WMUN 2018 Summer Conference

Disarmament and International Security Committee

Head Chair: Felix Seungje Lee

Deputy Chair: Kahyun Park

Table of Contents

I. Greetings

Felix Seungje Lee Head Chair

To the esteemed delegates of the Disarmament and International Security committee,

Hello, I'm Felix Lee, a rising junior attending Korea International School. It is my utmost honor to serve you as the Head Chair for this committee.

From this year's WMUN conference, I want my delegates to learn how to understand and represent the perspective of a country that they don't necessarily have connections with. When people read news articles about global issues or talk to their friend and teachers about them. It is very difficult for them to perceive the issue with an objective stance. However, in a MUN conference, as delegates aren't always assigned with the delegation that they are comfortable with, many delegates face difficulties attempting to consider a global issue in the identity of a nation that they don't represent in real life.

Personally, the experience of putting myself in someone else's shoes has occurred constantly throughout the conferences I've attend. During DIMUN, although I am South Korean, I had to represent the delegate of DPRK in the disarmament council that was tackling the issue of countering nuclear provocations. I also had to represent the delegate of Japan in the General Assembly, tackling the issue of territorial disputes in East Asia. Although I initially didn't agree with DPRK and Japan's stance, throughout those conferences, I tried my best to consider the issue in the perspective of those countries. As a result, I gradually became a more empathetic individual that could understand and recognize those countries' situations. After every conference I learnt not only about a certain global issue, but how different countries have different perceptions on those issues. Through WMUN, my hope is that I can hand on these valuable experience and knowledge to my delegates.

Kahyun Park Deputy Chair

Welcome, delegates! This is Kahyun Park from Sejong Global High School and I will be your deputy chair of Disarmament and International Security committee for the two days that we will spend discussing "Measures to Counter Cyber-warfare". It delights me to think that I will be spending two days together intensively discussing with au courant future leaders! Even if this is your first time trying out a MUN, don't be scared and feel free to ask for help to either chair! In the era of the Fourth Industrial Revolution, warfare is taking place in the cyberspace. This committee, DISEC will pursue ways to put a stop to such warfare. Currently, actions that could be considered as against the international law if done off-line are freely happening online because of the lack of actual international legislations to effectively put a restraint on states. Each delegate will represent a state highly interconnected with the agenda and seek possible solutions through cooperation and participation. As the deputy

chair, I hope to see excellent ideas and creative suggestions from all of you. Thank you all for signing up! Go WMUN 2018!

II. Committee Introduction

Disarmament and International Security Committee, better known as DISEC, mainly deals with global problems, disarmament and threats that affect international security and pursues solutions to bring peace to the international community. According to the Charter of the United Nations, "The General Assembly may consider the general principles of co-operation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armament." DISEC's main purpose is "to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources". It promotes cooperative arrangements and measures to stable the international community through armament at non-disruptive levels. DISEC may discuss any matter of disarmament and international security that fits the scope of the Charter of the United Nations or is relevant to the function of other UN organs.

DISEC was established in 1993 and is the First committee of the General Assembly. It was first established to deal with the implication of atomic bombs used and developed by many military powers during World War II and was formally called as the Political and Security Committee(POLISEC) until the 1970s. It gained great importance during the Cold War as the main agent to regulate international security. It was the stage for a world forum to allow all states to make their voice heard and therefore, all 193 UN member states are eligible as representatives and are given equal votes. Unlike the Security Council, because all states are eligible as representatives, there are no member rotation or veto powers. The very first resolution by DISEC was created in 1946 and regarded the "Establishments of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy". One of the best known resolutions to be made in DISEC is the Treaty of the Non-Proliferation of Nuclear Weapons (NPT) which concerns the reduction and limitation of arms. The NPT well shows DISEC's influence on international security. So far, DISEC has made many achievements in World History, but despite all that, international disruption in peace still exists and the threats increase non-stop. DISEC will continue to work against such problems and promote world peace for all.

DISEC works closely with other UN organizations like the United Nations Disarmament Commission (UNODA) and the Conference on Disarmament and oversees the Office of Disarmament. DISEC also collaborates with various international and non-governmental organizations that work in similar fields and pursue the same goals, so when writing

resolutions, the delegates are recommended to make use of the other organizations to effectively achieve goals.

So far, the UN's attitude towards cyber-warfare has been rudimentary at best. The General Assembly first adopted it as an agenda in 1998. There have been annual resolutions on cyber-warfare mostly on "developments with respect to information technologies in the context of international security", "combating the criminal misuse of information technologies", "creation of a global culture of cybersecurity" and etc. There doesn't seem to have been a Geneva Convention or any other binding agreements on the topic of cyber-warfare, in the United Nations.

When participating in a DISEC committee, as a representative of an individual member state, each delegate must consider the state's capabilities and limitations, and best ways to mitigate conflict without mandating a specific state's action. DISEC should not infringe other nation's sovereign policies so please be aware of the fact when writing resolutions. Further, because DISEC is a first stop before the Security Council, delegates must not rush to concrete solutions. Be aware that the resolutions of DISEC are not legally binding and cannot be subject to any legal action. DISEC has no authority to impose sanctions or authorize armed intervention. Nonetheless, resolutions do serve the purpose of establishing the tone on solutions for global issues. Because of the nature of the committee to debate the most challenging contemporary security issues, the delegates must try to seek creative unprecedented resolutions, without going against the set rules for DISEC. The delegates should try to seek resolutions that promotes world peace, keeps the International Law, and resolves the global problem in a way that most delegates can support.

III. Agenda Explanation

Measures to Counter Cyber-warfare

A) Background Information

The development of information and communication technology has resulted in the creation of cyberwarfare, the use of technology to impair or disrupt the activities of states, private organizations or individuals (RAND).

As states and terrorist groups become involved in cyberwarfare to achieve their political and economic ends, cyberwarfare is evolving into a major issue for governments internationally. Incidents of cyberwarfare attacks targeting critical infrastructures and strategic industrial sectors such as governments, medical facilities, and private sector corporations, which could trigger a breakdown in systems that functions the society, are increasing rapidly (World Economic Forum). The Russian intelligence agency, for example, targeted the Democratic National Committee, an administrative entity of the United States' Democratic Party, and leaked emails to intervene in the US presidential elections (Blake). Besides, the worldwide WannaCry ransomware cyberattack, which blocks the access to data, had brought international turmoil by infecting institution in more than "70 countries, including the Russian Interior Ministry and the National Health Service (NHS) in the UK" (Al-Jazeera).

Aforementioned events show cyber-attacks are afflicting significant damage to different areas such as government offices, corporations, hospitals, and transportation systems. As visible here, a single cyber-attack involves complexities and can have larger influences on these different areas. Thus, effective methods to implement enhanced cyber security measures must be considered as a solution. As government sectors maintain delicate security and civilian information, effective measures to mitigate cyberwarfare through the political lens call for recognition and deeper understanding.

Furthermore, ranking third in the list of global risks regarding the likelihood, malicious cyber-attacks have increased exponentially, sparking international attention on the issue (WEF). In fact, the financial costs of cyber warfare are rising due to the fact that businesses spend about $1 trillion responding to global cyber-attacks (Axel Wirth). According to the World Economic Forum (WEF), a study of 254 companies conducted in 2017 reported that the cost of coping with cyber-attacks increased 27.4% annually. It is evident that cyber - attacks have resulted in negative economic impacts on various entities such as states, infrastructures, large-scale corporations, and small-sized companies. This issue remains disruptive and prevalent because preventative measures must be continuously altered and improved in order to impede increasingly sophisticated cyber-attacks (Axel Wirth). Thus, investments in effective cybersecurity measures must be considered as an alternative solution.

In particular, fake news is a branch of cyber warfare that is complicated to maintain. Fake news is caused by independent entities with personal motives that fabricate or distort facts and circulate this fictitious information through internet search engines, news agencies, advertisements, and social media. Considering the extremely pervasive nature of fake news, it is impossible to eradicate every one of its sources. However, understanding its roots and characteristics can allow for anybody, from teenagers to Social Networking Sites (SNS), to protect themselves from being affected by falsified information.

A recent social issue regarding cyber warfare was the impact of fake news on the 2016 United States Presidential Elections. The Russian government and Internet Research Agency (IRA), a Russian intelligence agency, were accused of spreading fake news and advertisements that painted President Trump in a favorable light and runner-up Hillary Clinton in an unfavorable light, swaying the voters. According to the Cable News Network (CNN), 126 million Americans saw Facebook content by the IRA, and 11.4 million saw Facebook ads purchased by the IRA from 2015 to 2017. Furthermore, Twitter also reported that 36,746 Russian accounts generated 1.4 million election-related tweets that were viewed by 288 million users. Evidently, social media played a crucial role in allowing organizations to impress their views on the general public during the 2016 Presidential Elections.

B) Glossary

Crimeware : It is a computer program dedicated to conduct illegal actions through malware and automate theft of information. It is used in order to access others' financial and retail accounts for the purpose of taking funds from that account. Cyber-thieves use a variety of techniques to steal passwords or lure users into a counterfeit websites.

Espionage : It is the practice of using spies, mostly by governments seeking political or military information. In terms of cyber-space, it would mean spying on state secrets through hacking. Nowadays, espionage agencies target illegal drug trade and terrorists, and the US has charged at least 56 defendants for attempting to spy for China since 2008.

Hacktivism : It is the practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as a means of achieving political or social goals.

C) Past Actions and Possible Solutions

<u>International Legislative Cooperation</u>

Currently, various national efforts have been made to mitigate cyberwarfare attacks. Major countries that were previously affected by cyberwarfare have established their own separate cybersecurity policies and plans to nationally address cyberwarfare. The United States under the Chamber of Commerce, for example, has composed its own cybersecurity policies, and the Turkish government has formed its national cybersecurity policy in 2009 with the

development of a coordinating organization on cybersecurity called the Scientific and Technological Research Council of Turkey (NATO). Despite these various national efforts to maintain cybersecurity, cyberwarfare continues to threaten the global community.

Although a number of international communities have begun to draw "the mainframe and discussed the initial steps that need to be taken against cyber threats," according to the NATO Cooperative Cyber Defense Centre of Excellence's (CCD-COE) report, Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, the prominent reason why cyberwarfare continues to evolve is because "global measures against cyber terrorism has not been addressed specifically yet" (NATO). The report argues that an international legal framework under the United Nations is more effective than national cyber capabilities because "International law adds certainty to punitive actions and amplifies the cost of cyberattacks by engendering a negative response from the international community, not just from the attacked state" (NATO). As the low circumstances of cyberattacks, caused by the legal ambiguity of international laws, often prompt nations to launch them, establishing a universal legislation, just like any other international laws, would be effective for deterrence.

Similarly, the Council on Foreign Relations (CFR) and the International Institutions and Global Governance (IIGG) program also support CCD-COE's perspective on developing normative frameworks in their report Cyber Threats and International Cooperation. Stating that the current cooperation with the international institutions is "not kept pace with the growing and evolving threat of cyberattacks," CFR concurred that a more efficient cooperation is necessary to authorize frameworks for legitimate activities in cyberspace and standards for state responsibility upon cyberattacks (CFR). Specifically, the report argues that "identifying appropriate response options for cyberattacks below the act-of-war threshold and determining what offensive operations are acceptable in cyberspace" would assist the US and its allies to jointly retaliate against attackers with punitive measures (CFR).

In contrast, Mike Schmitt, professor of international law at Exeter University and a former US air force lawyer implied that international cooperation on creating a clarified norm is impractical after monitoring the dispute between Cuba and US, throughout a UN Group of Governmental Experts (GGE) conference, on the right to self-defense a cyberattack (Bowcott). Schmitt assumed that the reason why Cuba, China, and Russia disagreed with the establishment of legal frameworks was because they either "want to avoid the perception that the west gets to dictate the game for cyberspace" or "they want to deprive the west of a legal justification for responding to the hostile cyber operation that they themselves launch (Schmitt). Either way, he concluded that clarifying laws is not some nation's national interest because legal ambiguity provides them the flexibility to operate illegal acts without the risk of punishment (Schmitt). Although establishing legal frameworks is a praiseworthy approach to mitigate cyberwarfare, if the suggested framework relates to controversial matters such as national security, it may be impractical.

Corroborating the perspective of Mike Schmitt, Stefan Soesanto, the author of the report Cybersecurity in the European Union and Beyond; Exploring Threats and Policy Responses, who acquired an MA from Yonsei University with a focus on international law and cybersecurity policies, also concerns the practicality of UNGGE cooperation. He stated that the UNGGE process failed to establish a norm because of "top-down diplomacy," a diplomacy in which the most powerful nations dominate the conversation, and recommended governments to focus on creating a customary international law (Soesanto). Currently, the issue of cybersecurity is addressed under UNGGE with less than 30 states participating, including the permanent Security Council member states that have an overwhelming influence on the decisions. Additionally, the UNGGE Cuban delegate Miguel Roodríguez confirms Soesanto's perspective by suggesting the establishment of a new set of international laws under the General Assembly, which includes more states (Representaciones Diplomáticas De Cuba En El Exterior). This comprehensive approach of Soesanto that considers transparency and inclusivity would help promote international legislative cooperation.

Cybersecurity and Deterrence Cooperation

Implementing cybersecurity and deterrence in a governmental bureaucracy is challenging and complicated because a deterrence theory, "a military strategy under which one power uses the threat of reprisal effectively to preclude an attack from an adversary power," is usually advanced for the deterrence of physical attacks (Britannica). As finding the culprits of anonymous cyberwarfare attacks is difficult, governmental institutions must establish a proactive measure, not simply a defensive, when addressing cybersecurity.

Jim Legg, the CEO of Thycotic, a private software company that provides cyber access security, stated that "there needs to be better gathering and sharing of governmental cyber-threat intelligence, use of big data analytics, and operational processes in place to take immediate action" (Legg). Legg also promotes the cooperation between government agencies to establish a rapid risk management protocol with expertise and technology developed for intelligence on threats "as well as ability to track, measure and manage incidents"(Legg).

Besides cooperation between government agencies, the CFR and IIGG emphasize the importance of cooperation between the government and private-sector companies. The prominent benefits of cooperation between the two sectors are the enhancement of defense through the focus on technologies, collective strengthening of the U.S response protocols for future crisis scenarios, and the establishment of information-sharing analysis centers (CFR). As the separation between governmental and non-governmental defensive actors has been blurred, the cooperation not only among government agencies but also between private and public sectors would lead to a well-rounded cybersecurity program.

Conversely, Nathaniel Gleicher, the Head of Cybersecurity Strategy at Illumio, a cloud computing Security Company, and former director for cybersecurity policy in the National Security Council at the White House, calls upon the impractical nature of cyber deterrence

(Gleicher). Without the improvement in security, “dissuading all comers from exposed high-value information through deterrence alone would not only be incredibly difficult to achieve,” but the intensity of deterrence that is needed would be so excessive to the point that it could “destabilize international relations and be greeted with criticism at home and abroad” (Gleicher).

Considering the two areas of examination, it is clear that there is a strong need to establish an international legislative norm that is inclusive and transparent to all member states. Additionally, effective communication and compromise between cold war countries are necessary for a clarified standard that can facilitate punitive measures against cyberwarfare. Furthermore, cooperation between government security agencies and private and public sector entities would promote a more compelling proactive deterrence system against cyberwarfare. For this to happen, more national legislation must be authorized to encourage private sector involvement. With these two considerations, the international community would be able to sustain its law enforcement and judicial sectors to efficiently minimize cyberwarfare.

D) Case Study

The following are key powers to the agenda. The following countries’ stances and way of dealing the problem will be crucial to resolution-writing.

1. United States

Being one of the first countries to introduce the Internet and one of the major countries, the United States is very vulnerable to cyber-attacks. However, also being the biggest military superpower of the world, the US has taken great efforts to defense through unending patches and versions of systems and programs. The United States has a Department of Defense Cyber Strategy which aims to defend the US homeland and interests from attacks occurring in cyberspace. The United States has a notable policy of five pillars on how the US can prepare for cyber-attacks. The five pillars are recognition, active defense, defense of critical infrastructure, collective defense, and maintenance of advantage. There have been many contentious actions of cyber-warfare towards the US, such as the Chinese attack on the US Office of Personnel Management or attacks on US corporations such as Sony Pictures. However, the US has done equal amount of actions of cyber-warfare against Iran, China, Russia and various countries. In 2016, the US announced to use military Cyber Command to execute attacks against Islamic State. The United States will be a critical agent in solving the Cyber-warfare matters due to its leverage.

2. China

Chinese hackers have been accused of attacking other countries through cyberspace by various countries but the Chinese government has strongly denied the allegations of state-sponsored hacking. However, many analysts and experts claim that China's cyber-attacks are an active threat. China allegedly has various private organizations which are dedicated to international espionage. China also was blamed for the US Office of Personnel Management's massive data breach which contained over 21 million people's data. The recent economic warfare on trades between China and the US was also started because of President Trump's claim that the Chinese hackers were stealing trade secrets from the US corporations which caused huge loss in the US' revenue. Likewise, the Chinese cyber actors all strive to advance China's security interests and its standing.

3. Russia

The Russian government was often accused of conducting or orchestrating cyber-attacks against various countries. One of the best known events is the US official's claim that the Russian hackers were involved in the American election to disrupt the Democratic Party and the allegedly state-sponsored attack on Ukraine. The Russian espionage dates all the way back to the late 1990s and has been happening non-stop ever since. Allegations against Russia include spreading of propaganda and "fake news", internet surveillance and harmful malware.

4. Israel

Israel is recently emerging as a cyber-superpower. Israel allegedly retains 10% of global sales of computer and network security technology. The Israeli government invests a considerable amount of resources to promote security-related technology and develop combat means in the cyber-space. The most advanced army in the Middle East is the Israel Defense Forces (IDF) which bases their power on advanced weapons and new technology. As developed the country is, Israel also receives many cyber-attacks from other countries. In 2013, a group called the Syrian Electronic Army attacked the control system of Haifa and in 2014, the Anonymous also attacked hundreds of websites of banks, schools, and etc. Luckily, Israel was well prepared for cyber-attacks and reinstated websites quickly. Currently, the Israeli government stands at the forefront of cyber technologies and will even go to far measures to block the security threats the country faces.

5. North Korea

North Korea is believed to be behind a significant number of cyber-attacks, primarily against South Korea. Some analysts claim that North Korea is even a bigger threat than Russia. North Korea's elite hacking unit, the "Lazarus group" is believed to have created the WannaCry ransomworm in 2017. The malware took down worldwide IT systems and caused great damage to various countries. North Korea is expected to continue its attacks in 2018 as well.

The following are case studies of main cyber-warfare in the history. Understanding these key events will help the delegates to set the course for the resolution.

1. Ukraine crisis

On September 12th of 2013, Ukraine agrees to sign a trade deal with the EU to remove export tariffs. However, it was to be delayed a year to avoid a clash with the Russian government. Nonetheless, protesters broke out in the pro-Russian East Ukraine but the protest quickly escalated and left dozens of people dead. After a few months, the Ukrainian president launches a military action against the protesters which cause eastern regions to declare independence. In May of 2014, a new president replaces the former president. The replaced president signs the contentious trade deal, which angers Russia and the people of East Ukraine, causing them to commit actions of terrorism. Afterward, the fight keeps escalating to get worse up to 2015.

In the Ukraine crisis, one can find the cyber-space involved in an unprecedented way. Unlike other cases, Ukraine, one of the main agents, is not as digitally advanced or connected. Here, cyber-attacks are mostly done by the Russian government against Ukraine. In 2016, Russian hackers targeted the Ukrainian institutions about 6,500 times in less than two months. Russia repeatedly denies the accusations but analysts claim that the Russian president is resorting to hacking more and more. Through this case, the delegates can see that cyber-attacks can be used by states to target other states and mandate specific actions from the state.

2. 2007 Cyber-attacks on Estonia

The conflict started when in Tallinn, the capital city of Estonia, a Russian-speaking mob began rioting. Because of the riot, the Estonia government tried to remove traces of the Soviet Union from Estonia but caused anger from the Russian government. After this event, reports of digital attacks began flooding in. Websites of the Parliament, major universities, national newspapers and others were crashing. For a long time, Estonia had claimed to be the most technologically advanced government in the world but Estonia's maneuver towards the cyber-attacks was poor. Through this event, Estonia faced great loss in various areas and realized that the event was an act of war through the most unsuspected way. The global community and the Estonian government suspected the Russian government to be behind the attacks. However, there was no concrete evidence that the attacks were actually state-supported by Russia.

Currently, the Estonian government has a voluntary Cyber Defense Unit and the techniques that were pioneered in Estonia are known as the "Gerasimov doctrine". Through this case, the delegates can learn that no matter how much technology is developed in a certain state, the state must have additional ways to withstand cyber-attacks or the state can face the same situation.

E) Bloc Points

1. In terms of international security, should cyber-attacks be accepted as a new form of warfare and be prevented by DISEC?

2. Considering how challenging it is to track the perpetrators in cyber-space, could states blame other states for the attacks only by assumptions?

3. Should states be punished if state-sponsored individuals executed cyber-attacks on other states but claims that the execution itself wasn't ordered by the state?

Debatable points:

1. Is cyber-attack in form of warfare being overrated considering the number of attacks done each year? Some people claim that cyber-attacks aren't eligible to be considered as actual acts of warfare because its leverage is insignificant compared to actual body-on-body military wars. If the delegates claim that cyber-attacks shouldn't be considered as official warfare, there would be less of a need for the United Nations to try to control it, helping the cyber-developed countries. However, this stance has the potential to make the states look over the riskiness of cyber-attacks and make them vulnerable to attacks. On the other hand, if the delegates insist that cyber-attacks be taken as official acts of warfare, international security will be kept safer but the United Nations would need to control the development in cyber-space by states and might eventually cause the technological development to slow down. The ultimate consensus on stance of this would set the direction of the resolution, so the delegates are recommended to keep this is mind.

2. Should cyber-warfare be controlled by international organizations or state governments? This point could depend on how the delegates view cyber-attacks. Seeing the cyber-attacks as conducted by individuals would mean the delegates support control by state. Considering cyber-attacks as more of acts of warfare conducted state-to-state would suggest that the problem be mediated by international organizations. It is rare that attacks are conducted directly from state government building but a lot of the attacks are suspected to be state-sponsored. If the attacks are controlled by state-government, it would be easier to punish individuals for such actions without taking things to the International Court of Justice, but if the actions were conducted for the state's interests, there are dangers of weak punishment. This point could be connected to the above. Regarding cyber-attacks as inter-state would undermine the claim that cyber-attacks be controlled by states. During resolution-writing, the delegates will need to propose solutions and which agent the solution is connected to will be important.

F) Bibliography

http://bestdelegate.com/research-binder-friday-disec/

http://bestdelegate.com/how-to-model-un-research-ga-first-committee-disec/
https://www.saintpeters.edu/guarini-institute/files/2013/01/Disarmament-and-International-Security.pdf
https://edition.cnn.com/2016/09/29/asia/china-cyber-spies-hacking/index.html
https://investigaterussia.org/timelines/russian-cyber-attacks
https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/
https://www.meforum.org/articles/2016/israeli-defense-in-the-age-of-cyber-war
https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia
https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC?utm_content=buffer8c7a2&utm_medium=social&utm_source=plus.google.com&utm_campaign=buffer
https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia

Bibliography for Past Actions

"2017 Cybersecurity Policy Priorities." 2017 Cybersecurity Policy Priorities, U.S. Chamber of Commerce,

"71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." Representaciones Diplomáticas De Cuba En El Exterior, 23 June 2017,

Blake, Aaron. "Here Are the Latest, Most Damaging Things in the DNC's Leaked Emails." The Washington Post, WP Company, 25 July 2016,

Bowcott, Owen. "Dispute along Cold War Lines Led to Collapse of UN Cyberwarfare Talks."The Guardian, Guardian News and Media, 23 Aug. 2017,

D'Incau, Stefan Soesanto & Fosca. "The UN GGE Is Dead: Time to Fall Forward." ECFR, Ecfr.eu, 15 Aug. 2017,

Dogrul, Murat. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism . NATO CCD COE , pp. 1–15,

Eddy, Nathan. "Cyber-Terrorism Poses Major Threat to Government, Business." EWEEK, 4 Feb. 2018,

"Experts and Staff: Stefan Soesanto." European Council on Foreign Relations,

"Forrester." Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016,

Gleicher, Nathaniel. "Will U.S. Sanctions against Russia Fix Cybersecurity?" TechCrunch, TechCrunch, 9 Jan. 2017,

Government of the United Kingdom. Policy Paper: National Cyber Security Strategy 2016-2021. Gov.uk.

International Institutions and Global Governance program, and Council on Foreign Relations.Workshop Summary Report Cyber Threats and International Cooperation. Council on Foreign Relations, 2015,

Jazeera, Al. “'Major Disruption' as UK Hospitals Hit by Cyber Attack.” UK News | Al Jazeera, Al Jazeera, 12 May 2017,

Korzak, Elaine. “UN GGE on Cybersecurity: The End of an Era?” The Diplomat, The Diplomat, 1 Aug. 2017,

Mayer, Lauren A. “Cyber Warfare.” RAND Corporation, RAND,

NATO. “Tallinn Manual Research.” CCDCOE, 2 Feb. 2017,

Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press, 2015.

The Editors of Encyclopæ dia Britannica. “Deterrence.” Encyclopæ dia Britannica, Encyclopæ dia Britannica, Inc., 12 June 2017,

The Global Risks Report 2018 13th Edition. World Economic Forum, 2018,