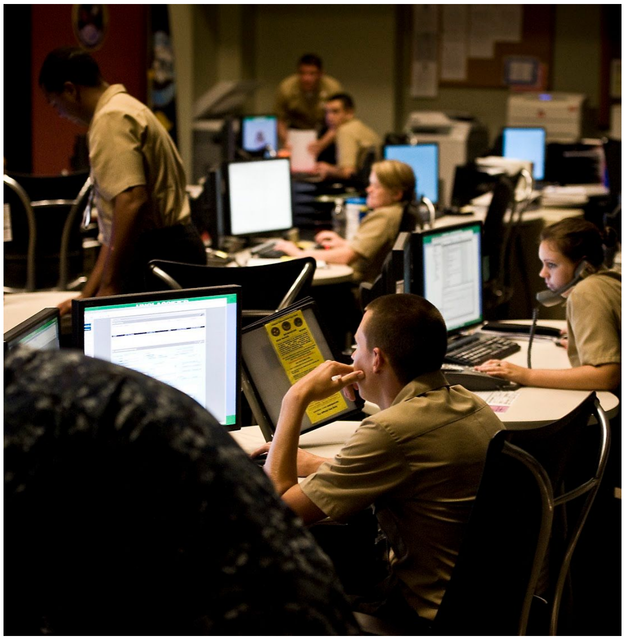
Cerritos Advanced Conference 2020

1st The Disarmament and International Security Committee (DISEC)



Topic A: The Regulation of Autonomous Weapons

Topic B: Cyberwarfare

Director: Neha Lala

POSITION PAPERS DUE on October 17th by 11:59 pm to Committee Email

October 24-25, 2020

To Delegates of CHSMUN Advanced 2020

Dear Delegates,
Welcome to CHSMUN Advanced 2020!

It is our highest honor and pleasure to welcome you all to our 2020 online advanced conference here at Cerritos High School. On behalf of the Cerritos High School Model United Nations program, we are proud to host our very first advanced conference, where you will become more knowledgeable on international issues, participate in intellectually stimulating discussions, and create new and everlasting friendships.

The CHSMUN program continues to compete around the world as a nationally ranked MUN program. Our delegates utilize diplomacy in order to create complex solutions towards multilateral issues in the global community. Our head chairs are selected from only the best seniors of our program, undergoing a rigorous training process to ensure the highest quality of moderating and grading of debate. Furthermore, all the topic synopses have been reviewed and edited numerous times. We strongly believe that by providing each and every delegate with the necessary tools and understanding, he or she will have everything they need to thrive in all aspects of the committee. We thoroughly encourage each delegate to engage in all of the facets of their topic, in order to grow in their skills as a delegate and develop a greater knowledge of the world around them.

Although this wasn't what we expected, our advisors and staff have put in countless hours to ensure delegates have an amazing experience at the online conference. Our greatest hope is that from attending CHSMUN 2020, students are encouraged to continue on in Model United Nations and nevertheless, inspired to spark change in their surrounding communities. With this strong circuit consisting of 6 schools and over 500 delegates, CHSMUN Advanced 2020 will provide a quality experience for intermediate delegates to enhance their speaking and delegating skills.

If you have any questions, comments, or concerns, please contact us! We look forward to seeing you at CHSMUN Advanced 2020!

Sincerely,

Anjali Mani and Karishma Patel

sg.cerritosmun@gmail.com

Secretary-Generals

A Note From The Director

Delegates,

My name is Neha Lala and I am so excited to be the head chair for the 1st DIsarmament and International Security Committee (DISEC). I am currently a senior here at Cerritos High School and this is my 5th year in Model UN. Model UN has provided me with many unforgettable memories each year, and continues to shape who I am today. I enjoy traveling to places such as UC Davis and New York for conferences, which give me the opportunity to bond with my peers. Outside of MUN, I am a part of the Swim and Waterpolo team, so you can often catch me poolside. I love talking to friends, riding my bike, and going on runs very early in the morning. When I'm not doing any of these activities, you can catch me curled up in the corner with a good boor, or an addictive TV show. Overall, I understand it is nerve wracking and new that conferences are online yet this is a great opportunity for us to learn how to do Model UN a different way, and hopefully we all can grow from this experience. Be confident in your speaking abilities! I can't wait to see you all and if you have any questions or concerns, please send an email my way! Good luck!

Sincerely,

Neha Lala

Disec.CHSMUN@gmail.com

Director, 1st DISEC

Committee Introduction

Established in 1946, the United Nations Committee for Disarmament and International Security (DISEC) was the first committee to be added under the General Assembly. Created in order to deal with issues regarding disarmament, global security, and the maintenance of world peace and international collaboration under Chapter IV of the United Nations Charter, it seeks solutions in order to ensure the security of nations worldwide. Charter IV states that the committee is responsible for maintaining international peace and security through the general principles of cooperation and those governing disarmament and the regulation of weaponry as well as to deliver recommendations to the Members or to the Security Council as to what topic to meet on next. Working closely alongside the UNODA, or United Nations Office for Disarmament Affairs, they are able to work together on disarmament topics such as nuclear, conventional, and weapons of mass destruction. Established in response to the atrocities of

World War II, the Nagasaki and Heroshima incidents became the committee's first focus along with growing concerns of the global implications of the atomic bomb. Since then, it has strived to prevent such acts of violence from occurring and threatening international security. Since then, DISEC has successfully dealt with topics ranging from the Syrian arms trade to bioterrorism, cybersecurity, nuclear disarmament, amongst many others. Recently, however, SPECPOL has taken a more specialized approach to many of DISEC's security roles, so the First Committee has been focusing on preventing weapons proliferation, with special emphasis on nuclear weapons since World War II. With the 21st century bringing a technological revolution, DISEC's responsibilities have expanded to accommodate our growing dependence on data, and how to protect the data, as well as the expansion into outer space. With this, some of the pressing topics dealt with thus far include the issue of international jurisdiction and peace in space, as well as maintaining digital privacy between countries. The 1st DISEC provides a platform for each country to share their views on issues regarding disarmament, global security, and the maintenance of world peace and international collaboration.

TOPIC A: The Regulation of Autonomous Weapons

Background:

Eliminating the human error in weaponry, artificial intelligence (AI) has been developed by computer scientists since the 1950s, in hopes to make weaponry able to detect targets without human intervention. These AIs would be able to use a network of algorithms which would allow them to be able to predict and act accordingly, based on the surroundings. The algorithms would allow the weapons to "learn" and adapt, freeing them from the need for outside control. With the increased interest in this technology, research has expanded to militaries wanting to acquire this technology in order to expand their arsonal for possible future warfare. These AI technologies would be manufactured into autonomous weapons making them self sufficient, deadly weapons. Autonomous weapons, as defined by the United States defense are weapons that "once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage in targets without further human input after activation." They have AIs making them self reliant, however, are immune to human judgement calls and emotions and therefore, will harm whatever they perceive to be a threat, regardless of whether they are or not. Autonomous weapons used in combat by militaries allows them to obtain and process information more efficiently, and use that information to make better decisions. The surveillance and database feeds provide the militaries with increasingly accurate information and interpretation of that information, which is done simultaneously. This not only saves time, making data gathering more efficient, but also allows for the militaries to make more accurate decisions with the extra information available. This also reduces the need to deploy information gathering personnel, allowing them to relocate the funding. The AIs in the weapons are programmed to be able to gather information about their surroundings and react accordingly. This decision making, which can be done without human intervention, eliminated the need for personnel to guide and control the actions of the weapons. Moreover, this allows the AI in the weapons to stay objective, where humans could be clouded by external factors such as fatigue, emotion, weather, and other judgement calls, among many others, which could be overwhelming, especially in high stress situations. Therefore, the long term improvement of the software for the autonomous weapons is allowing it to be expanded to other technology such as tanks and aircrafts, to not only revolutionize military capabilities but also allows a cost effective and efficient decrease in manpower, while also improving judgements in high stress situations. Issues with autonomous weapons however are widespread, as being self reliant is that there is no way it would be able to be programmed for every possible situation, leaving a large margin of error. As they are meant to be deployed in dangerous, high stress scenarios, they could be in situations which have not been anticipated, and would not know how to react. This makes them dangerous as it is difficult to see how they would respond until a situation as such, arises. To make matters worse there is no way to predict how they would react as there is no communication with the system in the weapon, so reasoning is hard to establish. Furthermore, interest in understanding how the systems in autonomous weapons react in a variety of situations has become a growing field with military experts arguing whether personnel would be needed to monitor it, making it counterproductive. Moreover, a fully loaded autonomous weapon would be a one time investment of around $230,000 while the yearly cost of having a human combattant is around $830,000, furthering the incentive for countries wanting to transition to autonomous technology. The main concern with replacing soldiers with autonomous weapons is that while they may be able to carry out tasks without hesitation, where human emotions would intervene, they may not be able to distinguish between an armed combatant and a civilian. With nations such as China, Israel, South Korea, Russia, the United Kingdom and the United States already possessing the technology for autonomous weapons, they have the power to dominate during warfare, making them powerful countries in the global community. Autonomous weapons have the power to break international laws, in which cause accountability comes into play. As these weapons are not controlled by humans, the question of accountability for mistakes made by the weapons becomes prevalent. Thus far, killer weapons which use AI, have been developed by Israel, and sold to the United States, Chile, China, India, South Korea, and Turkey. From which point China has reverse engineered a more advanced version, bringing the world closer to the use of fully autonomous weapons, which depend on AI. As such, accountability can not be placed on programmers, engineers, or the military personally as they have not committed the “crime”, and the system of algorithms within the weapons can not be punished as they lack the capability to have emotions or judgement making any attempts to “punish” futile. The United Nations Fifth Review Conference of the High Contracting Parties to the Convention on Certain Conventional Weapons (CCW) created the Group of Governmental Experts (GGE) reached the consensus that countries who deploy the lethal autonomous weapons, should be the ones held accountable for the damage that the weapons cause. Seeing as they are the ones who chose to deploy the weapons, as well as contracted the manufacturers, full responsibility should fall on the shoulders of the country who chose to utilize this weapon. As more nations follow the precedent set by China, Israel, South Korea, Russia, the United Kingdom and the United States, an arms race could be triggered. These weapons would transform warfare as it is known, and therefore more countries would follow in the development of this technology coming close to triggering a race as none would want to be left behind in this advancement. However, it is also important to keep in mind that not all countries have the resources to match and create this kind of technology and therefore it is important that no country is left behind. Seeing as fully autonomous weapons are not a reality as of yet, killer robots are the closest the world has today to these weapons. Yet, even as the predecessor of this lethal weapon exists, regulation and legislature is scarce and board. This is pertinent as it not only is vague as to which party assumes responsibility in the case of accidental harm or killing, but there are also no regulations as to what these weapons are allowed to do. The lack of these guidelines is what makes the situation even more dangerous, as despite fully autonomous weapons not being in use as of yet, they are going to be a reality in the very near future, and the global community is aware of this. There is no preparation happening in order to accommodate for these soon to be lethal weapons, which makes them much more dangerous. If the legislature is on hold until these weapons become a reality, then in their early days they could be allowed to run rampant which could cause unfathomable damage. Overall, as autonomous weapons develop more advanced artificial intelligence systems, virtually eliminating the need for both human commbattants and also those who monitor the current drones, but are also capable of taking lives, of both of their targets but also civilians who may get caught in the range of the drone. Being equipped with artificial intelligence it would be able to learn from each attack, but since it is not able to have the same judgement and emotional intelligence as their counterparts, it is impossible to predict how they would truly react in the variety of situations they would be put in. As they are able to kill, this uncertainty comes at a huge risk. With more and more countries striving to obtain this technology, autonomous weapons can change the future of warfare, making it deadlier than ever before.

United Nations Involvement:

The United Nations created the Convention on Certain Conventional Weapons in 1980 which consists of 125 member states. From this body, a treaty was established which bans the use of weapons that have the capabilities to be lethal to both soldiers and civilians. Since then, several Non Governmental Organisations (NGOs) and 19 countries have joined together to form a coalition known as the Campaign to Stop Killer Robots whose goal is to prohibit the development, manufacturing, and use autonomous weapons. This coalition has only grown since, as in 2017 greater than 70 countries in addition to the International Committee of Red Cross met at the CCW Group of Governmental Experts conference, in order to talk about the three major pillars of the integration of autonomous weapons: increased research on the AI software of the weapons, military usage, and the ethical and moral aspects in the usage autonomous weapons. With the constantly evolving nature of the weapons, a strict timeline was established in order to be able to accommodate any changes made to weaponry. The goal of this conference was to address the issue and create guidelines for future use of the weapons not to ban them. The United Nations Fifth Review Conference of the High Contracting Parties to the Convention on Certain Conventional Weapons (CCW) created the Group of Governmental Experts (GGE) whose purpose is to discuss advancements regarding autonomous weapons. The first meeting was in November 2017 and the first topic it covered was "examining emerging technologies in the area of LAWS, in the context of the objectives and purposes of the CCW, and with a view toward identification of the rules and principles applicable to such weapon systems." A consensus was reached at this meeting stating that international humanitarian law applies to autonomous weapons, and accountability for the actions of the weapons fall upons the country who deployed them. Furthermore, the United Nations Office for Disarmament Affairs (UNODA) partnered with the International Committee for Robot Arms Control under the Human Rights Watch held a discussion regarding "Pathways to Banning Fully Autonomous Weapons" in October of 2017. In this several member states met in order to discuss the future of autonomous weaponry, its production, and most importantly its implications on the global community and its peace. First DISEC has also met regarding the potential risks of the new weaponry (autonomous weapons) in which member states exchanged stances on the topic, with working papers underway.

Case Study:

As many predecessors of the autonomous weapon are currently in use all with the AI as a driving force, it is no surprise that some of these weapons are already having noticeable effects. The Northrop Grumman X-47B is an unmanned aerial vehicle (UCAV) which was created for carrier-based operations. Created by the United States in conjunction with the defense technology company, Northdrop Grumman, he X-47 project began as part of DARPA's J-UCAS program, and subsequently became part of the United States Navy's Unmanned Combat Air System Demonstration (UCAS-D) program. The X-47B is a tailless jet-powered blended-wing-body aircraft capable of semi-autonomous operation and aerial refueling. It was first utilized in 2011, and as of 2015, it has undergone extensive flight and operational integration testing, and successfully performed a series of land and carrier-based demonstrations. In August of 2014, the US Navy announced that it had integrated the X-47B into unmanned carrier operations as its AI had been successfully created, and by May 2015 the aircraft's primary test program was declared complete. The X-47B demonstrators themselves were intended to become museum exhibits after the completion of their flight testing, but the Navy later decided to maintain them in flying condition pending further development to not only their AI system, in hopes to develop a fully autonomous weapon, putting the country at the forefront of weapons advancement.It was given 635.8 million dollars by the Nary in 2007 in order to further their advancement, but by January of 2012, the X-47B's total program cost had ended up being close to 813 million dollars. Government funding for the X-47B UCAS-D program was supposed to run out by September of 2014 on the basis of lack of development. However, in June 2014 the Navy provided an additional $63 million for "post-demonstration" development of the X-47B as break through had happened with AI development, allowing for the device to be known as a killer robot, bringing the country closer to developing the fully autonomous weapon they desired. Thus far the United States has been in a close race with China to see who could build the first fully autonomous weapon, which would give them a huge advantage in the global community.

Nevertheless, it is safe to say lethal autonomous weapons are in our near future and will be a reality in the oncoming years.

Bloc Positions:

Western: The westen bloc is known to be at the forefront of technological advancements especially with the United States pouring the most amount of money into weaponry including autonomous weapons. Thus far, the United States is one of the few countries which has nearly developed fully autonomous weapons yet under the pressures of the international community has strictly regulated these lethal weapons. Canada and the majority of the bloc have supported the ban on autonomous weapons and have thus far not started to develop these weaponry, but the AI and software is underway and could be modified to be used in weapons in order to make them autonomous. Member states of the European Union have banded together to establish their own guidelines on autonomous weapons usage in warfare. Having established their own centers to research the technology, small scale research competitions have arisen between the countries.

Latin American and Carribean: The entice bloc supports the ban of autonomous weapons and the majority have been a part of the several coalitions and conferences. However, countries such as Chile and Brazil have developed artificial intelligence programs. These programs have been increasingly profitable as they have been able to detect their surroundings and transmit the data back to the military. Being in its early stages, this technology would not be able to support a fully autonomous weapon, but further development is still underway. With internal struggles, advancements are widespread. Chile and Brazil have been sharing their information with the lesser developed countries in the bloc, as they not only support the banning of these lethal robots, but also of not leaving the lesser developed countries behind when it comes to technological advancements.

African: The bloc has had none to little advancements when it comes to developing autonomous weapons technology, both the hardware and software. They have been trying to expand their information gathering technology, with little advancements such as Morocco starting a data portal, which would allow for increased information access to what they've gathered.

Asian-Pacific: While the entire block supports the ban on autonomous weapons with the exception of China and South Korea, they have also been expanding their AI technology which can easily be integrated into hardware. Having a centralized database regarding some of the information gathered, the majority of the countries work together, similar to the Latin American and Caribbean bloc, to ensure that the lesser developed countries are not being left behind in the development of this technology. China has spent 2 billion dollars thus far on the development of the AI technology for the weapons, and even more on the hardware to complement the AI software. South Korea has several lethal drones and are underway of developing fully autonomous weapons in order to revolutionize their military. These two are the only ones who possess the AI technology to have nearly fully autonomous weapons and are underway to perfect the technology.

Basic Solutions:

When addressing the peaceful and sustainable uses of outer space, delegates should be mindful to stay within the mandate of DISEC and the General Assembly, and focus on solutions regarding disarmament of weapons thus far, but also ensuring than if this technology does become widespread then it is contained and lesser developed countries, who do not have the resources to allocate to the development of such technologies, are not left behind and therefore are at a disadvantage. As several countries are coming close to developing fully autonomous weapons, it is imperative that the technology is not used to take unnecessary lives as they are lethal. With many countries already being a part of the coalition of the Campaign to Stop Killer Robots, it has already been decided to ban and severely limit the usage of autonomous weapons, but as this is only a suggestion, several countries have been furthering their development into this technology. With this, one feasible way to ensure that these weapons have not been deployed, which could possibly cause a transnational war is the use of X-Ray imaging and blinding lasers. X-Ray imaging, which would be done by satellites, would be able to detect these weapons, should they be deployed as they would be large enough to have all the AI technology and work remotely. Should they be detected as an international threat, blinding lasers could be deployed which would be able to temporarily disable the autonomous weapons and prevent them from causing any harm. All being done from the satellite, this is not only cost effective but also can be monitored at all times in order to make sure that these lethal weapons are not being used to initiate conflict. With the simple addition of the A1-7 software developed by the United States, and the laser deploying technology, this could be implemented, preventing conflict from these lethal, dangerous weapons.

Questions to Consider

1. Has your country signed any legislation or attended meetings regarding the use, development, or production of autonomous weapons? What legislation needs to be passed to ensure that autonomous weapons are not widely used?
2. Has your country developed AI technology for autonomous weapons, or have they started to develop such technology? If not, then what are future plans regarding the use of autonomous weapons?
3. What are some possible safety measures that can be implemented in order to make sure that autonomous drones do not break international jurisdiction or international humanitarian law?
4. How can accountability be established in the case of autonomous weapons? And to who (the country, the software, the manufactures)?
5. How can it be ensured that lesser developed countries are not left susceptible to other countries should they not have the technology? What kind of aid should be given?

6. What should be done with weapons who have entered another country's jurisdiction, whether intended by the country of origin or not? Should intent matter, as these devices are capable of making "decisions" for themselves?

Works Cited:

1. Felt, Coley. "Autonomous Weaponry: Are Killer Robots in Our Future?" *The Henry M. Jackson School of International Studies*, 14 Feb. 2020, jsis.washington.edu/news/autonomous-weaponry-are-killer-robots-in-our-future/.
2. "First Committee Weighs Potential Risks of New Technologies as Members Exchange Views on How to Control Lethal Autonomous Weapons, Cyberattacks | Meetings Coverage and Press Releases." *United Nations*, United Nations, www.un.org/press/en/2018/gadis3611.doc.htm.
3. *History & Development of Autonomous Weapons*, cs.stanford.edu/people/eroberts/cs181/projects/autonomous-weapons/html/history.html.
4. McCormick, Ty. "Lethal Autonomy: A Short History." *Foreign Policy*, 24 Jan. 2014, foreignpolicy.com/2014/01/24/lethal-autonomy-a-short-history/.
5. "States Call for Enhanced Arms Control Strategies to Regulate 'Killer Robots', Stem Rising Tide of Illegal Weapons, Delegates Tell First Committee | Meetings Coverage and Press Releases." *United Nations*, United Nations, www.un.org/press/en/2019/gadis3635.doc.htm.
6. "Stopping Killer Robots." *Human Rights Watch*, 18 Aug. 2020, www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and.
7. Hambling, David. "Autonomous Killer Drones Set to Be Used by Turkey in Syria." *New Scientist*, 20 Sept. 2019, www.newscientist.com/article/2217171-autonomous-killer-drones-set-to-be-used-by-turkey-in-syria/.
8. Jonah. "Killer Robots Aren't Regulated. Yet." *The New York Times*, The New York Times, 13 Dec. 2019, www.nytimes.com/2019/12/13/technology/autonomous-weapons-video.html.
9. McCormick, Ty. "Lethal Autonomy: A Short History." *Foreign Policy*, 24 Jan. 2014, https://foreignpolicy.com
10. "Taranis." *BAE Systems | International*, www.baesystems.com/en/product/taranis.
11. *U.S. Department of Defense*, www.defense.gov/.

Topic B: Cyberwarfare

Background:

It has become increasingly easy for countries to wage war against one another due to the threat of cyber warfare which has become increasingly prevalent in the past 20 years. With many countries going almost fully digital, the way countries and other organizations can hurt one another becomes much easier to accomplish. Due to havoc that cyberwarfare can cause and the hold that it has on today's population, it is natural that there are many ways cyber warfare can be performed which include espionage, sabotage, propaganda, and economic disruption, and there are a wide array of reasons behind cyber warfare which include military, civil, hacktivism, private secretary, and profit and non-profit research. Cyber warfare is not just used for countries or large organizations waging war against one another, in-fact, being cyber attacked is one of the most common types of attack waged, with over 765 million being affected in April, May, and June of 2018 alone. The twenty-first century ushered in a technological revolution which changed how people live their lives, but with this revolution comes many problems. Computers and smart machinery have become the most important resource a country has, as with everything moving to being remotely controlled. Between nuclear codes, sensitive governmental information, and centralized databases with information about nearly every citizen, the information which each country holds on the internet is insurmountable. Subsequently, other countries, terrorist organizations, and hackers amongst many others, want to get their hands on this information. This is done through the use of "cyber weapons", which are able to deploy attacks that can disable and take control of other countries' software. These attacks are classified as forms of cyber warfare, and arguably are more deadly than physical combat, as it not only deals with people's intellectual property, but also sensitive information about governmental projects, personnel, and other information protected by nations. Cyber Warfare attacks are a newer form of warfare, which many countries are left defenseless against, and can cause a massive amount of damage. Robert Tappan Morris, a student at Cornell, was the first to build a cyberweapon, more specifically the software of one, in 1988. Known as the "undetectable worm", he created an experimental program which is injected into the internet and can replicate fast, and spread to other computers even faster. To test this program, he put it into the internet from a computer in the Massachusetts Institute of Technology, and to his surprise, the program spread so fast and it was so powerful that the presence of the program was enough to slow down the processor causing the whole computer to shut down. As this was a shock to everyone, computers across the United States were affected with the worst effect being in military bases, medical facilities, and electrical grids. This result showed that programs could be made which could target computers worldwide, and with the correct modifications, it would also be able to extract information, and that countermeasures would be needed in order to combat this form of attack. In the last 20 years, these attacks are becoming increasingly dangerous which can threaten both national and international security. In 2008, a Turkish oil pipeline exploded as a result of being on fire, taking the lives of two workers, showing the world the true repercussions of a cyberattack. None of the motion detectors for security footage were alerted, forcing the cause of the attack to be ruled as unknown, until further inspection of the security measures takes place. After the inspection took place, it was established that hackers had taken control of the security cameras, security cameras and motion detectors and rendered them useless. After eliminating the security measures, they gained control of the pipelines pressure gauges among other settings, and increased the pressure allowing for an explosion to occur. This caused the Azerbaijani government to have to pay millions of dollars in order to repair the pipes, clean up the mess, and deal with the death of two of their citizens. This was done to show the global community of the catastrophic events that hackers can cause to occur, remotely. To prevent this from occurring again, the majority of the oil plants worldwide were forced to disconnect from the internet, as a safety precaution. Unfortunately, as technology is constantly evolving and growing more advanced, so are the hackers. As technology is present in almost every aspect of our lives providing us with convenience and comfort, this also allows hackers to have access to those parts of our lives. This is increasingly dangerous as information is key, and people knowing everything about it comes with a myriad of risks. The deeper technology is integrated into life, the more dangerous these attacks get, and unfortunately, we have already seen this happening. A malware virus known as Stuxnet is responsible for the worst cyber-attack to date. Created in 2010, it was suspected to have been developed by the United States and Israeli government in order to target and stall the Iran Nuclear Program's development. Understanding that the Iranian program used the data program known as Siemens, the goal of the Stuxnet virus was to get control of and search all of the devices which were created by the company which were running the Iranian SCADA manufacturing system. The Stuxnet's first step was to infect computers which were related to the Siemens manufacturing industry. From there, the virus would spread from the infected computer to all of the devices on the same network and operating system as it. It was then able to identify the devices which were being sent to Iran, connect to the internet, and infect each device it had not yet infected. It then updates its software in order to get past the system undetected. This virus compromised the SCADA system from there, and found its weaknesses. The information was sent back to the governments and the virus has gained control of the machinery. Having this control, they exploited the weaknesses and caused all the machinery to fail beyond repair, including the ones for the Iranian Nuclear Plant. Once this was discovered by the scientists in the plant, an evacuation and a temporary shutdown occurred. This sabotage, which is suspected to be from the United States and Israeli government was to prevent the Iran Nuclear Program from creating a nuclear weapon.Being the leading target of cyber attacks, the financial sector has to develop strong counter measures. However, despite having these countermeasures, small scale cyber attacks are a daily occurrence as they have the most lucrative and easily exploitable information. Having access to people's finances, account details, social security, address, and much more could not only devastated a person, as this information could lead to secondary issues such as identity theft, but also is an attack on the nation. If a large scale bank is attacked, they have access to thousands is not more, of the citizens private information, which could then be used both against them, and leverage against the government. By using this information, hackers, which could either be individual or sent by another country's government, could leverage this information for either other information from the government, or negotiate for what they want. Along with this, there is the obvious harm to large scale cyber attacks on the financial sector, with the theft of the banks money. This inturn provides monetary benefits, however is also an attack against the government as a whole as banks are supported by the national government and if banks are emptied out, the government loses their entire investment, which is generally millions of dollars.

United Nations Involvement:

While cyberwarfare is a newer issue, seeing as how devastating it can be, there have already been several UN actions on the issue which include conventions, the establishment of organizations, resolutions, and committee sessions discussing the issue. The first of which was in 1865, with the establishment of the International Telecommunications Union (ITU), which was adopted under the UN when it was established. The ITU now has 193 member states and 600 public partnerships. Dealing with the actions of all telecommunication technology, it has placed emphasis on the security of telecommunication. Under the General Assembly, the ITU passed A/RES/55/63 in 2001, which defined the punishment for cybercrimes, in broad and simple terms. This was the first resolution to be passed on the matter, and was therefore revolutionary. It brought to light the dangers of cyber warfare as well as addressing that cybercrime offenders should be incarcerated in the same way as other offenders and under the same legal rights. In addition, the resolution also said that all nations should have laws which specifically deal with technology related crimes. In addition, A/RES/45/121 was also passed, however, this stated that the Eighth United Nations Congress on the Prevention of Crime and Treatment of Offenders are responsible for defining the treatment of criminal offenders should they commit transnational crimes. Originally passed in order to deal with physical crimes, its jurisdiction had been enlarged in order to encompass cybercrime offenders as well. In 2015, a working paper on Information and Communication Technology (ICT) specifically dealing with International Peace and Security was started by the United Nations Institute for Disarmament Research (UNIDIR). The resolution A/RES/70/273 was passed in 2017 despite disagreement on many parts of the issue. When it came to light that telecommunication could be used as a weapon, 1st DISEC adopted the issue, and passed the resolution A/RES/1378 on November 20 of 1959. This was a landmark resolution as it was ratified by all member states. Being passed before knowing the threats of cyber warfare, its ideology still applies to the situation today.

Case Study:

In October of 2010, the United States stock market was hacked by another country. A malware was discovered in the NASDAQ servers. Seeing as the United States Stock Market is upwards of a trillion dollar industry, a search was conducted leading to upsetting results for the United States government. The search concluded that the malware contained military attack strike code, which could only be from another country. After this malware was discovered, a 5 month, in depth investigation was launched by the National Cybersecurity and Communications Integration Center. It was found that a previous development of this malware was developed by the Russian government, and the malware found was only an improved version of it. This spread panic throughout the financial private sector, as it brought to light the lack of security measures in place to protect such information, and how easy it was for another country's government to infiltrate a large part of the country's economy. The malware was detected before damage could be done, but it has been classified as a "digital bomb". When evaluating motives for the attack, it was found that it could either be for profit, sabotage, or destruction. However seeing as little damage was done by the Russian government, it was concluded that the attack from Russia was meant to intimidate the United States exchange, as well as gain information for their own exchange. According to the Bloomberg BusinessWeek, many financial institutions lacked the proper security guidelines to keep their information safe, and the only reason more damage was not inflicted was because the United States was "spared" by the Russian hackers, and if they even "bothered to try" then finances in the United States could have been cripled by the Russian government hackers. The attack on the NASDAQ exchange served to expose how vulnerable the rest of the United States was to cyber attacks. After this scare in 2010, security measures were revamped and servers, databases, and cyber infrastructure were made secure and resistant to hackers.

Bloc Policies:

Western: Being at the forefront of technological advancements, the western bloc countries heavily rely on technology and therefore use the most advanced cyber security software there is. That being said, the western bloc is also the most vigilant and has been suspected to have committed the most cyber warfare attacks. For example, the United States joined with the Israeli government in order to prevent the Iranian Nuclear Program from developing. Using such attacks to their advantage, the majority of the western bloc have been proactive in using cyber warfare in order to gain information from other countries, specifically about their arsenal, weapons and technology developing program, and information gathering projects which are underway. Having this information on other countries gives them an upper hand in the global arena.

Latin American and Caribbean: The Latin American and Caribbean bloc have been proactive in the regulation of cybercrimes in their countries. Mexico, Chile, Columbia, and Guatemala are at the forefront of this, as they have strict laws and regulations as to what constitutes a cybercrime and what punishment should be given out, based on the varying severity of cybercrimes. The bloc has been passive in involving itself in cyberwarfare suspicions, and is vigilant in protecting its own, and its citizens intellectual property as to not get into conflict with other countries over ownership of ideas. The more developed countries such as Brazil, Chile, and Columbia have been aiding the lesser developed countries in the bloc in protection of their technological development, and intellectual property.

African: The African bloc has the least advanced technological development amongst the other blocs however has been proactive on the protection of their data and technological infrastructure. Recently, in June of 2014, the African Union held a convention on Cyber Security and Personal Data Protection, in which they adopted a document. This stated that the countries of the union should be sure to have the proper firewalls and other security software in place in order to protect the data they have in the case of a cyber-attack. This includes protection of governmental activities as well as the citizens personal data which could be susceptible to attack.

Asian and Pacific: The Asian and Pacific bloc has been the victim of cyber warfare attacks from China for the past two years. In order to prevent this from continuing, they are strengthening both their security as well as their cyber weapons if the need arises to use them. They are interested in protecting their, and their citizens data, and do not want to go on the offensive. However, as they have been under attack for a prolonged period of time, they may go on the offensive. China however, has denied that they have committed any form of cyber-attacks and calls these accusations "absurd".

Basic Solutions:

Cyber Warfare is a broad topic which includes many subtopics such as cyber security, espionage, data protection, and transnational cybercrimes. It is important that delegates do not stray far from the main topic and get too caught up on the subtopics, which have a lot of specifics within themselves. Additionally, it is important that delegates do not stray from the mandate of DISEC and subsequently, the General Assembly, and make sure solutions revolve around international peace and security, disarmament, and regulation of weaponry.

Seeing as cyber warfare and small-scale attacks are a reality of the future, it is important that the international community has the proper defense software set in place. Seeing as virus malware is the most common form of attack it is imperative that cyber security be tailored to monitoring and protecting computers and other devices from attacks. Seeing as this malware is injected into one computer and then is spread to other computers through the use of the same network or mainframe, if computers have the software to detect this malware being injected into the computer, then it would automatically shut down, preventing the malware from spreading to other devices. A feasible way to do so is through the use of the SCALABLE Network Technologies' security softwares. Having security measure which range from protecting the electrical grids with the EXata Cyber software, networks from having malware and viruses spread on them with the EXata CPS software, as well as training the operators how to react in the case of a transnational cyber-attack with the Network Defense Trainer and JNE/Stealthnet. This would help protect databases, mainframes, and personal computers from being attacked by hackers, other nations, and anyone with malicious intent.

Questions to Consider:

1. Does your country have security set in place in order to protect the country in the case of a large-scale cyber-attack? If so, which ones, and to what extent do they protect the country's information? Does this protection extend to the citizens person all devices, or is it limited to governmental information?

2. Has your country passed any legislation which clearly states what constitutes a cyber-attack? If so, what are the specifics of the punishment of these offender's receiver? Are they tried under the same severity as physical offenders?
3. Should other countries get involved if two countries are attacking each other through the use of cyber weapons? Even if no lives are being taken? How should those countries be held responsible for breaking international resolutions and agreements?
4. How should hackers, who do not have any governmental affiliations, be tried? In the case that these hackers are committing a large-scale attack, involving several countries, under which country's laws should that individual be tried? Or should they be tried by a third party?
5. What cyber weapons does your country possess, if any? How should cyber weapons be regulated? Where should the line be drawn (for example: attacking governments for sensitive information or directly attacking the citizens to create panic, ect.)?
6. Where does your country stand in terms of censorship in order to protect its citizens? Do they believe this is unethical? Or have they participated in censorship themselves? If they have, then did they do it with the citizen permission or was it done without telling them beforehand?

Sources:

1. " Cyber Regulation in Latin America and the Caribbean." *Cepal*, 2020, www.cepal.org/socinfo/noticias/paginas/0/30390/newsletter15ENG.pdf.
2. Assembly, General. "Developments in the Field of Information and Telecommunications in the Context of International Security." *A/RES/53/70 - E - A/RES/53/70*, 4 Jan. 1999, undocs.org/A/RES/53/70.
3. "Cyber Security Defense Solutions." *SCALABLE Network Technologies*, 7 July 2020, www.scalable-networks.com/cyber-security-defense/.
4. "Cybersecurity." *Department of Homeland Security*, 17 Mar. 2020, www.dhs.gov/topic/cybersecurity.
5. Hackett, Robert. "Meet 5 of the World's Most Dangerous Hacker Groups." *Fortune*, Fortune, 23 June 2017, fortune.com/2017/06/22/cybersecurity-5-hacker-groups/.
6. Legroju. "The Directive on Security of Network and Information Systems (NIS Directive)." *Shaping Europe's Digital Future - European Commission*, 7 July 2020, ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
7. "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar." *Bloomberg.com*, Bloomberg, 10 Dec. 2014,

www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

8. Nakashima, Ellen, and Joby Warrick. “Stuxnet Was Work of U.S. and Israeli Experts, Officials Say.” *The Washington Post*, WP Company, 2 June 2012, www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.73747de39081.
9. Palma, Stefania. “Asia-Pacific Countries Fight Back after Wave of Cyber Attacks.” *Subscribe to Read | Financial Times*, Financial Times, 4 Oct. 2018, www.ft.com/content/e846aeac-914f-11e8-b639-7680cedcc421.
10. Pierluigi Paganini Pierluigi Paganini is Chief Information Security Officer at Bit4Id, and Pierluigi Paganini. “The Rise in Global Cyberattacks Highlights the Dangers of Cyberespionage.” *Veracode*, 19 Aug. 2015, www.veracode.com/blog/2015/07/rise-global-cyberattacks-highlights-dangers-cyberespionage-sw.
11. “STUXNET Malware Targets SCADA Systems.” *STUXNET Malware Targets SCADA Systems - Threat Encyclopedia - Trend Micro USA*, 1 Oct. 2010, www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems.
12. Riley, Michael. “How Russian Hackers Stole the Nasdaq.” *Bloomberg.com*, Bloomberg, 21 July 2014, www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.
13. That's according to an investigative report Bloomberg Businessweek. “Russian Hackers Placed 'Digital Bomb' in Nasdaq.” *CNNMoney*, Cable News Network, money.cnn.com/2014/07/17/technology/security/nasdaq-hack/index.html.
14. Yang, Stephanie. “The Massive Hack Of The Nasdaq That Has Wall Street Terrified Of Cyber Attacks.” *Business Insider*, Business Insider, 17 July 2014, www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7.