



Honorable delegates,

Welcome to the Disarmament and International Security Committee (DISEC) at the 2018 edition of the Massachusetts Institute of Technology Model United Nations Conference!

We are pleased to have the opportunity to be the chairs for this committee throughout the conference. Justin is studying aerospace engineering and enjoys engineering systems design, and space exploration. Alex is studying material science engineering and is passionate about the development of new materials as they relate to aerospace applications. We are both minoring in political science and interested in international politics and diplomacy. We are excited to be chairing once again at MITMUNC!

Participating in Model UN has been one of the most rewarding and enriching experiences we have had throughout our college careers. The opportunity to engage with your peers and discuss real challenges that our world is facing is a great one. The issues that we will be debating are relevant and unsolved: we have the opportunity to brainstorm solutions to these problems together.

The specific topics for our committee this conference will be the ongoing situation in North Korea and their continued development of nuclear weapons, as well as the proliferation of cyber weapons around the world. Both of these topics are sensitive and challenging; both are relevant to international security and are subject to intense debate by scholars, analysts, politicians, and world leaders.

During the conference we sincerely look forward to hearing all of your thoughts, opinions, and ideas. This is an opportunity for you to engage in meaningful discussion on these topics, and we hope that each of you will speak your mind openly and freely. We hope that this committee can be both fun and thought-provoking, and we look forward to meeting all of you at MITMUNC 2018!

Thank you,

Justin and Alex
Chairs, Disarmament and International Security Committee

Topic A: Democratic People's Republic of Korea (DPRK)

A. Introduction and Background

The tensions between the Democratic People's Republic of Korea and the United States have been mounting in recent months. The DPRK's obtainment of nuclear weapons has been one of the predominant security crises of the 21st century, and has been a topic of discussion by world leaders for years. Multiple nations and international organizations have attempted to minimize the tensions and concerns regarding the DPRK to no avail.

North Korea developed as a country in 1945 after the end of WWII. Once the Japanese surrendered, the Korean Peninsula was divided along the 38th parallel between the United States and the then-Soviet Union. The result of the division was two separate occupation zones with two separate governments: the Communist-ruled Democratic People's Republic of Korea (colloquially termed North Korea) and the Western-aligned Republic of Korea (colloquially South Korea); both governments claimed to be the legitimate and only government for all of Korea. From 1950-1953, the Korean War was fought over both governments' claims to rule the entire peninsula. The war ended with the restoration of the status-quo (division along the 38th parallel) and the installation of a demilitarized zone in attempts to mediate the tensions.



Figure 1: Map of the Korean Peninsula

Kim Il-sung, the leader of the DPRK since its inception, remained in power until his death. Throughout his regime, he developed a personality cult and emphasized the principle of self-reliance to get the nation through severe economic crisis in 1991.

There has been tension between the communist countries in the East and the democratic countries in the West for decades. The new administration governing the United States and the leaders of the DPRK have exchanged insults and snide comments over the internet, ranging from taunts and name-calling to an instance in which DPRK representatives referred to the United States as the “biggest terrorist organization in the world”. The changes in governments worldwide has led to an augmentation of enmity that has arguably not been seen since the Korean War.

B. Facts and Figures

Currently, the DPRK is run by Kim Jong-un, has a population of roughly 25 million people, and a GDP of around \$583 USD per capita, according to the World Bank. The DPRK believes that armament is key to protect itself from major foreign powers and in order to gain negotiation leverage with global superpowers. It is believed that the DPRK has produced, deployed, and stockpiled two or three nuclear warheads and toxic material, including over 5,000 tons of toxic gases. And so, nuclear threats from the DPRK are not new; they have been present for decades.

The DPRK is known to be an unpredictable and dangerous when it comes to nuclear weapons and mass destruction. Tensions between the DPRK and other nations worldwide increased in 2011 when Kim Jong-un succeeded his father and immediately performed rocket launches and nuclear bombs tested. In the six years that he has led the DPRK, Kim-Jong un has tested 84 ballistic missiles, which is more than twice as much as his father and grandfather.

The DPRK has been sanctioned on numerous occasions for similar behavior by the UNSC. Recently, in April 2017, the DPRK conducted an intercontinental ballistic missile test; although the test failed and the missile disintegrated quickly post-launch, international fears and tensions with the DPRK were renewed. And then in July of 2017, the DPRK successfully conducted its first intercontinental ballistic missile test. As a response to all of the DPRK’s nuclear missile testing, the UN Security Council has passed resolutions condemning the nuclear weapons and ballistic missile development activities conducted by the DPRK as a “flagrant disregard” of prior UNSC resolutions (June 2017) and expanded sanctions to additional sectors of the DPRK’s

economy (August and September 2017) to block the sale of coal, iron, and other commodities that represent one-third of the DPRK's total exports.

The DPRK is not alone as a nuclear nation. More than 24 countries have nuclear power infrastructure, but only nine countries have nuclear weapons programs or nuclear weapons in their possession. These countries are: Russia, U.S., China, India, Israel, France, Pakistan, U.K., and DPRK. Additionally, many nations that signed the 1970 Non-proliferation Treaty, including the U.S., Russia, China, France, and the U.K., have not fulfilled the treaty's terms for disarmament measures.

C. Subjects of concern for DISEC

One of the primary areas of concern for DISEC is the control and limitations of nuclear weapons. The use and up-scale of nuclear weaponry in the DPRK has been confirmed and is creating global tensions and fear.

In the past, the United Nations and individual countries have tried to work with the DPRK by issuing threats, conducting military exercises, implementing diplomatic sanctions, pressuring Chinese interference, and using cyber-sabotage. The DPRK views their nuclear programming as essential to their defensive strategy. Increasing tensions and verbal assaults have occurred in recent months, creating further concern about the outbreak of conflict.

D. Conclusions and Questions

DISEC has a wide ranging role and has held talks on the DPRK. Some questions that DISEC delegates at MITMUNC may want to address are listed below.

- How should the international community respond to nuclear weaponry development by the DPRK?
- To what extent is it the responsibility of the United Nations to intervene in the geographic and military strategy disagreements between countries?
- What can/should be done by the United Nations to prevent the further escalation of tensions, fear, and weapons development worldwide?
- How should the United Nations respond to the surge in tensions between the DPRK and the rest of the world that has occurred since the DPRK's most recent nuclear tests?

- How should the international community respond to various human rights violations and other international violations by the DPRK?

The questions listed above are intended to facilitate discussion and debate and is not exhaustive. Feel free to prepare responses to these questions in particular, related topics, or unrelated topics.

It is the role of DISEC to discuss disarmament, global challenges, and threats to peace throughout the world. The North Korea crisis presents one of the greatest challenges that falls within the scope of DISEC that the world has ever seen, and it is of utmost importance that the committee address this crisis thoroughly and thoughtfully.

Topic B: Proliferation of Cyberweapons

E. Introduction and Background

With the rise of the information age and increasing capabilities of computers, the issue of hacking has also increased. Hacking and illegal intrusion into computer networks has existed since the first creation of computers and networks themselves.

A cyberweapon is defined as a defensive or offensive agent employed for some military, paramilitary, or intelligence objective.

The development of cyberweapons has fundamentally changed the balance and scope of international security. Cyberweapons have an array of intentions and uses. Many are employed to steal classified information, data, and intellectual property. Covert surveillance is often a major objective. In some cases, cyberweapons have been used to destroy software, data, and even hardware.

F. Facts and Figures

Cyberweapons are an increasingly important topic in the global security sector. There are many examples of nations employing cyberweapons against other nations for a variety of reasons.

Nations with the largest known cyberweapons programs include the United States, Russia, China, Israel, North Korea, United Kingdom, and Iran. These countries collectively spend billions of dollars developing cyberweapons each year.

One of the most widely discussed incidents of cyberweapon use has been the Stuxnet virus. Almost certainly developed by the United States and Israel, the Stuxnet program specifically equipment and machines on factory assembly lines. The malware was used in Iran against nuclear weapon development plants, and was responsible for shutting down thousands of centrifuges used to refine nuclear material.

Surveillance cyberweapons have been the subject of many global information leaks over the last several years. One notable leak in particular in 2013 disclosed massive global surveillance by American intelligence groups and several of its European allies. These surveillance programs collected data from a large majority of the internet, and is considered one of the largest illegal spying and espionage operation in the world.

Some international security experts consider there to an ongoing arms race for cyber warfare capabilities. As the world becomes more interconnected and reliant on technology, cyberweapons have become increasingly relevant in the global security realm. The ability to employ both defensive and offensive cyberweapons is seen as a critical national security requirement in many nations, particularly by global and regional powers.

Cyber attacks are often difficult to trace. In many cases, a country subject to cyber attacks has accused another country of perpetrating said attack, only for the accused country to deny its involvement. Blame is difficult to prove and rarely do nations admit to be the developers and users of cyber weapons.

G. Subjects of concern for DISEC

Hacking and internet security remains a global problem and point of contention on a number of different scales. DISEC will be primarily concerned with the development and proliferation of cyberweapons by state-sponsored organizations and by government agencies. In particular, large scale cyberweapons that target large organizations and other nations are of utmost concern.

Increased reliance on technology and the failure of cybersecurity to keep up with increased threats is a major problem

Cyberweapons have the potential to directly harm both individuals and societies. Systems such as electrical power grids are susceptible to cyber attacks and could cause widespread disruption

and distress. Global financial markets, though generally more well secured than other industries, could be attacked and cause financial chaos.

Cyberweapons also have the potential to indirectly decrease security by escalating tensions. Many nations that would be hesitant to directly and physically assault or confront another nation are more willing to instead use covert cyberwarfare tactics to infiltrate and disrupt. When these cyber intrusions are discovered or leaked, they lead to worsening relations and could escalate conflict into military action.

H. Questions and Conclusion

International security is increasingly intertwined with cybersecurity. Therefore, it is the responsibility of DISEC to address how cyberweapons are being developed and used around the world. Some questions that delegates in DISEC may want to consider regarding this topic include but are not limited to:

- What is the responsibility of international organizations, such as the United Nations, to regulate the development and proliferation of cyberweapons?
- Should the international community develop protocols regarding cyberwarfare, as it has for conventional warfare?
- How should international organizations respond to cyber attacks?
- How can the international community prevent the escalation of cyber warfare, especially escalation of cyber warfare into military conflict?
- Are cyber attacks that target civilians to be considered war crimes?

The questions listed above are intended to facilitate discussion and debate and is not exhaustive. Feel free to prepare responses to these questions in particular, related topics, or unrelated topics on the proliferation of cyberweapons.

Cyberweapons are currently directly tied to international security, and are expected to become increasingly relevant to both peacetime and wartime security activities by nations throughout the world. DISEC has the responsibility to address this relevant topic and work towards solutions that contribute to world peace and security.

I. References and further reading materials

- <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>
- <http://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner>
- <http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf>
- <https://en.wikipedia.org/wiki/Cyberwarfare>
- http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf
- http://dspace.uni.lodz.pl:8080/xmlui/bitstream/handle/11089/12511/11-161_174-Kozłowski.pdf?sequence=1&isAllowed=y

J. Notes

This document is intended as an overview and introduction to each topic. Delegates are encouraged to consult resources outside of this document for more specific and in-depth information.

This document was prepared in December of 2017. As both topics contained within relate to ongoing issues, the information inside is subject to change.

Authors and Contacts:

Justin Gong, Alexandra Zele