General Assembly

Digital Geneva Convention

St. John's Preparatory School • Danvers, Massachusetts • 9 December 2017

SJPMUN XII

building a better tomorrow

Letter From the Author

Greetings Delegates,

Hello, my name is Chris Jerrett and I am the author of this paper. Aside from writing this paper I also serve as Secretary General for SJPMUN XII. Sadly, I will not be able to chair this committee, but I will make sure your chair is competent and friendly. Outside of MUN I also am the Software Captain of the robotics team and a member of the Spire Society and National Honor Society. The topic of cybersecurity is an incredibly interesting topic to me because the topic has been a rather niche and minor topic up until recently with the growth of the importance of computers in modern life. In addition I love the merger of technology, policy and ethics. Very few other topics have such a diverse range of fields involved. I look forward to seeing what ideas the committee has in store to stole this dynamic and pressing topic. If you ever see me walking around during the conference feel free to talk to me!

Sincerely,

Chris Jerrett ‘18

Author and Secretary General

Committee Description

The General Assembly is often what comes to mind when one first thinks of the United Nations. Commonly abbreviated as the GA, the General Assembly is the main deliberative, policymaking, and representative organ of the United Nations, where decisions on questions like peace and security, admission of new members to the UN, and budgetary matters, among others, occur.[1] Each country has one vote, regardless of size or population, and, depending on its importance, a resolution requires either a simple majority or a two-thirds majority to pass. Generally speaking, the most successful measures are those in which the entire GA has reached a consensus. However, for such a large committee to be successful, it is absolutely necessary to hear all perspectives from all delegates. Members of the General Assembly work together to find common ground and agree on solutions to injustices and problems that afflict the world before they become conflicts.

History of the Problem

Perhaps the first use of computers for offensive purposes was code breaking during the second world war. Alan Turing, known to many as the father of computer science, become famous after building the “bomb machine” which enabled the Allies to break the German Enigma cipher.[2] In 1989

[1] "United Nations, main body, main organs, General Assembly." United Nations. Accessed September 19, 2017. http://www.un.org/en/ga/about/background.shtml

[2] Crypto Museum. "Bombe." Bombe. Accessed October 10, 2017. http://www.cryptomuseum.com/crypto/bombe/.

Robert Morrison created the first known computer worm, or self propagating program. Morrison's worm was so successful because of the lack of protection that is managed to shut down the entire internet in through a *de facto* denial of service (DOS) attack.[3] Morrison's worm created the cybersecurity industry that we know today and demonstrated the dramatic effects of poor cybersecurity.

The Melissa and ILOVEYOU viruses during the 1990s again proved the importance of cybersecurity by infecting millions of computers and email systems. Unlike Morrison's worm, these viruses had a clear financial motive. Between 2005 and 2007, Albert Gonzalez stole 45.7 million payment cards used by customers of TJX, costing the company over $256 million.[4] In April of 2007 the Estonian government faced a denial of service attack from Russia following a disagreement over the removal of a statue. In the summer of 2008 the private email accounts of US presidential candidates was hacked by unknown actors.

In October of 2010 the largest computer virus, the Stuxnet Virus was discovered by security researchers. The virus spread to millions of computers and infected flash drives. These flash drives targeted specific Siemen Programmable Logic Controllers which were used by Iranian nuclear centrifuges. The virus succeeded in destroying Iranian infrastructure and served as a warning sign.

---

[3] Ted Julian Former IDC/Forrester analyst and CMO, CO3 Systems. "Defining Moments in the History of Cyber-Security." Infosecurity Magazine. December 04, 2014.

[4] Ibid

Statement of the Problem

The ever increasing importance of the internet and cyberspace in modern life serves as an incentive for both states and non-state actors to engage in cyber warfare, cyber espionage and cyber crime. The increased complexity of the internet and importance in modern day life creates a need for the a international body to create rules governing crimes between states and individuals. Because of lack of a need for physical presence most states lack the capability to legally respond within their own domestic legal frameworks. Little in terms of legal frameworks governing warfare, espionage and crime have been created for cyberspace.

Currently, an estimated 140 nations are developing cyber warfare capacity.[5] Many states are investing in cyberwar because of its low cost, low manpower requirements, and anonymity.[6] As the cyber domain has rapidly evolved in only the last few years, the United Nations collectively has done little about the cyber domain, in fact the United Nations lacks a definition of cyber-warfare and cyber-espionage and even may outside experts have trouble defining the issue.[7] The inactivity of the international community on the issue of cyber warfare and cyber espionage has caused corporate leaders, such as Microsoft's President and Chief Legal Officer, Brad Smith, to call for a new "Digital Geneva

[5] Brenner, Susan W., and Leo L. Clark. "Civilians in Cyberwarfare: Conscripts." Vanderbilt Journal of Transnational Law 43. Accessed September 10, 2017.

[6] Ibid

[7] Michael, Beaver, "THE UNITED NATIONS AND CYBERWARFARE." Global Risk Advisors. Last modified September 28, 2016. Accessed June 14, 2017.

Convention." Brad Smith called for a new bold and radical solution to prevent and protect from cyber-crime and cyberwarfare, stating, "Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace."[8]

Estimates predict the cost of cybercrime prior to 2019 to cost 2.1 trillion globally, a number which has tripled from 2015 estimates.[9] The increasing prevalence of government and large corporations relying on digital storage and computation has led to nation states and nonstate actors investing heavily into their cyber warfare capacities. The most notable example of state sponsored cyber war has been between the United States of America and the People's Republic of China, within the United States routine corporate and governmental intrusions became commonplace. Companies including the

[8] Brad, Smith, "The Need for a Digital Geneva Convention." Microsoft On the Issues (blog). Entry posted February 14, 2017. Accessed June 14, 2017.

[9] Information Systems Audit and Control Association. "State of Cybersecurity: Implications for 2016 ." State of Cybersecurity: Implications for 2016. Accessed September 16, 2017.

New York Times,[10] Google,[11] American Superconductor,[12] and thousands of others[13] have claimed to have their intellectual property stolen by People's Liberation Army unit 61398.[14]

Many companies have come forth with information and allegations that they have been the target of Chinese cyber espionage to steal trade secrets. The United States government also claims to be the target of Chinese attacks, perhaps the largest of which is the breach into the office of personnel management's records of over 16 millions American citizens.[15] According to leaked NSA documents over a five year period the NSA recorded more than 600 attacks on US industrial interests all of which could be traced back to Chinese hackers.[16] In 2014 the United States Department of Justice responded to evidence of Chinese hacking by indicating five Chinese Army officers tasked with the country's of-

[10] Fidler, David P. "Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies."

[11] Google. "A new approach to China." Official Google Blog. January 12, 2010. Accessed September 16, 2017.

[12] Stahl, Lesley. "The Great Brain Robbery." CBS News. January 25, 2016. Accessed September 16, 2017. https://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/.

[13]Ibid

[14] Fidler, David P. "Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies."

[15] Lorenzo Franceschi-Bicchierai to Vice News newsgroup, "How the Chinese Government Became the World's Hacking Superpower," July 26, 2016, accessed June 15, 2017,

[16] Robert Windrem to NBC newsgroup, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," July 30, 2015, accessed June 15, 2017,

fensive cyber activities. The United States does admit to engaging in cyber warfare, but not for the benefit of American Corporations.[17]

In an attempt to try to resolve problems of cyber espionage between the two countries in 2015 the US and China signed a joint agreement to increase cooperation in cyberspace and to halt their cyber espionage activity. The agreement between United States President Barack Obama and Chinese President Xi Jinping agreed to, stop all cyber theft of corporate trade secrets, prosecute cyber criminals within national legal frameworks, and the establishment of high level joint framework between the two counties.[18]

In addition cyberwarfare has interfered with democratic processes in multiple countries, most recently in the 2016 United States Presidential campaign. Both side accused Russia of engaging in disinformation and hacking and leaking confidential information. Fear of potential tampering with voter registration, accessing voting machines, manipulating storage and transmission of results also spread. Similar fears spread in France, Britain and the Netherlands.[19] Elections are a nation's sovereign territory and interfering in elections or domestic affairs violates Chapter I, Article 2, paragraph 7 of the Unit-

[17] Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace," The Diplomat, last modified January 19, 2017.

[18] Ibid

[19] Fidler, David P. "Transforming Election Cybersecurity." Council on Foreign Relations. May 17, 2017. Accessed September 06, 2017.

ed Nations Charter. As computers and information technology becomes more ingrained in governing legislative frames must be put into place to address issues relating to sovereignty.

Unlike many other vectors of attack cyber offers the added challenge of trying to correctly attribute an attack or hack. Currently, means of attributing the source of an intrusion can be incredible resource intensive and therefore something many companies are not willing to invest in.[20] Though expensive some firms are finding that multileveled and cooperative defense to be less resource intensive and more reliable. These systems work by pooling resources to conduct malware analysis and fingerprinting. Though with such a wide range of information sharing hands a privacy concern still has prevented compete implementation. Adding to the difficulty of attribution is the risk of a false flag attack. Attackers can impersonate another actor during a hack, leading a false trail back to a third party. For example Iranian Hackers have been known to use arabic (instead of farsi) while planning hacks. It was not until linguists teamed with cyber security professionals that the true source was uncovered. A hacker may use false flag attacks either to cover his or her tracks or to intentionally create hostility between the hacked and impersonated party.

Cybercrime and cyberwarfare, similarly to their more conventional counterparts, can have serious damage to civilians and have grave humanitarian impacts. Though, currently the Geneva Con-

[20] Thomas, | Hank. "Looking for a Smoking Gun Behind a False Flag Attack – The Cipher Brief." The Cipher Brief. July 25, 2017. Accessed September 19, 2017.

vention only protects civilians against cybercrime and cyberwarfare. Though, a critical distinction between conventional warfare and cyberwarfare is in cyberwarfare civilian owned system are more likely to be targeted because attacker would most likely be more concerned with attacking the viability of the target nation, not violating it territory.[21] In armed conflict civilians are protected by International Humanitarian Law, with many hackers and cyber warriors being civilians, they too are protected too from being directly targeted in armed conflict.[22] Though cyber warfare may exist in cyberspace it still can manifest itself in the physical world and thus humans can become casualties from cyberwarfare and cybercrime. Civilians can suffer from cyber warfare through direct casualties as a consequence of cyberwarfare, as means of attacking other targets, through an indirect attack or as a governmental response to cyber warfare.[23] In is thus important for civilian suffering to be minimized.

Questions To Consider

1. What rights do citizens have online?
2. How should governments protect these rights more effectively?
3. How should governments protect privacy?

---

[21] Brenner, Susan W., and Leo L. Clark. "Civilians in Cyberwarfare: Conscripts." Vanderbilt Journal of Transnational Law 43. Accessed September 10, 2017.

[22] International Committee of the Red Cross. "Cyber warfare and international humanitarian law: The ICRC's position." June 2013.

[23] Brenner, Susan W., and Leo L. Clark. "CIVILIANS IN CYBERWARFARE: CASUALTIES ." *University Of Pennsylvania Law*. Accessed September 10, 2017.

4. How should governments protect citizens from non-state and state sponsored actors?

5. What rules should govern cyber warfare?

6. How is cyber warfare defined?

7. Who has jurisdiction in cyberspace?

8. How can governments work together to prevent cybercrime?

Bloc Positions

Nations affected by cybercrime and cyberwarfare:

These nations have been targets of both non-state and state sponsored acts and as such want more international cooperation on the issue. These nations may pursue more strict guidelines, and more communication between nations to prevent cyber warfare. Some of these nations may have or are developing cyber warfare offenses and defenses.

Nations committing cyberwarfare:

These nations see cyber warfare as a national security and economic issue and an important part of one's military. They would be reluctant to have their offensive abilities reduced.

Works Cited

Brad, Smith, "The Need for a Digital Geneva Convention." Microsoft On the Issues (blog). Entry posted February 14, 2017. Accessed June 14, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hh0sza6bjfakrbz24kbh3-cus4.

Brenner, Susan W., and Leo L. Clark. "Civilians in Cyberwarfare: Conscripts." Vanderbilt Journal of Transnational Law 43. Accessed September 10, 2017. https://www.vanderbilt.edu/wp-content/uploads/sites/78/Brenner-_Final_1.pdf.

Crypto Museum. "Bombe." Bombe. Accessed October 10, 2017. http://www.cryptomuseum.com/crypto/bombe/.

Fidler, David P. "Transforming Election Cybersecurity." Council on Foreign Relations. May 17, 2017. Accessed September 06, 2017. https://www.cfr.org/report/transforming-election-cybersecurity.

Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace," The Diplomat, last modified January 19, 2017, accessed June 15, 2017, http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.

Google. "A new approach to China." Official Google Blog. January 12, 2010. Accessed September 16, 2017. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Information Systems Audit and Control Association. "State of Cybersecurity: Implications for 2016 ." State of Cybersecurity: Implications for 2016. Accessed September 16, 2017. http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2016.aspx.

International Committee of the Red Cross. "Cyber warfare and international humanitarian law: The ICRC's position." June 2013. https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf

Lorenzo Franceschi-Bicchierai to Vice News newsgroup, "How the Chinese Government Became the World's Hacking Superpower," July 26, 2016, accessed June 15, 2017, https://motherboard.vice.com/en_us/article/how-the-chinese-government-became-the-worlds-hacking-superpower.

Michael, Beaver, "THE UNITED NATIONS AND CYBERWARFARE." Global Risk Advisors. Last modified September 28, 2016. Accessed June 14, 2017. https://globalriskadvisors.com/blog/united-nations-cyber-warfare/.

Robert Windrem to NBC newsgroup, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," July 30, 2015, accessed June 15, 2017, http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

Stahl, Lesley. "The Great Brain Robbery." CBS News. January 25, 2016. Accessed September 16, 2017. https://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/.

Ted Julian Former IDC/Forrester analyst and CMO, CO3 Systems. "Defining Moments in the History of Cyber-Security." Infosecurity Magazine. December 04, 2014. Accessed October 10, 2017. https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/.

Thomas, | Hank. "Looking for a Smoking Gun Behind a False Flag Attack – The Cipher Brief." The Cipher Brief. July 25, 2017. Accessed September 19, 2017. https://www.thecipherbrief.com/looking-for-a-smoking-gun-behind-a-false-flag-attack.

"United Nations, main body, main organs, General Assembly." United Nations. Accessed September 19, 2017. http://www.un.org/en/ga/about/background.shtml.