Dear Delegates,

Welcome to the fourth Metro Detroit Model United Nations Conference. Over the past four years we have worked tirelessly to develop an exciting and innovative Model United Nations format that challenges our delegates in a competitive and inclusive environment. We work year-round to ensure that our staff members are as prepared as possible to ensure that all of our delegates can participate in our debates. Moreover, the topics that you will discuss have been carefully selected for their global importance and the larger questions that they ask. When reading through the following background guide, be sure analyze and evaluate what larger questions are being provoked by the topic and what commentary these larger questions make about the current international system. Finally, if you have any questions, be sure to reach out to your chairs on the email address provided on their committee page.

We look forward to welcoming you in January,

Mitchell Dennis
Secretary General of the Metro Detroit Model United Nations IV

Protecting Sovereign States from International Cyber Security Attacks

Why are Cyber-Attacks an important issue?

Cyber security is becoming a more prevalent issue, as more countries are sharing secure information and communicating through technology. Cybercrime racks up trillions of dollars in fees annually, and is becoming a more pressing issue for governments. Most modern power plants have a standardized network, meaning if a hacker figures out how to infiltrate it, their ability to attack others increases significantly. For each and every nation, it is absolutely imperative to protect all information, classified documents, safety of citizens, and the plants within their borders.

Cyber Attacks as an Act of War?

While cybercrimes committed by individuals or groups of individuals without political allegiance are becoming more common, so are attacks orchestrated or funded by sovereign states against other sovereign states. However, under current international law, cyberattacks are a grey area that are not well defined. In most cases of cyberattacks there is no physical damage, similar to what an armed battle would cause, yet cyberattacks come with heavy economic, social and political costs.[1] It is important that delegates work to reach a consensus on whether cyberattacks constitute an act of war and if they do, how to resolve that position with current international structures. Currently, the United Nations only recognizes wars that are approved by the Security Council or have a legal basis in self-defense. If cyber-attacks between nations are determined to be acts of war by the committee, then many other questions will have to be answered, not only by the committee but also by member states.

History of International Cyber Attacks

Previously, there have been cyber security attacks that have taken place around the world, effecting many countries and their infrastructures. The issue was first brought up for discussion in the United Nations by the Russian Federation in 1998, with Resolution 53/70.[2] Ever since that resolution opened discussion on "developments in the field of information and telecommunications in the context of

[1] "When is a cyberattack an act of war?" *The Washington Post.* https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html?utm_term=.bb969bafb03e.
[2] "Developments in the field of information and telecommunications in the context of international security." *United Nations General Assembly.* http://www.un.org/documents/ga/docs/55/a55554.pdf.

international security", it has constantly been in the discussion not only in the United Nations, but throughout the international community. The issue first began in the late 1980's when Robert Morris generated the first computer worm.[3] This worm is a virus that perpetuates itself within a computer and to other computer as well, similar to a biological virus. When it was originally created, the internet had much less user, and very limited capabilities and information, meaning that this worm causes a lot more harm now than it did when it was created. Then, in the 1990's, viruses became wide spread, the first major virus being the ILOVEYOU virus that infected millions of personalized computers, and caused many email servers to stop working.[4] At the time, it was the largest virus ever to hit computers, ultimately infecting over 45 million computers. However, the virus was not contained to a single country, it is thought to have begun in the Philippines before spreading to Europe and the United States.[5] In this sense, cyberattacks have always had an international nature, even before they were used to attack sovereign states. This virus and the threat of future viruses resulted in the creation of antivirus software.

In the 2000's, cyberattacks began turning more destructive and chaotic by targeting people's credit cards. The ring of attacks that took place in the mid 2000's led to 45.7 million people having their credit cards hacked, and cost the company that was hacked over $256 million. The hackers had snuck in by the heating and cooling system of Target, and eventually the virus made its way to Target's Point of Sales system, and the virus would grab the card number while it was in the system allowing the hackers to get ahold of nearly 40 million debit and credit cards.[6] Moreover, in this day and age we are noticing a rise in cyberattacks taking place by not only civilians, but member states, with critical energy systems hacked in Europe and the United States, as well as political campaigns.[7] Just this past year, Emmanuel Macron's campaign was allegedly hacked by a group linked to the Russian government.[8] In this we can seek the evolution of cyberattacks. From low level viruses attacking and crippling the personal computers of individuals, to hacks on companies to steal personal information, to more sophisticated attacks on sovereign states and critical infrastructure of these states.

Past Efforts by the United Nations

The United Nations

To this date, the ECOSOC committee of the United Nations had decided to hold a summit, where other committees from the United Nations, Member States, and civil organizations could gather to discuss the problems a lack of cybersecurity create, and create a global response to combat

---

[3] "A Brief History of the Worm." *Symantec.* https://www.symantec.com/connect/articles/brief-history-worm.
[4] "Love Bug : The Virus that Hit 50 Million People Turns 15." Vice News. https://motherboard.vice.com/en_us/article/d73jnk/love-bug-the-virus-that-hit-50-million-people-turns-15.
[5] Ibid.
[6] "Case Study: Critical Controls that Could Have Prevented Target Breach." *SANS Institute.* https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.
[7] "'New wave' of cyberattacks target US, European energy sectors." *ABC News.* http://abcnews.go.com/US/wave-cyber-attacks-target-us-european-energy-sectors/story?id=49666446.
[8] "Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group." *Fortune Magazine.* http://fortune.com/2017/04/24/macron-campaign-france-hackers/.

cybercrime. This had created a thorough discussion from a wide range of policies. The United Nations had also released a thought-out report, the Global Cybersecurity Index, which created a foundation for countries to help them address the issue of cyber-attacks.[9] This report looked over ways that countries could work together to build a stronger cybersecurity for all nations. This report agreed that norms and principles had to be put in place for the responsibility of Member States. It also agreed in this report that member nations had to come together to report their views on international law, to help ensure that cooperation to build stronger cyber security remain intact. Additionally, this report found that nearly half of all countries lack a national plan on cybersecurity.[10] Because the United Nations cannot mandate or force nations to adopt certain cybersecurity measures, it is crucial that countries develop autochthonous plans in order to better defend themselves.

Resolution 55/63 is a resolution that the General Assembly has passed in order to combat the criminal misuse of information and technologies.[11] This resolution calls for member states to ensure that they do not create safe havens within their nation for criminals who misuse informational technologies. It also notes that law enforcements over all concerned states should work in a cooperative and timely matter, and that law enforcement personal should be trained and equip to handle these misuses if they should arise. Lastly, this resolution also calls on member nations to take into account both the protection of individual freedoms and the right to privacy when further discussing policy on this issue.

Finally, Resolution 57/239 is a resolution passed by the General Assembly in 2003 that calls upon cooperation through Member-States and other international organizations to create a cyber security culture.[12] This resolution also calls upon able and willing nations to help developing countries receive the proper equipment and intelligence to have a secure cybersecurity system. The 2003 resolution was then built upon by the Resolution 64/211, which sought to create a global culture of cybersecurity.[13] Importantly, this resolution contained an annex that called upon member states to create voluntary self-assessment tool to protect critical information infrastructures. Specifically, it calls for collaboration between the public-private sectors in order for better incident management.[14]

Past Efforts by the International Community

The European Union

As released in 2013, the European Parliament and Council have produced a strategy for EU members when it comes to cyber security. The strategy outlines some of the EU's core values such as access for all people, the protection of fundamental rights (freedom of expression, personal data and privacy),

---

[9] "Half of all countries aware but lacking national plan on cybersecurity UN agency reports." *UN News Centre.* http://www.un.org/apps/news/story.asp?NewsID=57119#.We6mzohrzIU.

[10] Ibid.

[11] "Resolution adopted by the General Assembly." *United Nations General Assembly.* https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

[12] "57/239. Creation of a global culture of cybersecurity." *United Nations General Assembly.* https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[13] "64/211. Creation of global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures." *United Nations General Assembly.* *http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211*.

[14] Ibid.

and that the responsibility of security does not fall on one country, but on every nation united. The strategy have five main points: achieving cyber resilience, drastically reducing cybercrime, developing a cyber defense policy, develop industrial and technological resources for cyber security, and establish a coherent international cyberspace policy that reflects core values of the EU.[15] In order to meet the goals the EU has set, they have set up communications between EU institutions and the private sector, to ensure that if any attacks do occur everyone is working together to stop it from causing massive destruction and harm. The European Union would also like to see that the market for technology is a single market; meaning that they would like to incentivize those in the private sector to make goods that hold a high level of cybersecurity. The EU also stated that it would like to work closely with many other international organizations to ensure that the policy created for cybersecurity works hand and hand with the policy of other international organizations. While the plan of the European Union offers some potential solutions to delegates, they should keep in mind that their proposal and strategy was developed with its member states and their capabilities in mind. Therefore, it might not be replicable in other contexts.

Association of Southeast Asian Nations (ASEAN)

The ASEAN Cyber Capacity Program is aimed to fund training, and other resources to nations, in order to help create a strong infrastructure that is effective when it comes to countering cyber terror attacks. This will help with workshops, seminars, and consulting when it comes to formatting cybersecurity legislation and strategies. Many countries within ASEAN have cybersecurity initiatives that are highly ineffective because there is a lack of compliance mechanisms. The 2000 e-ASEAN Framework had a goal to increase electronic commerce, and highly focused on constructing the ICT infrastructure that existed in developing nations, while strengthening the member nations that are currently developed.[16] However, this framework was unsuccessful due to the inadequate discussion of security policy and breakdowns in cooperation among members.

Another cybersecurity initiative that was created by ASEAN nations was the idea of Computer Emergency Response Teams. The goal was that by 2005 (the initiative was proposed in 2003) all member states would have a system put into place where if there was a cyberattack on that nation or on a nearby nation, a crisis team and IT members would be on staff in order to prevent the attack from becoming large scale catastrophic. Not all member nations had these systems in place by 2005, but toady all member nations do have a CERT within their country. How reliant these CERTs are is dependent on the national resources and capabilities of the country. This program has flourished into regular cybersecurity exercises held between the ASEAN members and its regional partners, South Korea, China, Japan, India and Australia.[17] This year's exercise was held by Vietnam and focused on boosting cybersecurity forensics and investigating cyberattacks more effectively.[18]

---

[15] "Communication on a Cybersecurity Strategy of the European Union- An Open, Safe and Secure Cyberspace." *European Commission.* https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace.

[16] "e-ASEAN Framework Agreement." *ASEAN.* http://asean.org/?static_post=e-asean-framework-agreement.

[17] "New ASEAN Cyber Drill Kicks Off in Vietnam." *The Diplomat.* https://thediplomat.com/2017/09/new-asean-cyber-drill-kicks-off-in-vietnam/.

[18] Ibid.

Case Studies

2007 Hacking of Estonia

In 2007, the Republic of Estonia had experienced the first ever national scale cyberattack. The

hacker that had infiltrated almost every digital front of Estonia. Media outlets, commercial banks, telcos (a very large communications company) as well as government websites were all shut down by the attackers.[19] What had ignited the attack was what had taken place a few days earlier in Tallinn, the capital of Estonia. It had been decided by officials to remove the statue that was built in 1947 to honor the removal of the Nazis by Soviet Russia.[20] To many people who still live in independent Estonia, this statue is not a sign of victory, but a sign of oppression. The removal of this statue is what had sparked the hackers to carry out the attack. The attack led to media outlets' websites to be almost inaccessible. A webpage can only have so many people on it at one time, and no matter what the media outlets did to try and reopen the capacity (turn off commenting, removing ads and pictures, etc.), the hacker was constantly adding more spam as to ensure no one could read the news, this helped sow chaos throughout the country. Moreover, copy-cat hackers, who had copied the program line of the original hacker, and repeated it hundreds of time a second, also began to initiate attacks. There were also hackers that had the ability to hack into websites, delete legitimate content and create their own. As a way of defense, Estonia had to cut off international access to their websites, to narrow the search for the hacker, and prevent other hackers internationally from infiltrating.

Estonia eventually called in specialists to help develop a way for the attacks to never occur again. The specialists had the task to identify the attack and create worldwide filters to prevent anymore spam from overwhelming the server. The Estonian government still believed that the hacking was carried out by Russian hackers due to the Russian-language bulletin boards, and that one of the hackers had coded into an Estonia site saying "Hacked from the Russian Hackers." The Russian Federation strongly denies orchestrating the attack, although it bares similarities to more recent attacks throughout Western Europe, alleged to have been committed by Russia.[21] While the hack of Estonia is alarming in its own right, its potential greater implications are perhaps more so alarming. As a member of North Atlantic Treaty Organization, an act of war by Estonia requires other members to come to its defense.[22] If Russia had orchestrated the attack and cyberattacks were considered an act

---

[19] "A look at Estonia's cyber attack in 2007." *NBC News.* http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WfPYX4hrzIU.

[20] Hackers Take down the Most Wired Country in Europe." *Wired.* *https://www.wired.com/2007/08/ff-estonia/*.

[21] "A look at Estonia's cyber attack in 2007." *NBC News.* http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WfPYX4hrzIU.

[22] "How a cyber attack transformed Estonia." *BBC NEWs.* http://www.bbc.com/news/39655415.

of war, a conflict between 4 nuclear powers (United States, France and the United Kingdom, and Russia) could have been ignited. In this sense, delegates should reflect carefully whether they want to define cyberattacks as an act of war.

Hacking of the Iranian Nuclear Program

The Iranian Nuclear Program also experienced a cyberattack that concerned nuclear centrifuges. Stuxnet is a project that was worked on collaboratively between the United States and Israel. This program had reportedly destroyed a fifth of Iran's centrifuges by causing them to spin out of control.[23] Lesser known, is how the program developed an electrical blueprint, to tell those who run the program, how the computers that run the centrifuges operate to enrich the uranium. It was discovered that an electronic worm had entered into the server by a worker's thumbnail. The worm had worked its way in, and showed the control room that everything was running smoothly, while all of the centrifuges had been running rampant. The intentions was not to destroy the centrifuges, but to weaken the centrifuge's life span.[24] The code was tested in an Israel nuclear facility, and proved that it was the beginning of something big. The first wave of the virus went undetected for years, constantly highlighting a new way for future hackers to infiltrate the base because of the electronic blueprint that was created. The second wave of the virus caused the centrifuges to attack themselves, and the computers to self-replicate. The creators and culprits of the attack are alleged to be the United States and Israel, but neither nation has confirmed they were responsible.

Hacking of South Korea

Also, South Korea has also been hacked. The South Koreans had found malware within some military documents, some that were confidential. North Korea had breached the South Korean's military command. North Korea is known as an isolated country, but has invested heavily in cyber intelligence, which gives this country the capability to carry out cyberattacks at this scale. It has been found that since 2010, North Koreans have been working on programs that are designed to attack national infrastructures, and are believed to have planted malicious codes that could create massive damage to a country's infrastructure.[25] It is now alleged that the North Koreans were behind the 'WannaCry' attack against the British health system in 2017.[26] This attack eventually spread worldwide, affecting critical infrastructures.

Questions to Consider

- How can Member States learn from cyber-attacks of other nations?
- How should cyberattacks between sovereign states be defined by international law?
- How can we prevent terrorists from committing cyber-attacks against sovereign nations?
- How can those who carry out cyber-attacks be held accountable?

---

[23] "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[24] Ibid.

[25] "How North Korean Hackers stole 235 gigabytes of classified US and South Korean military plans. *VOX.* https://www.vox.com/world/2017/10/13/16465882/north-korea-cyber-attack-capability-us-military.

[26] "North Korea were behind WannaCry NHS cyber-attack," *Evening Standard.* https://www.standard.co.uk/news/uk/north-korea-were-behind-wannacry-nhs-cyberattack-says-uk-security-minister-in-sensational-revelation-a3669346.html.