkers on cyber espionage. It also briefly outlines the types of property theft during Operation Aurora. In addition, it gives information about the more recent Chinese-attributed operation, which used the "Sykipot" malware to pirate material related to U.S. unmanned aerial vehicles.

"Cyber Security Collaboration: A Critical Ingredient for Worldwide Security"
Entrust (November 2003)
https://www.entrust.com/wp-content/uploads/2013/05/cybersecurity_collaboration.pdf
How to actually define cyber security collaboration. What are the fine aspects that need to be observed and how the international society can be saved from such damage?

"Cyber Security: More Than a Good Headline" *Microsoft Corporation (October 2011)*
https://partner.microsoft.com/download/global/40177195
Microsoft's in-depth view on cyber security and the measures that be taken to protect against cyber warfare. It then explains how the Cybersecurity Agenda (or program) must be embedded in a country's existing legal framework, find cultural and social acceptance, and be technically and economically feasible.

"US and China form working groups to collaborate on cyber security, climate change", *The Verge (April 2013)*
http://www.theverge.com/2013/4/13/4220874/united-states-china-form-working-groups-cybersecurity-climate-change
U.S. Secretary of State John Kerry's trip to Beijing to speak about the recent cyber espionage and to negotiate with the Chinese government to prevent such situations in the future.

Works Cited

"APT1: Exposing One of China's Cyber Espionage Units." *Mandiant* (n.d.): n. pag. Web. 1 May 2015. <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

Baker, Peter. "Obama Expands Options for Retaliating Against Foreign Hackers." *The New York Times*. N.p., 01 Apr. 2015. Web. 01 May 2015. <http://www.nytimes.com/2015/04/02/us/politics/us-expands-foreign-cyberattack-retaliation-options.html?_r=0>.

Ball, James. "NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts." *The Guardian*. N.p., 25 Oct. 2013. Web. <http%3A%2F%2Fwww.theguardian.com%2Fworld%2F2013%2Foct%2F24%2Fnsa-surveillance-world-leaders-calls>.

"The Black Budget: Explore Top Secret U.S. Intelligence Funding." *Washington Post*. N.p., n.d. Web. 01 May 2015. <http://www.washingtonpost.com/wp-srv/special/national/black-budget/?hpid=z5>.

"Cyber Security Primer." *What Is Cyber Security?* N.p., n.d. Web. 01 May 2015. <http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm>.

"Cyberattack on U.S. Infrastructure: A Highly Disruptive Cyberattack on U.S. Critical Infrastructure." *Council on Foreign Relations*. N.p., n.d. Web. 01 May 2015. <http://www.cfr.org/global/global-conflict-tracker/p32137#!/?marker=2>.

Gellman, Barton, and Ellen Nakashima. "U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show." *Washington Post*. N.p., 30 Aug. 2013. Web. 01 May 2015. <http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html>.

Gellman, Barton, and Greg Miller. "'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives." *Washington Post*. N.p., 29 Aug. 2013. Web. 06 June 2015. <http://www.washingtonpost.com/world/national-

security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html>.

Green, Marcel A. "China's Growing Cyberwar Capabilities." *The Diplomat*. N.p., n.d. Web. 01 May 2015. <http://thediplomat.com/2015/04/chinas-growing-cyberwar-capabilities/>.

"The History of Cyber Attacks - a Timeline." *NATO Review*. N.p., n.d. Web. 01 May 2015. <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>.

Knake, Robert. "Cybersecurity Legislation in Congress: Three Things To Know." *Council on Foreign Relations*. N.p., 30 Apr. 2015. Web. 01 May 2015. <http://blogs.cfr.org/cyber/2015/04/30/cybersecurity-legislation-in-congress-three-things-to-know/>.

Macaskill, Ewen, and Gabriel Dance. "NSA Files: Decoded- What the Revelations Mean for You." *The Guardian*. N.p., 1 Nov. 2013. Web. 1 May 2015. <http%3A%2F%2Fwww.theguardian.com%2Fworld%2Finteractive%2F2013%2Fnov%2F01%2Fsnowden-nsa-files-surveillance-revelations-decoded%23section%2F1>.

Macaskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications." *The Guardian*. N.p., 21 June 2013. Web. 6 June 2015. <http%3A%2F%2Fwww.theguardian.com%2Fuk%2F2013%2Fjun%2F21%2Fgchq-cables-secret-world-communications-nsa>.

Rapoza, Kenneth. "U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press." *Forbes*. N.p., 22 June 2013. Web. <http://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/>.

Sanger, David E., and Nicole Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat." *The New York Times*. N.p., 22 Mar. 2014. Web. <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=1>.

"Targeting Huawei: NSA Spied on Chinese Government and Networking Firm - SPIEGEL ONLINE." *SPIEGEL ONLINE*. N.p., 22 Mar. 2014. Web. <http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html>.