Fair Lawn Model United

Nations Conference V

2016

United Nations Security Council

Chairs:

Bhavesh Koppala

bhaveshkoppala@gmail.com

Stuart Alcala

tigerfang115@yahoo.com

Letter from Your Chairs

Greetings Delegates!

Welcome to Fair Lawn's Model United Nations Conference V, and welcome to UNSC. My name is Bhavesh Koppala, and I am currently a junior at Fair Lawn High School. I joined Model UN a bit late as a sophomore, and after attending weekly club meetings and conferences, I regret not joining as a freshman. I attended AMUN XVII, where I represented Germany in DISEC. The experience was a bit nerve-wracking at first, but I knew I was interested in the in the club. Besides Model UN, I am interested in science and math, and was a member of the school's soccer program. It will be interesting to see the ideas that you bring to the table and how heated the debate will become. I am eager to be your chair and hope that our committee is successful!

Welcome Delegates, to Fair Lawn High School's fifth Model UN conference. My name is Stuart Alcala and I'm currently a senior at Fair Lawn High School. My past involvement with MUN has been as a volunteer, typing up working papers, resolutions and taking pictures. I am very familiar with the dynamics of a committee session and encourage you all to immediately jump into debates with confidence. Although we have prepared the Delegate Guide to help you in your initial research, you should still utilize other resources. Please do not hesitate to contact me for specific questions about the committee topics!

See you on the floor!

Cordially,
Stuart Alcala and Bhavesh Koppala

Topic 1: Cyber Warfare and International Security

Introduction of Technology:

Computers were initially created to compute mathematical equations and to create graphs for artillery during war. The computer eventually coincided with the Internet as people then had access to valuable information they could utilize in their daily lives. While the Internet was once seen as one of the greatest assets to people, it has also ushered in a new era of cyber warfare. Governments are able to use their IT to disrupt communications, hack into the infrastructure of other governments, or even steal government secrets. Cyber warfare jeopardizes the security of every country in the world as anyone is prone to having his or her information viewed and publicized.

These attacks are capable of disclosing private information on official government websites, freeze a person's assets, stealing valuable information, or even destabilizing economies. Cyber warfare has become a threat to innocent civilians and the welfare of every country. Some countries have unfortunately seen the devastating effects of cyber warfare.

The Increased Danger of Cyber Warfare:

The first time technology was considered to be a threat was the creation of the Morris Worm in 1988. A graduate of Cornell University created the Worm: Robert Tappan Morris. The worm was initially designed to test how big the Internet actually was.

However, due to a flaw in the program's code, the worm started to infect computers. The Morris Worm caused over 10% of the Internet to slow down. Even though the worm only caused computers to slow down, some countries saw the dangers in technology and how vulnerable people are.

Previous Incidents:

Despite the creation of the CERT, there have been incidents where countries and their welfare have still been infiltrated. In 2007, Estonia and its citizens suffered greatly from cyber-attacks launched by Russia. The statue that commemorated the Red Army was relocated, which offended the

Russian government, due to their reverence towards the statue, and Russia then began to launch cyber-attacks on Estonia. Estonia's government, banks, welfare, and infrastructure all slowed down, and some even shut down. A year later, Russia launched another cyber-attack on the country of Georgia. Georgian citizens were unable to access the media and the Internet for a short period of time, and Russian hacktivists were able to infiltrate other countries to damage their economies and way of living. In both of these incidents, Russian hacktivists were to blame for the cyber-attacks and not the government itself.

Hacktivists are more than capable of attacking a country's economy. For instance, in 2007, Israel was able to launch a cyber-attack on Syria. Israel's attack prevented the Syrian Air Force from gaining knowledge of an impending air strike on behalf of Israel. Syrian Air Force systems were consequently shut down and this allowed Israel to launch an air-strike on Syria without suffering any casualties or losing any men in the process.

In January of 2011, the Canadian government was attacked by hacktivists located in China. The hackers gained access to classified files and also caused the Finance Department to completely shut down its activity and go off the internet. However, unlike the incidents involving Estonia and Georgia, the hackers who were responsible could not be determined to be Chinese; the hackers were so experienced that they were able to cover their tracks.

Organizations to prevent Cyber Warfare:

Eventually, the Computer Emergency Response Team (CERT) was created at Carnegie Mellon University. The program was created in wake of many countries realizing that computer programs such as the Morris Worm can be created to do more than slow down a computer. The CERT was assigned to gather and record information about a computer's security and create precautions in case a computer's security becomes jeopardized. The CERT encountered a situation similar to the Morris Worm. Cyber Warfare started to become common amongst teenagers as well and not just adults.

Countries Involved in Cyber Attacks:

Countries that are much more advanced in the field of technology are more prone to becoming victims of a cyber attacks. Such countries include: United States, Japan, United Kingdom, France, Belgium, Spain, and South Korea. Countries such as China and the United States are to blame for over 50% of the world's cyber-attacks. However, although developing countries in Africa and Asia have a lower chance of being hacked, that does not mean that they are completely immune.

Bloc Positions:

United States - The U.S. can be exposed to cyber-attacks at any time due to how much the country depends on the Internet. The Department of Defense acknowledges that the Internet is a threat to the U.S.'s security and has prepared to use the five pillars if the Department of Defense or the U.S.'s national security were ever to be exposed. In 2011, the U.S. had said that if the U.S. was to ever be attacked, that they would be allowed to use military force on the country that launched the attack.

Asian Bloc- China is responsible for over 41% of the world's attacks, and has been involved in several espionage cases. The countries of Australia, Canada, India, and the United States have all accused China of harming their countries' welfare. However, the Chinese government has denied any involvement in launching cyber-attacks.

European Nations- In 2013, the U.K. had acquired hundreds of computer experts in order to defend its country against any cyber-attack. They stopped over 400,000 cyber threats that could have developed into a cyber war.

In 2014, France decided to boost its defenses to prepare for any threats that are made against the country. France is a part of the National Cyber Security Organization. The CCDCOE (National Cyber Security Organisation) helps France decide what do if there is a cyber-attack, as well as manage their defenses.

The Russian Federation has had a history of infiltrating other countries via cyber-attacks. The Russian government was not involved in the incidents that occurred in Estonia or Georgia, but a group of hacktivists from the country were. In 2014, a group of Russian hacktivists was able to take advantage of a bug that they found in Microsoft, which allowed them to spy on NATO and the European Union.

Questions to Consider:

1. Is your nation affected by cyber warfare? Has your nation ever been attacked by another country?
2. What has your nation done to limit the number of cyber-attacks? What plans or precautions has it taken?
3. Is your nation allied with other nations? Is it apart organizations to combat cyber warfare?
4. What does your nation hope to achieve in regards to cyber warfare? Would it want to work with other nations to prevent cyber-attacks from occurring?

References:

1. https://www.us-cert.gov/
2. http://www.reuters.com/article/us-britain-cyber-warfare-idUSBRE98S0GO20130929
3. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
4. http://www.economist.com/node/12673385
5. https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/
6. http://www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660/

TOPIC 2: Biological & Chemical Weapons

Introduction:

The rapidly increasing number of chemical and biological weapons being made and used since the Cold War has escalated to a point where it has become one of the most important issues on the United Nations security agenda. In August 2012, news that the Syrian regime had used chemical weapons was confirmed. The Chemical Weapons Convention has outlawed this means of warfare since 1993 because they were especially deadly due to their lasting effects on civilians. Biological weapons have similar effects to that of chemical ones, however instead of using chemicals, organisms and pathogens are the fundamental agents. Hence, biological weapons were also outlawed in 1972 because of the immense threat it puts upon civilians.

UN Definitions:

Biological Weapons - "Microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict."
Chemical Weapons - "Any chemical which through its chemical action on life processes can cause death, temporary incapacitation or permanent harm to humans or animals. This includes all such chemicals, regardless of their origin or of their method of production, and regardless of whether they are produced in facilities, in munitions or elsewhere."

History/Background:

After the huge growth in biological weapons being used throughout the world. Some countries made the dangers of these weapons clear and two declarations were made by The Hague in 1899 and by the Brussels in 1874 to internationally ban biological weapons. However, these declarations did not do much to enforce this agreement, and some ignored the treaties. The German army continued to develop these weapons and then used them during the First World War. Soon after, the majority of countries had started their own biological and chemical research for warfare. Japan proved the harmful effects of biological weaponry when killing thousands of Chinese people in 1947. However, after their defeat, the Geneva Conventions banned all biological warfare. The Chemical Weapon Convention around this time.

Current Situation:

In the following years after the Geneva Convention and the CWC came into force, more countries have come under the rule of the conventions, which have in turn helped reduce the amount of chemical weapons being created. Currently, the Chemical Weapon Convention obligates 188 countries to develop a system to stop the increase of these weapons.

Current Critical Areas:

Syria - In the modern world Syria is one of the worst countries for using biological warfare. It's believed that the world's largest stockpile of biological weapons have been in Syria since 2013. There are thousands of cases in which Syrian patients have been seen with symptoms of biological weaponry, though none have been proven.

United States - Although the United States displays a strong commitment to the CW and BW conventions, they lack verification towards the destruction of the biological weapons left from the Cold War. After the 2001 anthrax attacks following the 9/11 attacks, the U.S. has shown enormously increased interest in protecting against bioterrorism with Obama's National Strategy for Countering Biological Threats in 2009.

Bloc Positions:

China

China states that it denounces these weapons and has been in full compliance with the BWC obligations. The nation has also never had an active biological weapons program. Regardless, the U.S. suspects that BW activities continued after China joined the BWC.

Syria

According to a 2010 report, President Assad has hinted that Syria is in possession of biological weapons. Several countries have begun monitoring the situation in Syria as civil conflicts worsen and the risk of biological/chemical weapons increases.

United States

Although having declared to destroy all offensive BW agents between 1971 and 1973, a report by the Russian government in August 2010 accuses the United States of undertaking research on Smallpox, which is prohibited by the World Health Organization. As of August 2013, the United States has destroyed 25,000 metric tons of chemical agents and believes that the destruction will be completed by 2023.

Questions to Consider:

1. Is your country prepared for a biological or chemical attack?
2. Have other countries or groups launched biological or chemical attacks recently?
3. What countries are currently developing these forms of weapons, why?
4. What can your country do to prevent these form of attacks?
5. Will your country intervene in biological or chemical conflict amongst other countries?

(Picture on the next page)

References:

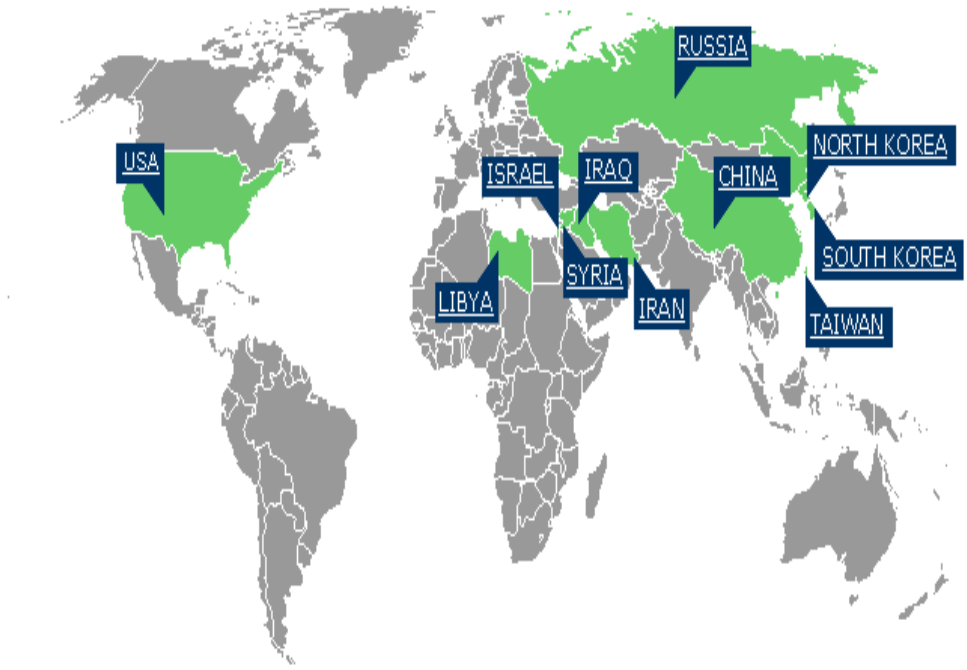
[News]
https://www.icrc.org/en/war-and-law/weapons/chemical-biological-weapons

[Country Signatures]
https://www.armscontrol.org/factsheets/cwcsig

[Chemical Weapons Convention]
https://www.opcw.org/chemical-weapons-convention/

[Definitions]
a. https://www.opcw.org/chemical-weapons-convention/articles/article-ii-definitions-and-criteria/
b. https://www.un.org/disarmament/geneva/bwc/

[Positions on chemical & biological warfare]
https://www.armscontrol.org/factsheets/cbwprolif


RUSSIA
USA
ISRAEL
IRAQ
CHINA
NORTH KOREA
SOUTH KOREA
SYRIA
LIBYA
IRAN
TAIWAN