Cleveland Council on
WORLD AFFAIRS

Cleveland-Spring Conference

2019

Position Papers for:

General Assembly

Delegation from: Algeria
Represented by: Strongsville High School

***Position Paper for* Disarmament and International Security (GA1 DISEC)**

The issues before Disarmament and International Security (DISEC) are as follows: Addressing the Uses of Cyber Warfare and Protecting Trade from Somalian Pirates. The issue at stake is the decree to work to maintain cooperation and peace in the world and find a middle ground of level security among all countries.

I. Addressing the Uses of Cyber Warfare

DISEC has the responsibility of facilitating a relationship of peace and security between the internet and humans. The digital age is one that is virtual and physically untouchable. The idea of virtual warfare is one that is becoming of our generation and being idolized as the ideal weaponry attack system. Taking a stroll through history, the internet really did not surface until 1990, even though the United Nations (UN) prefaced the issue 1945 with Article 51 and the addressment of issues demanding "armed response". Yet the idea evolutionized with time to turn from this idealistic enemy to one that sits in front of the president of the United States. One tweet in this virtual age could push the self-destruct button on the United States and Korea's missile would be here in ten minutes. That being said, cyber warfare, the movie Blackhat in and of itself, is the next pawn in this warfare game that the world is playing with itself. People are utilizing the vulnerability of computer systems to hack in and take a piece away from countries and make them lose control at the hands of faith in their security and life.

The country of Algeria is extremely interested in the preservation of a sanctuary for Algerian citizens to be guarded from danger. Algeria over the past ten years has increased their defense spending and protection funds from 4,814,000 in 2009, to 7,673,000 in 2012, to 10,073,000 in 2017. Algeria in history has been denoted and resides in the position of 130th out of 193 countries for cyber security concerns. The main issue falls under the truth that Algeria is placed in the poorer continent of Africa that starts off not having adequate resources and help, then to go on and try to protect oneself against technological threats to government, when people in the country are not even drinking clean, fresh drinking water, is an issue that harrolds support higher than the country can give to itself. To have the means to regain with time the energy to stand up and fight the statistics of horrid resolve in Algeria.

Currently, Algiers are focusing on utilizing the National Gendarmerie and new forms of organization in the public continuum of security in a comprehensive approach to systems inlogs. Algeria's commander of the National Gendarmerie (GN) General Menad Nouba noted with the help of national security units, the Center for the Prevention and Fight Against Computer Crime and Cybercrime (CPLCIC), they tackled 1,000 cybercrimes in 2017, a 68 percent increase from in 2016. In April of 2018, the western city of Oran hosted the 6th African Cyber Security Summit to present findings of its barometer on cybersecurity in institutions and companies. The majority of users remain unprotected with little knowledge of threats and data. Over half of the respondents planned to increase security budgets by 21% in 2019 from the current situation now.

II. Protecting Trade from Somalian Pirates

DISEC has the integrity and provided responsibility to protect every individual under every notion of relating to keeping all people safe. However, the morals of a strong body are tested when it comes to the protection and security of a group of people who are just making it by from stealing to be with their families and provide for them, something that every human has distinctly instilled in one. The issues before DISEC regarding protecting trade from Somalian pirates comes as a package deal being that the truth of the issue being that a majority of people are in some way, shape or form are impacted in a way from the stealing of Somalian pirates and to consider that alongside that the situation of government the people find them in is so rough that people cannot provide for themselves and must fall on oneself to find goods and steal from others and wreck one's own morals. The moment is found that one sits in the chair of uncertainty and says, "Do I do what I can do to help or do I not care? Do I realize that the impact of my decision can completely alter and impact the lives of people? How do I make a change in these lives? Is it possible?" The answer is yes to all of that.

January 1st, 2011, on a vessel called the MV Blida, headed for a port in Mombasa, Kenya, blindsided and captured by a group of Somali pirates looking to make bank off of this group of 25 Algiers who just were with their families for the holidays, now gone for ten months, separate and afraid This is the force that is slowly taking down and damaging piece by piece the well-being of the countries that are being affected by this, predominantly Algeria as well. Algeria, residing on a part of water encounters this threat on a daily basis when it comes to making their way to ship themselves all over the world. The main issue is that the Somalian pirates believe they have gotten away with their deliberately painful and wrenching crimes that have ultimately left a footprint on this world's faith and trust in people. Thus, it takes great effort to begin erasing and trying to work away some of the tarnish on their reputation to eliminate the idea of them getting away with the price to still pay on their reputation.

Efforts to prevent this heinous crime from occuring has been slowly gaining support since the surge in pirate activities. Spending in the East African tourism sector of the budget has grown 25 percent more slowly than that of sub-saharan African budgets as far as piracy protection goes. The World Shipping Council (WSC) and the International Chamber of Shipping (ICS) are working closely together to help revise and advise the Best Management Practices (BMPs) industry for ships to prevent and respond to pirate attacks effectively, The catching of tuna fish in the Western Indian Ocean has declined by 26.8% during a time when any food that can be obtained for the country is important enough. The International Maritime Organization (IMO) and other governments are closely monitoring the activity in the water of the Indian Ocean to prevent future attacks from occurring. In 2017, the IMO approved interim guidance by private, armed guards to ship owners and operators in an attempt to prevent them from being blindsided by pirate attacks.

Delegation from India
Represented by Westlake High School

Position Paper for the United Nations Disarmament and International Security Committee

I. Uses of Cyber Warfare

In recent years, India has shown support for improving its cyber security and is progressively working to act on that encouragement. In previous years, the Indian government has not had an official government body that addresses cyber security issues along with cyber crime, but India has become more stringent on cybersecurity policies considering the cyber attacks that have occurred at the expense of Indian universities websites. A pakistani hacker group that calls themselves the 'Pakistan Haxor Crew' vandalized and contorted numerous websites belonging to several Indian Universities, namely Army Institute of Management and Technology, Defence Institute of Advanced Technology, Army Institute of Management, et. al. There have been cyber attacks on Indian governmental departments as well including the Prime Minister's Office, the Ministry of External Affairs, the Indo Tibetan Border Police, and the Defense Research and Development Organization.

In response, India has allocated the responsibility of preventing cyber crime to several government-backed agencies including the National Technical Research Organization, the Indian Emergency Computer Response Team, and the National Critical Information Infrastructure Protection Center. Kiren Rijiju, Minister of State for Home, has ardently voiced that India's efforts towards closing the gap between India's cyber warfare capabilities with those of other countries has become obligatory with consideration to the cyber programs of other countries that can cause serious damage if enabled to do so. Hence, looking forward, India remains firm in seeking preventative measures that ought to be taken to impede cyber terrorists from destroying the infrastructures of underdeveloped and electronically vulnerable countries worldwide.

II. Protecting Trade From Somalian Pirates

Maritime Somalian pirates have become increasingly problematic for India as a plethora of ships have been hijacked with the intention of demanding and receiving a monetary ransom. Additionally, Indian crew members aboard ships have been specifically targeted by Somalian pirates, indicating their newly promoted stance that involves subjugating overseas trade not only with India, but other countries around the globe as well. Piracy attacks have increased exponentially in recent years, involving incidents where hundreds of ship crew members have been taken hostage. Thus, India places prime importance on protecting trade not only due to the economic limitations piracy can create, but the consequential humanitarian crises as well. India is more than willing to work with other countries in stopping piracy from terrorizing overseas trade and fervently values the economic future of other countries in the very same sense.

I. Restricting the Use of Cyber Warfare

Over the past decade, the advancement of technology has greatly improved the status of common life as well as the power of many countries. However, as all great inventions of humanity are, technology was bound with a tragic flaw: its vulnerability to cyber attacks and hacking. The problem of cyber warfare has worsened in recent years and continues to concern the governments of many countries. As the world proceeds to enhance technology with smarter databases and quicker responses, the security of data online continues to be questioned.

Iran is an Islamic Republic founded in 1979 and believes in taking strong measures to establish our power. Iran's scientific advancement is reported to be the fastest in the world, and many of our technological aspects such as electronics and robotics continue to show great potential. These include the humanoid robot Surena II, as well as the production of multiple supercomputers over the past decade. In order to protect ourselves from the concerning increase of cyber warfare, Iran initiated an organization named "The Cyber Defense Command" in 2010, as well as the Iranian Cyber Police in 2011. According to the Institute for National Security Studies, Iran is seen to be a very active and powerful participant in the international cyberspace. Due to Iran's complicated relations worldwide, cyberwarfare is a sensitive and worrying issue for Iran.

Iran presents a comprehensive plan for the restriction of cyber warfare. As a victim of constant cyberattacks from the United States and Israel, Iran strongly believes the victims of security breaches need to be compensated for the political, economic and diplomatic losses. First, Iran believes in the establishment of associations in every interested country to maintain multinational cybersecurity. A clearly organized self-defense plan in each country against cyber attacks will be a crucial component in stopping data breaches. Second, Iran calls for an international organization of volunteers based on the United Nations GA1 committee that can present effective regulations and legislations for cybersecurity. There will be an international "police" under the supervision of all participating countries. In addition, this organization will develop stronger firewalls and advanced systems of encryption to lessen the impact of cyberattacks. Third, Iran also calls for biennial international conference to discuss the current situation of cybersecurity. The location will be determined by countries who feel is in the most critical and weakest position of cybersecurity, and it will be ultimately decided by the vote of international representatives. Each aspect of this solution establishes an organization on a national, international nongovernmental, and international governmental level. In conclusion, Iran wishes to restrict the use of cyberwarfare through these all-encompassing plans which discusses the conflict in diverse features.

II. Protecting Trade from Somalian Pirates

In a world where pirates seem like the creation of fantasy, Somalian pirates are pushed to steal goods from trading ships in order to survive. Their increasing number of hijacking commercial vessels have costed great economic loss. Resolution 2077, 2125, and 2383 has been established by the United Nations as a method to control these attacks, yet each of these resolutions were set to only last a year. With only temporary solutions given to the continuous attacks of Somialian pirates, the issue remains at hand for United Nations.

Iran was one of the victims of Somalian pirate attacks. During 2008 and 2009, the Somalian pirates went rampage in the Gulf of Aden and caused Iran to send two warships to the Somalian coast to protect Iran from such assault. Briefly before this situation, Russia also handed over Somalian pirates detained in their navy to Iranian representatives. The commander of the Iranian Navy even stated that the Iranian warships would stay at the Gulf of Aden until the Somalian pirates were no longer threatening. Due to these unsettling events, Iran and Somalia has been in serious diplomatic conflicts concerning the Somalian pirates.

Iran presents a multifaceted plan for protecting trade from these dangerous Somalian pirates. First, the countries wishing to support the Somalian pirates with funding and donations shall have their way. By giving Somalian pirates what they need, they will not cause problems that cause serious damage. Second, the warships of the concerned countries are to be located near the Somalian coasts to suppress hijacking and pirating. The countries that are involved with Somalian pirates will have to take individual actions, as such provided, for the sake of security and safety of their vulnerable ships. However, Iran understands that funding, donations and warships simply cannot make up for the necessity of the Somalian pirates. Thus, Iran presents the final part of the solution, which is the execution of Somalian pirates when necessitated by a global organization geared towards Somalian pirate control. This is the most simple, and the most clear-cut solution concerning this conflict. The cause of the problem must be eradicated somewhere, and it starts with eliminating pirates who have constantly imposed trouble. It is an easy process of thought: if there is no one to steal, nothing will be stolen. In conclusion, Iran presents a three-pronged solution concerning the Somalian pirates organized to the level of severity. By donations, the usage of warships, and executions, Iranian hopes to see a decrease in Somalian pirate conflicts.

Delegation from: State of Israel
Represented by: North Royalton High School
Committee: **General Assembly**

Position Paper for the United Nations General Assembly

The issues presented to the United Nations General Assembly this year are: Use of Cyber Warfare and Protecting Trade from Somalian Pirates. The State of Israel hopes to engage in cooperative discussion on both pressing matters. The State of Israel realizes the growing threats posed by growing cyber attacks and hopes to do what is necessary to ensure the international cyber safety. In addition, Israel is ready to enforce great measures of protection for trade in the area around Somalia.

I. Uses of Cyber Warfare

Israel is a state that heavily depends on cyber security technology. Every day our nation suffers innumerous amounts of cyber attacks across our networks, and we have considered it one of our gravest threat. Israel has been at the forefront of cyber security development and we seek solutions to defend against the common, yet strong threats to our national safety.

The motivation behind cyber attacks can be either political or criminal. Politically motivated attacks are used to critically disable military, governmental, or civilian networks in hopes of gaining an advantage over the enemy. The attacks forced upon us intend to weaken Israel, both internationally and physically. These attacks are carried out by forcing a device or system to take an action that it does not want to complete. These may lead to physical damage if the attack turns kinetic, which can occur in places such as nuclear power plants, water facilities, oil pipelines, factories, hospitals, transit systems, apartment buildings and more.

Israel has participated in cyber warfare, both defensively and offensively. In collaboration with the United States, Israel has created the Stuxnet and Flame viruses. These viruses have been used to gain intelligence on and temporarily delay, not completely disable, Iran's Nuclear Program. This attack was advantageous as it was unique because it allowed us to confirm locations of secret Iran facilities and subtly take information across known facilities without a direct invasion, which would be problematic on Iran's terrain. Israel's recently created Intelligence Unit 8200 and the General Staff's C4I branch have been involved in the development of offensive malware which will be used in potential counter-measures in case of attack.

In response to offensive cyber attacks, Israel has created Tehila and the National Information Security Authority (NISA). These two programs ensure the security of government office connections and critical national infrastructure. In addition, Israel has established the

National Cyber Bureau and Cyber Command in hopes of strengthening cybersecurity and preventing attacks from enemies that may soon catch up in cyber space and penetrate Israeli defenses. A proper goal of these government programs is to detect cyber attacks before they happen, as they are much harder to terminate once they are in effect. Israel has employed hackers given the objective of hacking our own public and private systems. This allows us to identify techniques used by attackers and construct new security measures to pre-emptively prevent any threats. Israel's Computer Emergency Response Team (CERT) also aids in identifying potential threats by highlighting ISP's with the highest potential to host attacks and blocking them before there is an opportunity to strike.

II. Protecting Trade From Somalian Pirates

The Somalian pirates have been a threat to shipping in the Gulf of Aden, Guardafui Channel and Somali Sea ever since 2005. Originally, the pirates had focused on hijacking fisherman boats and holding the crew captive for ransom. The motive for these attacks is unclear, but it is speculated that the somali fishermen may have been defending their fishing territory or resorting to violence after foreign toxic dumps caused heavy loss of sea life. As these attacks gained more organization and momentum, the pirates' targets have grown from fishing ships to international trade ships.

As the Somalian pirates keep heading for ransom of ship crews, Israel has deployed larger forces of security on trade, cruise, and fishing ships. Armed guards are prepared to fend off pirate skiffs that sail to the protected ship and are ready to use lethal force if necessary. In recent years, Israel had dominated the shipping security industry and employs retired IDF combat unit fighters to ensure trade and commercial ship safety.

The amount of organized pirate hijackings has decreased ever since the presence of the Combined Task Force 150, which is comprised of Russian and Indian Navy forces. New defense plans are enforced to ensure protection of trade ships sailing through the Gulf of Aden. Israel hopes to aid in preventive attacks against pirate strongholds and give effective contributions in future defense plans.

Delegation from: Jordan
Represented by: North Royalton High School
Committee: **General Assembly**

Position Paper for the United Nations General Assembly

Jordan recognizes the importance of the issues presented by the United Nations General Assembly and understands the need for increased conversation and debate on the topics. On the topic of Cyber Warfare and its uses, Jordan recognizes the need to set further guidelines and protections as this style of warfare becomes more and more prevalent in this modern world. Jordan also recognizes the need for the protection of trade from threats especially around the area of Somalia.

I. Uses of Cyber Warfare

Jordan strongly recognizes the highly destructive danger of Cyber Warfare and the need for the United Nations to address the issue. Jordan has been forced to witness to some of the greatest conflicts in recent memory like the continuous conflicts between the Israel and Palestine, the ongoing refugee crisis in Syria, and the looming threat of the Islamic State. In order to help alleviate some of the suffering, Jordan has opened its doors to refugees, however, this has placed increasing strain on existing infrastructure and has hindered economic growth and further development. However opening up these battles on a new front through cyber warfare forces additional tension in the Middle East and places Jordan under the direct threat of attack.

Jordan recognizes that this form of warfare is inexpensive in terms of money and that of human lives so it will become increasingly more prevalent in the years to come. Cyber attacks can cause the turbulent political landscape of the Middle East to change in an instant as nations now have easy access to espionage, offensive and defensive opportunities, and to launch entire attacks in an instant without hesitation. In order to protect the interests of Jordan and that of the refugees, Jordan stands united with the United Nations to set up efforts to create guidelines and/or a set of rules that would help determine the uses of such a decisive form of warfare.

Jordan has created programs and other opportunities to help protect from cyber attacks as Jordan's internet presence makes up roughly seventy-five percent of of the Arabic presence on the internet. Recently, Jordan has worked in partnership with the North Atlantic Treaty Organization (NATO) in order to implement an impactful national defense strategy as a member of NATO's Mediterranean Dialogue. Jordan strongly encourages the conversation about cyber security to continue and for there to be a reasonable solution.

II. Protecting Trade from Somalian Pirates

Jordan also recognizes the importance of trade is not interrupted or hindered by the actions of groups interested in pirating or stealing goods. Most notably, this has occurred off the coast of Somalia as a large portion of the world's trade travels through the area that is the Red Sea and the Indian Ocean. These vessels and their safety is necessary to ensure that trade (which is often vital to the success of many nations) is able to be performed.

Jordan encourages nations to individually and to collectively research and determine the best course of action in order to correctly address the issue and to provide the most cost effective and quick solution. Additionally, Jordan supports the efforts of the United Nations to further look into this issue and encourages further conversation between nations who struggle to protect their trade routes especially this in part of the world.

Delegation from: Mexico
Represented by: Saint John School

Position Paper for the General Assembly

The issues before the General Assembly are: Uses of Cyber Warfare; and Protecting Trade from Somalian Pirates. Mexico expresses its concern for international security, and is devoted to the contribution towards safer practices between nations.

I. Uses of Cyber Warfare

Technology has developed rapidly since the 21st century, and is continuing to improve every day. Although these developments improve many aspects of life, it poses a threat to national security. Hacking can be done virtually any time, anywhere, thus keeping national governments, as well as the United Nations (UN) on their toes. These security breaches concern intellectual property, digital trafficking, black markets, including uncirculated currency, such as Bitcoin, as well as many safety concerns. Larger world powers, such as China and the United States are at a technological advantage in comparison to smaller countries, posing a threat that is both unfair and unjust. With national technological threats, countries have little to no choice but to reciprocate, whether it be technological, or physical- both putting the safety of the world at risk. As a country faced with this issue on a national scale, among many others, Mexico believes that this issue is of utmost importance, and precautions, as well as policies must be set in place for the safety of the world as a whole.

For years, Mexico has been a common target for cyber warfare due to its vulnerable economy and strategic location. It is ranked as the second most attacked Latin American country with growing rates of attacks. It is not only a costly flaw, but it threatens the safety and overall well-being of our citizens. In 2017, Mexico, in collaboration with the Inter-American Committee Against Terrorism (CICTE), approved a new policy regarding cyber security. By approving Resolution AG / RES. 2004 (XXXIV-O/04), a Secretariat is delegated to build a cyberspace capacity for the responsible security for both national, public, and private sectors of web browsing. This resolution established Computer Security Incident Response Teams (CSIRTs), in each country to develop and regulate cyber security policies. Other countries utilizing this approach include Colombia, Panama, Trinidad and Tobalo, Jamaica, Paraguay, Chile, and Costa Rica. RES. 2004 has thus improved cyber security, yet it has its flaws, and must be built upon to ensure maximum security.

Mexico recognizes the rapidly developing issue of cyber warfare, and wishes to collaborate with the UN to develop a more detailed approach under the inspiration of RES. 2004. By understanding the necessity of technology in our day-to-day lives, as well as the concern of safety for all, we believe that a stricter regulation of entities such as browsing history and/or collected data is necessary. With the rapid increase of smart technology and artificial intelligence, the need for enhanced security is in dire need worldwide.

II. Protecting Trade from Somalian Pirates

Pirating has been a battle thus fought by the United Nations for decades. There has been a significant upswing in piracy in 2015 and 2016, and a slight downswing in 2017 and 2018. However, it is not a matter to overlook, as it both jeopardizes the safety of our oceans and sailors, as well as greatly affects foreign trade. The Somali economy is suffering, impoverished, and affected by illegal fishing in Somalian waters, thus pushing an increased need for piracy. On the other hand, there are better ways of improving such conditions with aid from the UN that will protect sailors, ships, trade, and Somalia as a country.

The Gulf of Mexico was once a large target for Somali Pirates, as it serves as a large coastal port for the shipment of products such as gas, oil, and drugs. It may not be a primary concern at the moment, but more incidents are arising, and it still poses a threat to Mexico. Although no official measures have been taken in regards to attacks in the Gulf, the UN has thus set forth temporary measures. In the 1982 UN Convention of the Law of the Sea, legal measures in regards to stopping piracy outlined how nations are to assist in protection against piracy. In addition, two resolutions have been passed specifically by the UN. Resolution 2077 secured military forces to conquer and prosecute captured pirated, later renewed as Resolution 2125. In 2017, Resolution 2383 was passed to commit ground troops to fight somali pirates, as well as expand naval support. The fatal flaw of both Resolution 2077, and Resolution 2125 is that they are only temporary. Considering the success of both resolutions, the UN must thus enforce permanent, strict measures to protect against piracy.

The idea of securing military forces, both land and naval, to protect trade ships from piracy is the strongest concept in both resolutions. However, certain changes should be applied. These appointed forces should not try to fight violence with violence, but rather work diplomatically with Somalia, to combat economic struggles. Naval ships are to patrol various bodies of water to ensure safe, clear trade routes between countries, whereas land troops should work with Somalia to conquer economic struggles, as well as work towards the persecution of captured pirates. Both troops are of equal importance, and serve as a safekeeping for all countries.

Delegation from: Democratic People's Republic of North Korea
Represented by: Gilmour Academy

Position Paper for Disarmament and International Security (First Committee)

The issues before the Disarmament and International Security Committee are Uses of Cyber Warfare and Protecting Trade from Somalian Pirates. The Democratic People's Republic of North Korea is heavily invested in promoting a peaceful digital climate, but would also like to note that it is dedicated to protecting its people from any acts of aggression, whether it be in the physical realm or the digital realm, and has thus thoroughly prepared itself to protect its people from any digital assault. The Democratic People's Republic of North Korea is also invested in securing its trade networks and is eager to work with other member states to eliminate the threat that Somali Pirates pose.

I. Uses of Cyber Warfare

As stated previously, The Democratic People's Republic of Korea is dedicated to promoting a peaceful climate worldwide. However, The Democratic People's Republic of North Korea would like to emphasize its priority of defending itself from western imperialism, and thus any talks of decreasing our cyber defensive capabilities are off the table. Fortunately, we have not been forced to engage in cyber warfare of any form, despite what the many smear campaigns propagated by the our enemies may claim. While The Democratic People's Republic of North Korea stands ready to defend itself from any act of cyber aggression, it notes that international cybersecurity is not a significant issue for member states at the moment, and that instead of dedicating funds to improving their cybersecurity, member states would significantly benefit from focusing their efforts on more pressing matters, like that of the second issue.

II. Protecting Trade from Somalian Pirates

The Democratic People's Republic of Korea is invested in maintaining its trade relations with various nations of the Horn of Africa and is deeply troubled by the interference of commerce that has been perpetrated by Somalian Pirates. The Democratic People's Republic of North Korea has had altercations with Somalian Pirates before, specifically that of the Dai Hong Dan incident of October 29, 2007. The Democratic People's Republic of North Korea thanks the United States of America for their assistance in dealing with the Dai Hong Dan incident and recognizes this assistance as evidence of a bipartisan struggle against those who engage in trade interference. The Democratic People's Republic of North Korea recognizes the universal disdain for these pirates and is eager to work with member states to resolve this concern that adversely affects all nations using trade routes in the Arabian Sea, and hopes that this bipartisan teamwork will not only serve to combat trade interference but also work to increase trade relations between The Democratic People's Republic of North Korea and other member states.

Delegation From: The Republic of Korea
Represented by: St. Vincent-St. Mary High School

Position Paper for the General Assembly

The issues before the General Assembly, First Committee Disarmament and International Security (Disec) are: Restricting the Use of Cyber Warfare and Protecting Trade from Somalian Pirates. The Republic of Korea is ready to represent the welfare of its citizens and come to peaceful resolutions for each of these topics.

I. Restricting the Use of Cyber Security

Over the course of technology's adaptations over fifty percent of private companies have experienced a cyber attack incident. With that, every citizen of every country is at risk to fall suit to a cyber attack whether an external or internal party. Cyber warfare is defined as "the deliberate use of computer technology to disrupt the activities of a nation state or organization". These forms of disruption can vary from simply stealing information to completely shutting down entire servers. Though cyber security has developed overtime to protect sensitive information, while the counter protection is developing, new complex and improved attacks through technology are developing as well. The Republic of Korea takes these threats seriously and holds cyber security to its utmost importance.

The Republic of Korea is no exception to the idea that every country has experienced a cyber attack. In recent history, South Korea's Hydro and Nuclear Power (KHNP) was attacked in 2014. This was not the first attack South Korea has endured. The country's agencies had be targeted for their sensitive information whilst compromising the welfare of both government officials and citizens. Attacks like these have prompted the Republic of Korea to enforce many technological security protocols. Programs such as the National Police Agency Cyber Terror Response Center, National Cyber-Security Center, and the Korea Internet and Security Agency have been created with the purpose of countering these attacks and ensuring that they become less frequent and eventually cease. The Republic of Korea hopes to use its past experience with cyber issues to effectively work with other delegations in DISEC to develop a resolution.

In this committee, the Republic of Korea will not be arguing the validity of a cyber attack but instead recognize the ability of any country to retaliate against a personal cyber attack and suggest specific guidelines on how a country should handle the situation. South Korea is looking forward to working with and hearing from each delegation in the committee. With many ideas and perspectives the delegation of the Republic of Korea is eager to develop strong resolutions to the issue regarding cyber warfare.

II. Protecting Trade From Somalian Pirates

Crime has always existed in the world but organized crime that affects businesses and governments alike is continuously becoming more common. Somalian pirates can be considered as an example of organized crime. These pirates have plagued the seas off the coast of Somalia and continue to interrupt the trade routes and systems of multiple countries trying to conduct business. While it is easy to only focus on the surface of this issue and the crime, this committee must look past the surface and analyze the stem of this issue, Somali, the country, as a whole. The Republic of Korea is invested in solving this issue in DISEC.

The Republic of Korea has personally dealt with issues concerning the Somalian Pirates. The most notable being the seizure of our chemical tanker, Samho Jewelry. The South Korean ship holding the tank was captured in the Arabian Sea and held in International waters so the pirates could successfully use the tank as part of their other ship attacks. The country defended themselves by launching Operation Dawn of the Gulf of Aden. This Operation included a destroyer and thirty naval commandos being sent to repossess the ship and rescue the crew. The Republic of Korea successfully handled the problem and thus publicly addressed crimeful the issue of the Somalian pirates. With the history of interactions between South Korea and Somalian Pirates, the delegation of the republic of korea is dedicated to permanently stopping the actions of the somalian pirates against every country.

The Delegation of Korea believes that this issue should be tackled with a short and long term solution. The short term solution pertaining to the surface level crime and the long term solution pertaining to the stem, the country. With a multi-facilitated approach, this committee can not only fix the issue but also set a precedent for other crime organizations that affect businesses and governments on a major scale. South Korea is willing to work with any nation on a solution as well as listening to counter perspectives on the topic. With the diplomacy, vigor, and knowledge, as a committee, DISEC has the ability to put forth a solid resolution for the benefit of all nations affected.

Delegation from: Spain

Represented by: North Royalton High School

Position Paper for Disarmament and National Security Council

The current issues brought to the council are: the rising problems with cyber warfare and how countries can restrict the use of it, as well as determining the proper use of force or protection for traders against Somalian pirates. Spain is well developed in its fight against cyber warfare and is determined to reduce pirate attacks, especially on their own country.

I. Restricting the use of Cyber Warfare around the World.

Warfare in today's world can be as easy as just a push of a button. The creation of the internet has led to a new form of crime involving hacking. Our world has become a hackers paradise. They can hack anything from social media to government secret files. Some hacks maybe miniscule and not be a problem, but some can take out power grids which could lead to thousands of people without power. Organizing several those attacks at a time and now a country could potentially reach a state of emergency. The need for protection against this threat is more important than ever before.

Spain is very set on the need for global restrictions on cyber warfare. Currently military advisors believe they are at a critical risk of cyber attacks. Colonel L.F. Hernandez Garcia specifically emphasizes that due to certain weak parts in their country could leave them vulnerable. Right now about 80% of required infrastructure such as energy plants and water treatment is lead by the private sector. This means that security for these important facilities could be hacked much easier than government run facilities. This makes protection against cyber warfare very important to Spain.

Due to intimate threats of cyber attacks Spain has a large amount of influence in the debate. Spain would prefer to see strong legislation passed in order to restrict how it is used and where it is used. They would also be in favor of legislation that would allow quick retaliation with strong force against countries that act with cyber attacks. Spain would help support and even take charge in the process of clarifying this new threat our world is facing.

II. Protecting Trade Ships from Somali Pirates.

The problem with somali pirates has been around for many years. However within the last 10 years these attacks have become much more prominent. Very often people are killed in the Arabian Sea and in surrounding areas due to these pirates. More recently the pirates have been capturing ships and taking hostages for ransom. People give in, which in turn gives the pirates more funding to buy better boats, weapons, ect. All the problems around the area is making trade much more dangerous for merchants and country's representatives.

This is also an important problem to Spain. Currently Spain has six somalian pirates in custody and they are being sentenced to 16 years in max prison. This is not a new thing for Spain. They have consistently faced the effects of these pirates and their hostilities. Spain has had trad ships, warships, and private owned vessels attacked by these pirates. Most of the time they are forced into ransom, but recently Spain has moved more towards strong force in an effort to end these attacks. However it appears to just be making them attack more public ships. This is why Spain is taking this matter seriously and making it of high importance.

Spain recognizes that action is desired against these attackers but would like to be at the front of creating the terms of action allowed against them. Currently there is very limited legislation for how pirates are to be handled. Some suggestions Spain has discussed is potentially creating a United Nations ran tactical team to help patrol the waters, and provide security for vessels in the area. Another idea is potentially going in with ground forces and taking out pirate bases and hideouts in hopes to entirely get rid of the threat. Either way Spain believes legislation is a must and the problem with somalian pirates needs to be resolved.

Delegation From: Sweden
Represented by: North Royalton High School

Position Paper for the General Assembly, DISEC

The issues before the General Assembly are: Restricting the Use of Cyber Warfare and Protecting Trade from Somalian Pirates. The French Republic is committed to aiding its citizens as well as other countries when dealing with development issues.

I. Restricting the Use of Cyber Warfare

As the emergence of the internet has drastically altered the way people communicate, there has been an inherent presence of cybercrime and cyber warfare. In 2017 alone, one in five Swedes were victims of cybercrime. These crimes summed up to a financial loss of nearly 4 billion USD. To combat this issue, Sweden implemented a national strategy on cyber security that focused on six principal areas. These included creating a comprehensive process for cyber security dealings, improving network security, increasing capability to prevent, detect, and intervene in cyberattacks, promoting IT expertise, and heightened involvement in international cooperation.

Sweden is supportive of developing more efficient cyber security systems as well as cooperating with other nations to work on resolutions that would decrease the frequency and severity of cyber attacks. If cyber warfare goes unchecked, the national security of all countries will be compromised. Sweden has recognized the dangers of cyber warfare, as in 2018, government spending on signals intelligence and cyber domain defence increased by ten percent to five-hundred ten million euros. Also, in 2019, Sweden will finish work on a comprehensive risk assessment looking into the nation's current cyber security measures. Sweden is committed to improving its cyber defense systems and hopes that other nations will do so as well.

As the internet's becomes more intertwined into daily life, it is important that action is taken to protect people's personal data, businesses, and critical governmental information. Sweden is devoted to preventing the proliferation of cyber warfare. Sweden hopes that other nations are willing to collaborate on resolutions that prevent cyber warfare, increase security measures, and penalizes aggressors.

II. Protecting Trade from Somalian Pirates

Within the last decade, there have been several dozen incidents in which Somali pirates have attempted to hijack sea vessels. The pirates have repeatedly interrupted international trade and have in some cases killed crew members of the ships they have seized. In other cases, captive crew members have been held as hostages for ransom. Sweden believes that action should be taken to more effectively protect commercial ships from pirates. Unless a long-term cooperative plan to mitigate Somali piracy is enacted, the safety of commercial vessels will remain suspect. Sweden is supportive of working on resolutions that would minimize the amount of pirate attacks, improves sea vessel security measures, and promotes economic development in Somalia.

Position Paper for Disarmament International Security

The issues that face the Disarmament International Security organization: Restricting the Use of Cyber Warfare; and Protecting Trade from Somalian Pirates .The delegation of Switzerland is committed to a productive debate that comes to a resolution reasonable to all countries involved.

A. Restricting the Use of Cyber Warfare

As technology expands and develops, it gives people access to harm others. Every 39 seconds, a hacking attack occurs. Technology may bring many benefits, but it also gives way to many evils. Cyber warfare is a growing issue that is only going to to get worse unless the committee of DISEC can come up with a reasonable resolution. With more than 200 billion technology devices in the world, the delegation of Switzerland wants tech users to be safe and secure on their devices.

Currently, Switzerland is unprepared for major cyber attacks. In the past, the country of Switzerland has been infiltrated by Russian hackers targeting Swiss state-owned defence contractor. Switzerland is attempting to build up its cyber defence, but is losing many of its IT specialists to google. Every year, 250 specialists are trained, but 200 go to work with Google. Switzerland aims to have 150 specialists by 2020. Switzerland has reported 14,033 cyber crime cases last year, a number that is much greater than any year before. A survey conducted 2 years ago has shown that 88% of Swiss companies have experienced cyberattacks. This is 34% more than 2016. These already-high numbers are going to continue to rise as they have been doing if this committee doesn't stop it.

Aware that most cyber threats come from Russia, the delegation of Switzerland would suggest a resolution that targets Russia. Switzerland would like to see the DISEC committee work together to create resolutions that provide safety and security on the cyber level.

B. Protecting Trade from Somalian Pirates

Since 2005, the Somalian pirates have been a threat to many countries' trading. What was once started as a Somali water protection group, has turned into an aggressive force of boat hijackers. In order to protect trade and the distribution of resources, the delegation of Switzerland is committed to a fruitful debate and the creation of a impactful resolution.

There are no records of a Swiss ship ever being attacked by Somali pirates. However, the delegation of Switzerland understands the hardships that other countries face because of it. Many of Europe's dry commodities and containerized goods come through the Gulf of Aden. Not to mention that almost 7% of the world's oil is traded along these routes. 30% of Europe's oil goes through the Gulf of Aden. These are very important resources that may be in danger because of Somalian pirates. The delegation of Switzerland believes a good solution to this problem is the use of military for trade protection. This has already been seen to decrease the amount of attacks. With a lot of its resources on the Gulf of Aden, the delegation of Switzerland would like to see this committee put an end to these pirate attacks.
The country of Switzerland calls for assistance from other countries in resolving this issue. Switzerland is open to working with other countries to find potential solutions to this issue, both short and long term.

Syria

Position Paper for Disarmament and International Security

The issues before the committee of Disarmament and International Security are: Uses of Cyber Warfare and Protecting Trade from Somalian Pirates. The delegation of the Syrian Arab Republic is committed to a productive debate that comes to a resolution reasonable to all countries involved.

Topic A: Uses of Cyber Warfare

Cyberwarfare is the use or targeting in a battlespace or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations pertaining to the threat of cyber attacks, espionage and sabotage. Cyber Warfare poses many different types of threats. Cyber Warfare can be used for espionage, sabotage, propaganda, economic disruption, electrical power grid disruption.

The use of cyber warfare has been used against the Syrian Arab Republic. Israel used cyberwarfare to carry out Operation Orchard, an airstrike that went undetected due to cyber warfare. Cyber warfare has played a very visible role in the Arab Spring and the subsequent Syrian Civil War. The Arab Spring, which broke out in Tunisia in late 2010, began to inspire political activism against the regime of Syrian President, Bashar al-Assad, in January of 2011. By March, this political activism was mobilized into non-violent, anti-Assad protests. The main grievances of the protesters were political and economic in nature. The protesters were upset about the economic inequalities and unemployment that had arisen from neo-liberal economic reforms that had been enacted by the regime.

The delegation of the Syrian Arab Republic would like to propose a committee to battle cyber warfare. The Cyber Security Committee (CSC) would hire highly skilled technical engineers to battle any form of cyber warfare.

Topic B: Protecting Trade from Somalian Pirates

After the collapse of the central government in the ensuing civil war, the Somali Navy disbanded. With Somali territorial waters undefended, foreign fishing trawlers began illegally fishing on the Somali seaboard and ships began dumping industrial and other waste off the Somali coast. This led to erosion of the fish stock and local fishermen started to band together to try to protect their resources. An escalation began, leading to weapons being used and tactics such as taking over a foreign ship until their owners paid a ransom. After seeing the profitability of ransom payments, some financiers and former militiamen later began to fund pirate activities, splitting the profits evenly with the pirates.

Somalian Pirates and terrorist groups have joined together to make profits. Terrorism has been a massive problem in Syria.

The delegation of the Syrian Arab Republic would like to propose having communication systems on all trade ships to alert close by militaries of countries that are part of the UN.

***Delegation of*: Tajikistan**
***Represented by*: Chardon High School**

Position Paper for Disarmament International Security

The issues that face the Disarmament International Security organization: Restricting the Use of Cyber Warfare; and Protecting Trade from Somalian Pirates .The delegation of Tajikistan is open to a constructive debate that comes to a justifiable resolution that works for all countries involved.

A. Restricting the Use of Cyber Warfare

Technological advances in the last decade have had a immensely large impact on the world and unfortunately it has not only been a good impact. The military had significantly grown in all areas such as decreasing man to man warfare, creating more lethal weapons, and created easier and more efficient weapons. All because of these great things, a new problem of cyber warfare has occurred. We need to find a balance between what is going too far and what is helping the military. The delegation of Tajikistan believes cyber warfare is a valuable improvement to the military and wants to see it used correctly and safely.

As of right now, Tajikistan is completely reliant on Russia because of the recently ended war and the fact it is a struggling third world country. Tajikistan is very undeveloped in technology, especially because around 1% of households have a computer in their homes. The majority cannot pay for internet in their homes because they can barely pay for food to eat. Because Russia supplies a large amount of money to Tajikistan, It means that we have to fully support Russia and the use of cyber warfare.

Because most of the cyber attack threats come from Russia, Tajikistan suggests that we come up with an agreement with Russia and write a resolution explaining how to limit and better control cyber warfare.

B. Protecting Trade from Somalian Pirates

The problem of Somalian pirates has gotten way out of hand. Especially because the expanding number of attacks has almost doubled in the time frame of one year along with hostages being taken is also rising. The United Nations has already addressed this issue before but because of the recent statistics, it needs to be re looked at. They created multiple resolutions in order to stop this problem. The delegation of Tajikistan is open to a productive debate to recreated resolutions that work for all countries.

Relating to the country of Tajikistan, Somalian pirates are not directly affecting them but they are directly affecting Russia. Somali pirates have been recently targeting Russian submarines and ships. The resources being stolen or destroyed are crucial for the countries they are being delivered to. But the delegation understands why the pirates are doing this because the country of Somalia is struggling economically just as much as we are. Tajikistan is open to collaborating with other countries to find ways to help Somalia become stable in order to eliminate the pirate issue.

The delegation of Tajikistan wants to work with other countries to revisit the previous resolutions created by the United Nations, write new resolutions making a stricter policy for trading goods through ships, and come up with ways to help stabilize Somalia's country.

Delegation of: Thailand
Represented by: **Chardon High School**

Position Paper for (Committee)

The issues that face the Disarmament International Security organization: Restricting the Use of Cyber Warfare; and Protecting Trade from Somalian Pirates. The delegation of Thailand is open to a constructive debate that comes to a justifiable resolution that works for all countries involved.

Topic A: Restricting the Use of Cyber Warfare

Technological advances in the last decade have had a immensely large impact on the world and unfortunately it has not only been a good impact. The military had significantly grown in all areas such as decreasing man to man warfare, creating more lethal weapons, and created easier and more efficient weapons. All because of these great things, a new problem of cyber warfare has occurred. We need to find a balance between what is going too far and what is helping the military. The delegation of Tajikistan believes cyber warfare is a valuable improvement to the military and wants to see it used correctly and safely. The US is attacking the government websites in Thailand and it is affecting millions of people in Thailand. To solve this issue the delegation of Thailand proposes to create a UNfunded committee in order to prevent cyber warfare being used.

Topic B: Protecting Trade from Somalian Pirates

Somalian Pirates are joining up with ISIS and are taking out trade ships and commercial vessels in order to make some profit. Somali pirates successfully attacked a Thai fishing vessel over the past 24 hours. Although one crew escaped, an anti-piracy expert said there were another two unsuccessful attempts this month. In March, another two vessels were captured just off the Somali coast. The crew of the Jaba escaped by overpowering their captors, but the Siraj crew was taken ashore in September. It was the first successful attack in the Gulf of Aden in two years. To resolve this issue the delegation of Thailand proposes to arm all ships and vessels travelling through Somali territory to prevent future raids against trading vessels.

Delegation of: **Uganda**
Represented by: **Chardon High School**

Position Paper for Disarmament and International Security

The issues before the General Assembly are: Restricting the Use of Cyber Warfare and Protecting Trade from Somali pirates.

Topic A: Restricting the Use of Cyber Warfare

The delegation of Uganda believes that the restriction of cyber warfare is a pressing global matter that concerns the safety of all citizens. In the last 30 years, technology has grown exponentially around the world. The internet has become societies form of storage, entertainment, and communication. While having this resource can be very useful, it can also be dangerous. The use of cyber warfare has emerged while the use of the internet has grown. Cybercrime and hacking have derived a total of 122 billion shillings, just in Uganda. Restricting cyber warfare is critical.

Overall, the delegation of Uganda as well as other underdeveloped countries are considered at a high risk for cyber attacks. In recent years, Uganda has seen a significant increase in internet usage by its citizens. According to the United Nations Department of Economic and Social Affairs, Uganda's internet access and usage has grown from 0.1% to 31.3% since 2000. With the rise of this access comes the rise of Ugandan cyber criminals. Thanks to hackers sophisticated knowledge of the web and the lack of cybercrime protection, Uganda has become one of the most at-risk countries for cyber breaches.

Statistically, the US is one of the most prepared countries for cyber warfare attacks. While internet has evolved, the US's cyber-defences have developed. Additionally, US citizens are aware of what a cyber attack is, what it looks like, and how to deal with it. If Uganda took the same precautions, their vulnerability to cyber attacks would decrease. The education of their citizens about cyber warfare is vital. Not only that, but developing a better cyber defence system would be beneficial for combatting these issues.

Topic B: Protecting Trade from Somali Pirates

The delegation of Uganda believes that the Somali pirates are causing a detrimental unrest along the Eastern Coast of Africa. The Somali pirates have hundreds of vessels in the Arabian Sea and Indian Ocean Region. Although not all of these attacks have been successful, it has happened enough times to raise concerns. The United Nations has taken actions on this problem before, but currently it is not enough to prevent this issue fully. Maritime transport is Africa's main gateway to the global market. If Maritime security is not improved, trade itself could be turned on its' head.

The country of Uganda receives resources to aid refugees as well as benefit the people of Uganda. However, the Somalian pirates continue to ravage the eastern coast, preventing the promotion of a better

life for the people of Uganda and the refugees staying there. The Somali pirates disrupt the imports and exports of Uganda. Trade is very important, especially for a country whose main source of income is agriculture. When the Somali pirates hijack ships and steal them, they are taking resources away from countries that need them.

Many countries on the East coast face huge challenges in fighting transnational maritime crime such as illegal fishing, drug trafficking, toxic waste dumping, and human trafficking. Enhancing Maritime security would combat all of these problems. In addition, if the force of the African Union was stronger, a lot of these maritime crimes could be prevented. The delegation of Uganda urges the United Nations to strengthen the presence of the African Union in Somalia.

Delegation from: United Kingdom of Great Britain and Northern Ireland

Represented by: North Olmsted High School

General Assembly, First Committee Disarmament and International Security (DISEC)

I .Uses of cyber warfare

Cyber warfare is one of the newest ways to conduct war between nations and has had very little regulation and prevention efforts by the United Nations. There has been little to describe how to react to cyber attacks since the start of the United Nations when it was addressed in Article 51 of the U.N.'s charter when it stated "that a nation can defend itself, if an (cyber) attack reaches a level of force that requires an "armed response"". The U.K. wishes that there can be improvements on the current standards on cyber warfare as it keeps growing in popularity and will continue to become more destructive in the future. Many countries throughout the U.N. are affected by cyber attacks with the majority of victims being in Russia and Asia, victims are also reported in western European countries and North America although at a much lower rate.

The U.K. believes that the top priority for the U.N. should be to reduce use of cyber attacks and minimize any potential effects it may have on citizens of the target nation. When a cyber attack is carried out there are many ways a nation state can be compromised along with its civilians being at risk of confidential information being stolen. There is a very clear example that was observed during the cyber attacks called "Red October" when governments agencies, embassies, and militaries computers all over the world were hacked and their information was transmitted to the individuals responsible for the program. The program was discovered on October 12 and uncovered on January 13 by a Russian firm called Kaspersky Lab. Kasbery Lab reported that the program may have been running for up to 5 years in many nations technology. The program has now been removed, but despite being a very widespread and security risk there was very little of a U.N. response to the attacks.

Cyber attacks that inflicts damage to technology or steal information can result in catastrophic issues within countries. The U.N. should address these new threats with specific and well defined circumstances for the use of cyber warfare and when an armed responses is necessary. The U.N. members should also work to minimize the use of cyber warfare between countries both part of the U.N. and not part of it for the benefit of public safety. The U.K. thinks that a beneficial strategy to solve this would be to have more accessible information between countries in order to get key information to halt cyber attacks. The United Kingdom thinks that all countries that are part of the United Nations should favor addressing and restricting use of cyber warfare and implementing measures that would minimize damages to the target nation and its population, expecaly between world power in the U.N. such as Russia, China, and the U.S. .

II . Protecting Trade from Somalian Pirates

Protecting trade from Somalian pirates have been a issue raised by the U.N. community due to a increasing frequency of pirate attacks on commercial ships. The U.N. has addressed these problems in "Resolution 2077" that secured the support of military forces to help fights against the pirates in nearby areas. Resolution 2077 also set in place prosecuting measures for pirates that have been captured by security forces. But since than there has been little help by U.N. legislation to aid in combating the growing amount of pirates. There should be more aid by the U.N. to help fend against these criminals.

The U.K. has very little experience when dealing with modern pirates but we still recognize that there needs to be some aid to help with this crisis. Some issues causing this increase of piracy in Somalia are poverty and famine. These can be traced back to illegal fishing which eliminates jobs and sources of food for local citizens of the area. In 2017 there were two pirate attacks in the area of concern both were solved with no reported casualties, but with an increase of regularity that may not be the same next time.

The U.K. wants the U.N to adopt a proposals that would help reduce the issues causing these acts to be necessary and we do that by mitigating problems like illegal fishing, poverty, and famine. Another solution to this problem would be to tackle the pirate issue directly via implementing measures that increase security in places of interest or making it less accessible to conduct pirating. The first solution would be more effective long term than the first so there should be a focus on those issues as opposed to the others.