Dear Delegates,

It is a pleasure to welcome you to the 2016 Montessori Model United Nations Conference.

The following pages intend to guide you in the research of the topics that will be debated at MMUN 2016 in committee sessions. Please note this guide only provides the basis for your investigation. It is your responsibility to find as much information necessary on the topics and how they relate to the country you represent. Such information should help you write your Position Paper, where you need to cite the references in the text and finally list all references in the Modern Language Association (MLA} format.

The more information and understanding you acquire on the two topics, the more you will be able to influence the Resolution writing process through debates [formal and informal caucuses], and the MMUN experience as a whole. Please feel free to contact us if and when you face challenges in your research or formatting your Position Papers.

We encourage you to learn all you can about your topics first and then study your country with regard to the two selected topics. Please remember that both committee members need to be well versed and ready to debate both topics.

Enjoy researching and writing your Position Papers.

We look forward to seeing you at the Conference!

MMUN Secretariat Team

info@montessori-mun.org

Disarmament and International Security

General Assembly First Committee

The First Committee deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime.

It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of

international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva- based Conference on Disarmament. It is the only Main Committee of the General Assembly entitled to verbatim records coverage.

Source: http://www.un.org/en/ga/first/

Cybersecurity

Topic Background

The growth of the Internet has allowed nations, organizations, and people to connect in ways previously unimagined. This new interconnectivity has allowed for collaboration, partnerships, and growth to reach unprecedented levels and has permitted the world to become a much smaller place. However, along with the benefits of the Internet, there are many new dangers created by this technology. The very nature of the Internet allows for individuals to hack information systems to steal information, cripple the delivery of services, and commit fraud. These cybercrimes are difficult to fight against, so it takes an international effort to combat them.[1]

This issue has come to the forefront in recent months after it came to light that organized hackers based in China were responsible for a series of hacks against American government offices and businesses.[2] In 2015, the United States Office of Personnel Management was hacked which resulted in over 20 million government employees' sensitive information being leaked, including some confidential information about intelligence community officials.[3] While government officials and experts have told press that the evidence demonstrates that the Chinese government was responsible for this breach[4], the US government has not made an official statement on Chinese government involvement, and Chinese state media has denied any government involvement in the hacks[5], stating it was carried out by criminals within China[6]. In recent years, numerous hacks against businesses around the world have also been identified, perpetrated by groups ranging from underground hacking collectives like Anonymous, to cyber-wings of military organizations such as the Syrian Electronic Army[7] or ISIL. The objective of these hacks has been to steal or government secrets, cripple infrastructure, or co-opt communications systems, which angers corporations and governments wishing to protect their interests, their information, and their security[8].

Sometimes cyberattacks can have more tangible effects. In 2009, the US and Israel allegedly launched the Stuxnet virus against Iranian nuclear enrichment facilities and destroyed roughly a

---

1 "Cyber Warfare". UN News Center. http://www.un.org/press/en/2014/gadis3512.doc.htm

2 Marc Goodman, Future Crimes (Doubleday 2015), 32

3 "US Considering Retaliation to Chinese Hacks" The New York Times. http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html

4 "U.S. decides against publicly blaming China for data hack" Washington Post. http://wapo.st/1RP2gYb

5 "China's Xinhua says U.S. OPM hack was not state-sponsored". Reuters. http://reut.rs/1P9X4Ka

6 "Chinese government has arrested hackers over OPM breach" Washington Post http://wapo.st/1PwmNiO

7 "10 Reasons To Worry About The Syrian Electronic Army". Business Insider. http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1

8 P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everybody Needs to Know. Oxford University Press

fifth of all Iranian centrifuges by making them spin out of control.[9] In 2007, Estonia was targeted by Russian sympathizers for wanting to remove a Soviet statue from the capital, Tallinn. Several prominent government websites were hacked, and essential government services were disrupted. In December 2013. the credit and debit card information was stolen from over 40 million shoppers at Target stores over the holiday season. After it was announced, people avoided shopping at Target and the company lost 46% of its profits and had to pay over $10 million in damages to affected shoppers.[10]

Some analysts warn this is only the beginning. As the internet and internet-linked technology become more widespread, the potential danger of cybercrimes increases. If nothing is done to combat this scourge, almost nothing can be considered safe. Smartphones could provide hackers with a wealth of financial and other private information from its users. Stock markets could be manipulated to wipe out entire economies overnight. Power plants and water treatment facilities could be switched off, leaving people without basic necessities.[11] Clearly this is an issue which needs to be addressed and the only way to address it is through international dialogue and cooperation.

Past Actions

The UN General Assembly, Economic and Social Council, and Security Council often stress the importance of cybersecurity and regularly call on member nations to combat cybercrimes. These organs usually refer responsibilities to the International Telecommunications Union (ITU) which is a UN agency based in Geneva which is responsible for coordinating efforts on these issues. They study cyber activity and set standards to which various governments are supposed to adhere to.[12] The difficulty with such organizations is these standards are often non-binding and there are not enough mechanisms to force countries to play by the rules.

A major difficulty in combating cybercrimes is the sheer amount of data that needs to be monitored in order to catch cybercriminals. Several NGOs have stepped up efforts to monitor cyber activities and on reporting on cybersecurity issues. The International Association of Cybercrime Prevention, "provides information and training about cybercrime prevention. It is also an interdisciplinary research organization bringing together experts, professionals, and

[9] "Stuxnet was Far More Dangerous." Business Insider. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
[10] "9 Recent Cyberattacks Against Big Businesses." The New York Times. http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html
[11] Marc Goodman, Future Crimes (Doubleday 2015), 50.
[12] "About ITU." International Telecommunications Union. http://www.itu.int/en/about/Pages/default.aspx

individuals involved with the misuse of Information Communications Technology."[13] The Cyber Peace Foundation is another NGO which is also involved with raising "awareness, counseling, education, training and to reach out to the citizens, the governments, law enforcement agencies (LEAs), private enterprises, NGOs working in cyber crimes and cyber security, universities, cyber security experts and bug bounty hunters; to provide a common platform on a global level."[14]

There is also hope that bilateral agreements can help solve these issues. In September 2015, Chinese President Xi Jinping and American President Barack Obama met and discussed issues related to cybersecurity and came to a tentative agreement.[15] Prior to President Xi's visit to Washington, Obama administration officials had warned that disagreements over cyberwarfare may lead to sanctions by the US government, and that products might not be able to be sold on international markets. In their meetings, they discussed steps each government should take to curb cyber-spying on boths sides and they agreed to disallow any hackers from committing acts of cyber espionage.

Possible Solutions

It is important for delegates to keep the following in mind when brainstorming solutions to cybersecurity threats:

1. What measures can be taken to improve the monitoring of cyberspace?
2. How can international actors be held accountable when they are found to have taken part in cybercrimes?
3. What steps can be taken to ensure a free, but safe Internet?

One of the major problems with guaranteeing cybersecurity is the sheer amount of data that makes up cyberspace and, coincidentally, the difficulty in monitoring it all. The United States has been better able to monitor cyberspace than many other nations, but this has created some difficulties within the international system. Some nations have viewed America as the greatest protector of cyberspace while others view it as its greatest threat. Increasingly, individuals have become more worried about privacy issues and leaks of government information from Edward Snowden which demonstrated US spying practices on foreign leaders have only increased this worry[16]. Also, since most of the servers which contain the Internet reside within the United States, there is concern that the US has an unfair monopoly in cyberspace ownership.

[13] "About Us." International Association of Cybercrime Prevention." http://www.cybercrime-en.org/about-us-cyber-crimes
[14] "About Us." Cyber Peace Corps. http://www.cyberpeacefoundation.org/aboutus.html
[15] "Xi Jinping, Obama Talk Cybersecurity". Al Jazeera. http://america.aljazeera.com/watch/shows/live-news/2015/9/xi-jinping-obama-talk-cybersecurity.html
[16] "NSA boss: We lost trust with allies after Snowden leaks". The Australian. http://bit.ly/1QMqboq

Increasingly, it has been argued that the Internet needs to be governed by an international agency which is responsible to answering to the international system as a whole and not individual parties. The Non-Aligned Movement has expressly stated the need for independent control of some parts of their internet to guarantee the protection of defense secrets as well as the ability to guarantee internet use for the growth of their economy.[17] However, the makeup of such a body is still being debated.

Another major problem with guaranteeing cybersecurity is the issue concerning how to hold nations and international actors accountable for their actions. Nations like Russia[18] and China[19] believe cyberspace should be controlled locally by various national governments and should respect cultural norms and national policy agenda if a state determines the need for this. In much of the West, people believe in a free Internet, but in less democratic countries leaders may feel threatened by a free internet and wish to control it directly.

Coincidentally, this has sparked debate around the world about how much freedom individuals are willing to give up in order to maintain security online. Originally, the Internet was a completely free place where individuals could express themselves and feel free to come up with applications never thought of before. As the technology has become more widespread and available, dangers have arisen. There is a large debate concerning how much freedom should be allowed in cyberspace. If governments took more control over cyberspace, they could most assuredy be more effective in improving cybersecurity, but there is a risk they would also decrease the level of freedom permissible on the Internet. This debate is especially pertinent in the European Union where individuals are asking where to draw the line between security and freedom of expression.

There are many challenges to creating an international framework for cybersecurity. Though the challenges are great, the potential danger of not doing anything is far greater. The problems posed by cybercrime are serious, but they are solvable. It is hoped the international community can put aside their differences and create a free and open Internet which is safe from cybercrime.

Further Research

- The UN and Cybersecurity
- Information on International Telecommunications Union

[17] "Cyber Warfare". UN News Center. http://www.un.org/press/en/2014/gadis3512.doc.htm
[18] "Cyber Norm Emergence at the United Nations" UN Economic and Social Council Press. http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf
[19] "Statement by China on Cybersecurity at the the 68th UNGA" UN Office of Disarmament Affairs. http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf

- Information on Cyber Peace Foundation
- The Cyber Security Forum Initiative

Questions

1. What was the name of the virus the United States and Israel launched against Iranian nuclear facilities?
2. What store was targeted in December 2013 to obtain users' credit/debit card information?
3. What was the name of the US government office that was targeted by hackers in 2015 to steal federal employees' information?
4. Who met in September 2015 to work out disagreements concerning cybersecurity?
5. Which country hosts the most internet servers globally?

Answers

1. Stuxnet
2. Target
3. The Office of Personnel Management
4. Chinese President Xi Jinping and American President Barack Obama
5. United States of America