Digital Geneva Convention
St. John's Preparatory School - Danvers, Massachusetts - December 2019

Letter From the Chair

Dear Delegates,

Welcome to SJPMUN XIV! My name is Conor Beswick, I'm a sophomore at St. John's Prep. This is my first year doing High School Model UN, but I participated in Middle School Model UN for 2 years. I'm a three season student athlete (Football, Fencing, Crew). We had some problems at the last minute with the topic of Security vs. Privacy so the Secretariat and I decided that this would be the best topic to debate. We would like to give credit to the writer of this paper, Chris Jarett. Chris graduated from here a few years ago and we are very excited to be using his paper. I am excited to see you on the 14th and please email me if you have any questions.

Cbeswick22@stjohnsprep.org.

Sincerely,

Conor Beswick, Chair

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.

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

Statement of the Problem

Modern warfare no longer adheres to the rules set by history, today, the battle is fought both on the field and on the web. The problem herein lies that the citizens are under a new, additional threat to safety from the crossfire of nations going head to head. While cyber-warfare is not yet a common means to do battle, the increasingly digital world promises that it will be a bigger threat in the future. Whether it be identity theft, monitoring citizens' activities, jeopardizing the democratic process, disabling communication and financial systems, or attacking the power grid, cyber-warfare has the potential to wreak havoc on the citizen population of nations. Citizens should not be put in a position of great loss, or be used as pawns for leverage against their own government, just as POWs were used against their own government in WWII. This committee must update the Geneva Conventions to include destructive acts resulting from cyber-warfare.

What we are not talking about: Cyber-crime. In May 2017, WanaCry was a ransomware that targeted Windows computers with the unpatched Windows 10 software, and encrypted important files on these computers, demanding payment in Bitcoin for decryption. WanaCry has roots in North Korea, and attacked the British National Health Service, along with many computers in Britain and America, which has left many to believe that this was likely a coordinated attack by the North Korean government. Another example of cyber-crime was the ILOVEYOU viruses from the 1990s. These reinforced the importance and need of cybersecurity by infecting millions of computers and email systems. Unlike earlier worms 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[2]. While cybercrime acts

[2]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/.

against the interests of civilians, this committee will not be covering it. Cybercrime and cyber warfare are two different subjects, and this “Geneva Convention” will only be covering the warfare aspect of cyber attacks.

History of the Problem

As nation-states and the responsibilities of governments for their citizens evolved to replace empires, and modern warfare extended the destructive possibilities of war reached more deeply into the civilian population, the Geneva Conventions created a rules of war regarding the protection of civilians. The 1st Geneva Convention (1864) stated that there should be no discrimination of race, religion, or ethnicity when distributing treatment to wounded soldiers. It also addressed the topic of torture, saying that torture and the destruction of personal dignity must be prohibited. "After the Nuremberg and Tokyo trials, numerous international treaties and conventions attempted to devise a comprehensive and enforceable definition of war crimes. The four separate Geneva Conventions, adopted in 1949, in theory made prosecutable certain acts committed in violation of the laws of war. The conventions provided for the protection of wounded, sick, and shipwrecked military personnel, prisoners of war, and civilians. Like the convention on genocide, however, the Geneva Conventions specified that trials were to be arranged by individual governments" (Penrose)[12]. The 2nd Convention (1949) replaced the Hague Convention (1907) and focused on the protections of shipwrecked soldiers and medical ships. The 3rd Convention (1949) gave protections to, and defined, "prisoners of war", while the 4th Convention gave protections to civilians who are in situations of war or occupancy, essentially protecting places like hospitals.[3] While the Geneva Conventions, prior to 1993, did not have a binding aspect, after 1993 the Security Council adopted a resolution that would

[3] Staff, LII. "Geneva Conventions." LII / Legal Information Institute, 19 June 2017, www.law.cornell.edu/wex/geneva_conventions.

"[make] them binding on non-signatories to the Conventions whenever they engage in armed conflicts"[4].

The advent of the Internet changed the nature of warfare. Perhaps the first use of computers for defensive purposes was code breaking during the WWII. Alan Turing, known to many as the father of computer science, became famous after building the "bomb machine" which enabled the Allies to break the German Enigma cipher[5]. For a long time afterward, computers were seen as a tool to manage the data in creating traditional defensive or offensive weapons systems. However, in 1989 Robert Morris created the first known self-propagating program or computer worm. Morris's worm was very destructive because the Internet lacked protective mechanisms. It managed to shut down the entire Internet through a *de facto* denial of service (DOS) attack[6]. Morris's worm was the impetus for the cybersecurity industry that we know today and demonstrated the dramatic effects of poor cybersecurity. Worms have become even more sophisticated and dangerous today. NATO documented this progression of cyber attacks up to 2013, which can be found through the link[7]:

Cyber attacks, however, fall under one of two different categories: cyber warfare and cyber crime. According to John B. Sheldon, professor of cyber security at the School of Advanced Air and Space Studies,

> "Cyberwar, which can also be searched as cyber war, cyberwarfare or cyber warfare, is war conducted in and from computers and the networks connecting them, waged by states

---

[4] "Fourth Geneva Convention." *Wikipedia*, Wikimedia Foundation, 12 Nov. 2018, en.wikipedia.org/wiki/Fourth_Geneva_Convention.
[5] Crypto Museum. "Bombe." Bombe. Accessed October 10, 2017. http://www.cryptomuseum.com/crypto/bombe/.
[6] 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/.
[7] https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

> or their proxies against other states. Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use. Cyberwar should not be confused with the terrorist use of cyberspace or with cyber-espionage or cybercrime. Even though similar tactics are used in all four types of activities, it is a misinterpretation to define them all as cyberwar. Some states that have engaged in cyberwar may also have engaged in disruptive activities such as cyber-espionage, but such activities in themselves do not constitute cyberwar" (Sheldon)[13].

The distinction between these two types of attacks dictate what attacks will be covered in this committee, and therefore should be noted.

According to the definition provided by Sheldon, the modern world has and still does face instances of cyber warfare. In April of 2007 the Estonian government faced a denial of service attack from Russia following a disagreement over the removal of a statue.[8] This attack lead to the civilians facing failure of banking systems, specifically, "cash machines and online banking services were sporadically out of action"[9]. Furthermore, In the summer of 2008 the private email accounts of US presidential candidates was hacked by unknown actors.[10] Such election meddling, which could be the result of an outside government, leads civilians' actions in their own government to not have effect, thus interfering unfairly with the domestic life of citizens in an attack against the government.

The best possible outcome of cyberwarfare can be illustrated by the Stuxnet Virus. In October of 2010 the largest computer virus, the Stuxnet Virus, created by the American and

[8] McGuinness, Damien. "How a Cyber Attack Transformed Estonia." BBC News, BBC, 27 Apr. 2017, www.bbc.com/news/39655415.
[9] McGuinness, Damien
[10] Glendinning, Lee. "Obama, McCain Computers 'Hacked' during Election Campaign." The Guardian, Guardian News and Media, 7 Nov. 2008, www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

Israeli governments, was discovered by the infosecurity community. The virus spread to millions of computers worldwide and infected flash drives. These flash drives targeted specific Siemen Programmable Logic Controllers which where used by Iranian nuclear centrifuges and meant to destroy Iran's nuclear capability. The virus succeeded in destroying Iranian infrastructure and served as a warning to nations around the world regarding the danger and abilities of cyber attacks.[11] Unlike many other attacks, while Stuxnet infiltrated most of our computers, it did no harm. It only acted, with surgical precision on its specific target. Stuxnet proved itself to be an effective attack while avoiding civilian crossfire.

On the other hand, while it never came to fruition, the U.S. planned cyber-warfare towards Iran that would have greatly harmed its people. Prior to the Joint Comprehensive Plan of Action, commonly known as the Iran nuclear deal, the U.S. designed a cyber attack which would have destabilized all of Iran through the shutdown of power grids. Such a wide scale attack would have put the citizens in danger, trying to avoid violence without being able to freely communicate the upcoming danger with each other.[12] Unlike Stuxnet, this never went into effect, and from the limited details at hand, it can be assumed that such an attack would not act like Stuxnet, only attacking the target, instead having widespread effect and massive amounts of crossfire with civilians and their way of life. Updating the Geneva Convention is necessary to create clear deterrents to actions such as these.

---

[11] Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" CSO Online, InfoWorld, 22 Aug. 2017, www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
[12]Sanger, David. "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." The New York Times, The New York Times, 19 Jan. 2018, www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Questions To Consider

1. Considering how the 4 Geneva Conventions currently protects civilians and how the potential of cyberwarfare could impact civilians in new ways, what new impacts on the civilians should be prohibited?
2. What rules should govern cyber-warfare? How will they be enforced? What are the consequences of violating the regulations.
3. Who has jurisdiction over cyber-space regarding warfare?
4. How does virtual geography impact the definition of attacker and attacked? Are states accountable for non-state actors that make attacks from that state's actual territory?
5. How can governments work together to prevent violations citizens' rights due to cyber-warfare? What can be done collectively to prevent violations of this agreement?

Bloc Positions

- Nations Affected by Cyber-Warfare:
    - 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 Who Commit Cyber-Warfare:

- 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.

References

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

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

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/.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." BBC News, BBC, 27 Apr. 2017, www.bbc.com/news/39655415.

Glendinning, Lee. "Obama, McCain Computers 'Hacked' during Election Campaign." The Guardian, Guardian News and Media, 7 Nov. 2008, www.theguardian.com/global/2008/nov/07/obama-white-house-usa.

Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" CSO Online, InfoWorld, 22 Aug. 2017, www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

Fruhlinger, Josh. "What Is WannaCry Ransomware, How Does It Infect, and Who Was

Responsible?" CSO Online, InfoWorld, 27 Sept. 2017, www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

Sanger, David. "U.S. Had Cyberattack Plan If Iran Nuclear Dispute Led to Conflict." The New York Times, The New York Times, 19 Jan. 2018, www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Staff, LII. "Geneva Conventions." LII / Legal Information Institute, 19 June 2017, www.law.cornell.edu/wex/geneva_conventions.