DISARMAMENT AND INTERNATIONAL SECURITY COUNCIL

Topic A: Cyber Security
Topic B: Humanitarian Intervention

Chair: Stephanie Smelyansky
Vice Chair: Jack Spector Bishop
Moderator: Courtney Morrison
Dear Delegates,

Welcome to the inaugural GBSMUN conference and specifically to the Disarmament and International Security committee! Allow me to introduce myself. I am a senior at Glenbrook South High School and I hope to pursue a double major in biochemistry and political science next year in college. Model United Nations was a large part of my high school experience and I am glad to say that I found many of my closest friends through Model UN. My dais staff and I have worked hard to provide you with a realistic conference. Hopefully you will find the conference both a challenge and a good learning experience.

Our two topics for this conference are humanitarian intervention and cyber security. Both topics pertain heavily to international peace and stability and require the utmost attention to detail. As the chair of this committee, I want this conference to be a learning opportunity for new and experienced delegates alike, and thus I encourage all of you delegates to prepare beforehand and to also ask questions and engage with fellow delegates during committee sessions. If you have any questions about anything regarding the committee, please email me at 156306@glenbrook225.org.

Best regards,
Stephanie Smelyansky
History of Disarmament and International Security Committee (DISEC):

The United Nations has a long history dating back to the early twentieth century. At the end of World War I, President Wilson of the United States proposed a League of Nations which was to be a multilateral international body that would maintain world peace. Such a body was established but many nations such as the US did not join. As a result, the League of Nations was incredibly weak and was unsuccessful at preventing global calamities. As Japan and Germany became increasingly aggressive nations in the 1930s, they seceded from the League and they eventually formed the Axis powers in World War II. While the League of Nations was inefficient at creating peace, however, many people still had hope for an international governing body. Thus, President Roosevelt of the US and Prime Minister Winston Churchill of the UK drafted the Atlantic Charter in 1941 which set the outline for the principles that still guide foreign affairs today. The Atlantic Charter was the foundation of the Tehran and Moscow conferences in 1944 at which the leaders of the US, the UK, the USSR, and China agreed on a basic outline for an international peace-keeping body. At the Dumbarton Oaks Conference, the US, UK, USSR, and China further built the basic structure of what was to become the UN. Then, at the San Francisco Conference, delegates from 50 nations came together to create the first UN Charter in the spring of 1945. By October 24th, 1945, all of the five permanent members of the Security Council had ratified the UN Charter, and the UN was born.

The United Nations consists of many committees and subsidiary bodies, but one of its most important bodies is the General Assembly. The General Assembly is the policy-making organ of the UN as it is made up of all member states. Resolutions passed by the General Assembly typically require a simple majority, except for a few important questions such as those pertaining to
international peace, the election of non-permanent members to the Security Council, and the election of members to the Economic and Social Committee (ECOSOC), that must be settled with a two-thirds majority.\(^1\) Each member state receives one vote. The General Assembly is a key part in the codification of international law as well.

The Disarmament and International Security Committee is the first committee of the six main committees in the General Assembly. As a main committee, DISEC contains representatives of all member states of the UN at any given time. The responsibilities of DISEC include making recommendations to the Security Council about world peace and stability, discussing issues regarding international peace and stability, and make recommendations for the peaceful settlement of potential conflicts between nations. DISEC essentially debates all disarmament and security measures within the scope of the UN Charter. The committee also works closely with the UN Commission on Disarmament and with the Geneva-based Conference on Disarmament.\(^2\)

DISEC’s powers are dictated by the UN Charter. While DISEC is the main committee tasked with international peace, the committee cannot take many substantial measures in times of crisis. In times of crisis, DISEC’s role is to advise the Security Council on its future course of actions in response to a crisis unless the Security Council is already discussing the situation. Otherwise, during times of peace DISEC’s role is to make recommendations to the global community and the Security Council on maintaining world peace and to make recommendations for the friendly settlement of disputes between nations.\(^3\) DISEC does not have the ability to take actions that infringe on a nation’s

\(^1\)http://www.un.org/en/ga/about/ropga/plenary.shtml  
\(^2\)https://sites.google.com/site/ncsdmuncom/committees-3/ga  
\(^3\)http://www.un.org/en/ga/about/background.shtml
sovereignty, such as sending peacekeepers, and can only recommend such actions to the Security Council.

Works Cited


Topic A: Cyber Security

History of the Problem:

Cyber security can be defined as the necessary means or measures which are taken in order to ensure the protection of a computer system against an unwarranted attack. Through the past decade, as each nation has become increasingly reliant on technology as a means of storing data and operating their institutions, cyber security and cyber threats have also evolved into troubling issues. Many institutions that contribute immensely to the functionality of the country find themselves vulnerable to cyber-attacks from opposing, and often-hostile nations. Businesses, banks, schools, hospitals, and even government communications, are made susceptible to other nations that desire to sabotage and acquire information, thus destabilizing and threatening the security of the nation as well.

Hacking the control systems of the security and intelligence infrastructure has become increasingly widespread, no matter how safeguarded they may be. As so much of today’s society is completely dependent on functioning computer systems, cyber terrorism represents a serious threat to the international community. When assessing this threat, it is necessary to distinguish between three forms of cyber terrorism: attacks via the internet that cause damage to electronic communication systems, the Information Technology (IT) infrastructure, and other systems; dissemination of illegal content involving terrorist plans, actions, or rhetoric; and other logistical uses of IT systems by terrorists, such as internal
communication, information acquisition, and target analysis. Ultimately, Cyber-attacks have the ability to devastate not only a country’s well being but threaten their economic health.

Cyber attacks date as far back as the 1980s. In 1988, Robert Tapan Morris attacked the US infantile security structure called the UNIX system. The Morris Worm, as the bug was called, progressed by exploiting existing weaknesses in the UNIX system and slowed computers down until they were unusable. Despite Morris’ claims that the goal of his bug was to gauge the size of the Internet, he was the first person convicted by the US Computer Fraud and Abuse Act. Several cyber attacks followed in the subsequent decades, the most notable being when Estonia’s government systems were attacked by a foreign hacker in 2007. Though the Estonian government restored government services within a matter of hours, the attack provoked widespread fear. In 2008, the databases of both the Republican and the Democrat presidential campaigns in the US were hacked and downloaded by an unknown intruder, contributing to instability surrounding impending elections. DISEC has a responsibility to the international community to minimize the prevalence of such attacks for future generations.  

Current Status of the Problem:

As the world advances through the technology era, our increased dependency on technology has resulted in rising vulnerability to cyber-terrorism. Not only does this threat affect the world’s
common population, but also the various governments and businesses across the globe. Federal information, databases, consumer information and identities now have the potential to be stored through modern day technology. As our virtual world expands, enhancing cyber security systems and warding off cyber threats pose a major topic of interest to the United Nations.

Recently, JP Morgan Chase Bank, a banking system in the United States, was one of the thirteen victims of a mass-hacking attack. Investigators deemed this attack one of the worst attacks in history, as mass data was stolen from two of the major businesses targeted. The widespread attack breached the personal information of 76 million different households, presenting a massive security threat for Chase Bank. The hackers had the personal information of millions of people, making identity theft swift and easy, and also gained valuable information on Chase Bank itself. James Dimon, the chief executive of the bank claimed that Chase will be doubling its budget for cyber security in the future, according the the Wall Street Journal.

Snapchat, an international application used on smartphones to send and receive pictures, recently was hacked releasing over 13GB of personal pictures to the World Wide Web. As these pictures were sent to private “friends” through Snapchat, it is in clear violation of Snapchat’s terms of use. Snapchat has had encounters with cyber security issues before, but this
massive hacking has been declared the worst yet. DISEC will need to determine when to deem such events as inflictions on personal security as well as provide solutions to deter these hacks from occurring in the future.

Another massive cyber attack was launched against Target prior to Thanksgiving of 2013. In the weeks leading up to the holiday, someone installed malware into Target’s security and payment software. The malware functioned to record the credit card number of anyone who shopped at Target across all 1,797 stores after its installation date and then funneled the numbers to a Target server controlled by hackers. Despite Target’s investment in a $1.6 million security system called Fire Eye, which is also used by the CIA and the Pentagon, the cyber attack went unnoticed because security operators working for Target dismissed the alert given by the security system. In turn, Target went under fire with more than 90 lawsuits from customers and banks, losing millions of dollars as they tried to compensate for the breach. Consequently, DISEC also needs to address industry standards for cyber-security systems and standards for personnel staffing and developing security systems.

The European Commission of the European Union proposed the Network and Information Security Directive (NIS Directive) in March of 2014. This directive is aimed at attacking the global cyber security issues that lurk throughout the world by establishing five elements of a successful cyber security system: a national strategy that encompasses companies and government agencies, a trans-national cooperation network to combat international threats, creating minimal security standards,
imposing these security standards on the private sector, and finally enforcing them as law. According to the commission's consultation, 57% of respondents had recently encountered Internet security problems over the previous year. In addition, the United Kingdom has ruled Internet security as a Tier 1 threat to combating terrorism. If the NIS Directive is passed and adopted in 2015, it will provide minimum-security requirements for all cyber users.

These events are a few examples of the critical cyber security conflicts our world faces. DISEC will need to address and compromise on a solution to cyber security conflicts that has the potential to be implemented in every country in the United Nations.

Possible Solutions:

Cyber security is a polarizing issue that will drive debate throughout much of the twenty first century. However, there is a consensus that there are a few common international goals in the cyber security debate. Firstly, there is common interest in each nation protecting its critical infrastructure for cyber threats. This coincides with increasing timely responses to cyber threats. There is the common interest in strengthening cyber infrastructure and holding security agencies up to a standard international level of merit as well. Many countries lack any cyber infrastructure and thus the integration of cyber security into those nations is another goal.

One potential model for establishing cyber security systems would be to adopt the Framework model from US Executive Order 13636. Under the Framework, the Department of Homeland Security

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>Institutional understanding to manage cybersecurity risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td>Safeguards to ensure delivery of CI services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td>Identify the occurrences of a cybersecurity event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td>Take action (address) a detected cybersecurity event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td>Restore impaired capabilities or CI services from a cybersecurity event</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
develops a government-run cyber security system that is voluntarily adopted by individual companies. Companies can adopt the Framework when they become a significant part of the Framework’s security infrastructure. The problem with the Framework is that it’s a heavily government run program that’s voluntary and doesn’t establish universal security guidelines. For countries to adopt a Framework model, they would need to have a secure and centralized system of government, rendering the Framework obsolete for independent actors within countries experiencing political instability. Another potential model is to regulate cyber security at a minimum and allow government agencies and individual actors to purchase whichever cyber security plan they choose as long as it cooperates well with national security standards. While this approach keeps the security infrastructure from becoming too government regulated, it lacks integration and cooperation between different security actors and thus can often be ineffective in a security crisis.

Additionally, as the DISEC represents the international body of recognized states, it has the responsibility of drafting international cyber security standards. Such standards should outline which areas of cyberspace fall under the jurisdiction of a nation, essentially outlining the extent of a nation’s sovereignty regarding cyber security. An international set of standards should also outline good cyber security practices and potential models that individual nations and/or companies can adopt, loosely based off
of the Standard of Good Practice for Information Security document as it is currently the most comprehensive security guideline in existence today (Information Security Forum). This document stresses cyber resilience, data privacy in the cloud, mobile device security (BYOD), and critical infrastructure standards. Finally, solutions should seek to protect the individual rights of people who use any forms of modern telecommunications and the Internet.

**Bloc Positions**

*Developed Countries:*

There are multiple blocs regarding cyber security. One of the main blocs is comprised of Western and developed, democratic nations. These nations have largely developed technology systems and currently use many forms of cyber security. They are at the highest risk of a cyber attack as they centralize many of their security systems in cyberspace. As such, these nations seek greater regulation and development of cyber technologies so as to further develop their cyber security systems and ward off impending attacks.

*Underdeveloped and Developing Nations:*

Underdeveloped nations in Africa and in parts of Latin America comprise a second bloc. These nations often have unstable governments incapable of supporting large cyber infrastructure projects and thus do not rely much on cyber security. These actors however are interested in technological development and as time progresses wish to integrate into modern cyber security systems.
now, they are not as concerned with the details of cyber security standards and regulations as with the fair and easy access to cyber security systems and technological development.

The Middle East and Northern Africa:

The Middle East and Northern Africa constitutes a third bloc. Among this region, many states are either unstable or autocratic and they have a history with counterfeit legal documents and limited security. However, non-state actors such as terrorist organizations in these regions pose large cyber security threats not just to the Middle East but also to the world. These nations care more for the development of strong security systems that protect governments from terrorist attacks rather than creating affordable cyber security systems. These nations also are not concerned with civilian rights such as cyber privacy if this prevents them from developing stronger, more overbearing security systems.

The Developed Autocracies:

A fourth and final bloc is comprised of developed but largely autocratic nations that utilize cyber security systems. These nations, such as China and Russia, rely on cyber security but believe that international regulation on cyber security impedes on national sovereignty and thus do not believe in establishing an international set of standards for cyber security.

Questions to Consider:

1. How much of a role should the international community play in establishing uniform cyber security systems? How much of a role should the national government play in national security systems?
2. What role do non-state actors pose as security threats? What role do state actors pose as security threats?

3. How can the rights of individual citizens be protected?

4. How can non-belligerent, non-state actors be integrated into overarching security systems?

Works Cited


Topic B: Humanitarian Intervention

History of the Problem

Humanitarian intervention has been defined as a state's use of "military force against another state when the chief publicly declared aim of that military action is ending human-rights violations being perpetrated by the state against which it is directed." Humanitarian aid has been defined as “material or logistical assistance provided for humanitarian purposes, typically in response to humanitarian crises including natural disaster and man-made disaster. The primary objective of humanitarian aid is to save lives, alleviate suffering, and maintain human dignity.” Throughout history, however, these definitions have continued to clash. When other countries enter humanitarian crisis, how a foreign country intermediates can be perceived as either humanitarian aid or intervention, and sometimes neither is wanted or appreciated.

The Peace of Westphalia was a series of peace treaties, which concluded both the Thirty Years War in the Holy Roman Empire and the Eighty Years War between Spain and the Dutch. These treaties initiated the concept of a sovereign state (Princeton). A sovereign state is defined as “a geographic location having a permanent population, defined territory, one government, and the capacity to enter into relations with other sovereign states” according to existing International Law. It has become DISEC’s duty to determine when to classify relations between separate sovereign states as humanitarian intervention or humanitarian aid. The issue on whether nations, acting through the
United Nations, can serve to protect innocent civilians of different countries without other sovereign states perceiving such actions as abuses of power still presides over DISEC today.

The United Nations has been in charge of humanitarian intervention issues since the end of the Cold War. The main challenge for the UN is determining the rights of individuals versus the rights of states. The body was created with the underlying principle of not using violence or force to resolve humanitarian issues that occur globally. However, in past decades there have been arguments that the international community bears responsibility over all citizens in the case of a humanitarian crisis. During the Rwandan genocide in 1994, over 800,000 Tutsi and Hutu people were brutally murdered in an ethnic conflict. The UN Secretariat and the UN Secretary General were heavily criticized for not providing sufficient aid for the Rwandans in a timely and efficient manner. Individual nations were blamed as well for their lack of response to the genocide. The United Nations Assistance Mission For Rwanda (UNAMIR) was established to ease the peace process between two colliding groups, the Tutsis and Hutus. Although UN Peacekeepers were provided in Rwanda, they did not have the right to enforce any new laws or change the Rwandan government. Despite their benign intentions of aiding civilians, the UN peacekeepers presence was deemed a violation of sovereignty by the Rwandan government and thus few actions were actually taken by the peacekeepers.
Humanitarian intervention is usually regarded as legitimate when it is approved by the UN Security Council, however this bureaucratic process is often long and inefficient and typically heavily contested. The DISEC has a responsibility to procure a set of guidelines of what constitutes intervention so as to facilitate faster decisions by world bodies to act on behalf of civilians in danger without having to go through the arduous process of getting Security Council approval. The guidelines this committee will create would serve as the first universal foundation for addressing humanitarian crises across the globe, an important goal that will demand compromise and debate.

Current Status of the Problem

The increasingly interconnected global community of the 21st century has made natural disasters, humanitarian crises, and conflicts. The prevalence of these crises has pressured governmental agencies to take action in order to suppress the dissent of their constituents, and thwart impending disasters. However, the increase in governmental activity has raised the question of at what point does a government’s helping hand become an unwelcome intruder. This question has led to rising debate between what is constituted as humanitarian intervention and humanitarian aid. The distinction may seem trivial, but in reality it is the differentiation between war and peace, and this committee must come to terms with solid definitions on the distinction between these two concepts.

Recently, the international community has witnessed multiple debates over the motivation for humanitarian aid, and what legitimizes humanitarian intervention. The Journal of Humanitarian
Assistance notes that the predominant justification for humanitarian intervention is that of self-defense. Policymakers have argued that article 51 of the United Nations Charter states that when an event has the possibility of causing transnational refugee flow it constitutes unilateral or multilateral intervention into the nation in question. The intervention in this case would be justified due to empirics that indicate transnational refugee flow can be destabilizing to a relatively conflict-free region. Thus, policymakers argue that when nations are threatened from the potential of mass refugee flow, it is justified to take military intervention to return stability to the nation affected. This is exemplified by the recent events in Syria. The recent international intervention into the sovereign nation has been noted as a direct response to the threat that that nation posed against their own nations. This event further illustrates the complex nature of distinction of intervention in the world’s current state.

Furthermore, recent policymakers have begun to argue that intervention focused on humanitarian efforts are in reality a means to extend a nation’s international influence. In the case of the former Yugoslavia, the humanitarian efforts employed in the nation were simply a ploy for nations to illustrate their ground presence and militaristic abilities. Recently, American intervention in Syria was supposedly based on the concept of humanitarian aid. However, multiple authors have argued that the U.S. ignored the well-being of citizens within the country and the surrounding areas, instead focusing on the means to gain more credibility. The president went as far as to offer the dictator an ultimatum regarding his use of chemical weapons. These authors argue that the offer was aimed at
showing America’s hegemonic presence, and ultimately was strategically offered in the hopes of further legitimizing the unspoken influence that the U.S. holds.

However, the situation has once again become complicated as nations look to the situations that are developing in nations such as Yemen. Recently, Yemen’s central government came to terms with the radical militant group Houthis that had raided critical government buildings and forced out Prime Minister Mohammed Basindwa. The peace agreement between Houthis and the government however seems to have been pointless as Houthis has not demobilized. Now, Yemen is faced with an impending civil war that could cause a massive humanitarian crisis. In this case, the United States government and others have taken a hands off approach and are planning to send aid in lieu of participating in direct intervention. This form of “humanitarian aid” starts to complicate the previously stated definition that declared that intervention was justified whenever impending conflict were sensed. Ultimately, this crisis poses the question of whether or not countries will and should have the right to intervene in this conflicted nation.

However, there are several examples of successful humanitarian intervention missions. One such example is the 2011 military intervention in Libya, conducted by the NATO block. The military intervention in Libya was a response to humanitarian crimes committed by Libya’s then head-of-state, Muammar al-Gaddafi, in the Libyan Civil War. The United Nations first passed a resolution establishing a no-fly zone over Libya and also condemned al-Gaddafi’s actions but then a multilateral coalition comprised of several NATO countries launched an air offensive against Libya aimed at protecting civilians,
enforcing the no-fly zone, and policing the arms embargo on Libya. The coalition’s efforts in Libya allowed the rebel opposition to make headway against al-Gaddafi, eventually capturing and assassinating him. Many in the international community believe that this is a successful model of humanitarian intervention because it was a multilateral effort, it was efficient, and it protected the lives of tens of thousands of civilians.\textsuperscript{53}

These events are a few examples of the critical humanitarian aid and intervention crises that our world faces. Thus, the DISEC will need to find a way to appropriately define when it is and is not appropriate to intervene within a sovereign nation.

### Possible Solutions to the Problem

While there are many potential solutions to the issue of humanitarian intervention, all of them require either reworking the definition of national sovereignty or they require that national sovereignty be breached. In terms of one potential new definition of sovereignty, sovereignty based on Lockean principles is derived by rulers from the consent of the people. If the rights of the people are breached, then the ruling party no longer has sovereignty and thus humanitarian intervention would not constitute a breach in sovereignty. However, this definition, while readily accepted by some states, will be steadfastly opposed by others.

\textsuperscript{4} http://www.thedailybeast.com/articles/2014/11/13/yemen-s-a-model-alright-for-disaster.html

\textsuperscript{5} http://www.foreignaffairs.com/articles/137073/ivo-h-daalder-and-james-g-stavridis/natos-victory-in-libya
There are multiple mechanisms to realize the responsibility to protect doctrine. One mechanism would be for regional and sub-regional groups to develop internal protection and intervention protocols aimed at maintaining stability in a particular region. Via partnerships with the UN, such regional organizations could receive UN backing when exercising the responsibility to protect. Similarly, multilateral decision making regarding humanitarian intervention at different levels of the UN reinforces the political and humanitarian legitimacy of the responsibility to protect doctrine. That being said, the UN is often a polarizing and cumbersome process that often deals out intervention too late.

Another possible solution exists in allowing the military invasion into sovereign country experiencing a humanitarian crises on the basis that military forces would be used to distribute aid and protect civilians. This however is complicated as many nations would refuse such a protocol and deem it as a violation of sovereignty. By the same token, many militaries have a stronger capacity to distribute aid than NGOs, which are often uncoordinated and underfunded. Militaries can airdrop supplies via drones and helicopters and have the capacity to set up medical centers on the ground. As a result of the intricacies of this topic, DISEC is charged with defining sovereignty, defining the difference between humanitarian aid and intervention, and determining the manner in which humanitarian aid must be carried through.

Bloc Positions

Authoritarian countries:
Many large, unipolar states steadfastly oppose humanitarian intervention on grounds of national sovereignty. These nations believe that it is the right of a state to exercise complete authority over its internal affairs— and that no external forces should be allowed to intervene. Nations in this bloc may or may not have their own histories of human rights abuses which they want to cover up or prevent international action against. Nations in this bloc include China, North Korea, Syria, and Russia. However, taking into account Russia’s recent seizure of Crimea, Russia ostensibly supports intervention on the grounds of protecting ethnic heritage.

**NATO & EU Countries**

On the other hand, many NATO and EU member states are more often inclined to humanitarian intervention. Nations in this bloc are usually Western, highly developed countries which have proven their willingness to engage in humanitarian intervention again and again. Although these nations claim that their humanitarian intervention is benevolent and purely unbiased, there are often ulterior political and economic motives at play. NATO humanitarian intervention can be seen by the 2011 intervention in Libya and recent bombings of ISIL locations. Nations in this bloc obviously consist of the key members of these two organizations.

**Developing and Underdeveloped nations:**

Many of the world’s developing and underdeveloped nations are politically unstable and contain non-state political and military actors that threaten the safety of the state. This instability can
result in humanitarian crises that are outside of the government’s control. Thus, in many cases these nations seek efficient humanitarian intervention carried out by stronger states. However, these nations also fear for their sovereignty and do not want an intervention carried out within their borders if they do not deem the situation as dangerous.

Questions to consider

1. Is the notion of Westphalian sovereignty still applicable today? If not, does the definition of national sovereignty need to be reworked?

2. Who should carry out humanitarian intervention?

3. What criteria justify humanitarian intervention? What constitutes an international threat to peace or security?

4. What procedures should be put in place for carrying out effective humanitarian intervention plans?

5. What measures should be taken to ensure that the results of humanitarian intervention are long lasting?

Works Cited


