# UCBMUN XXI

# DISEC:
# The First Committee of the Secretary-General

Head Chair: Mounika Yepuri

# Table of Contents

**Chair Welcome Letter**

My name is Mounika Yepuri, and I am excited to serve as your head chair for the first committee of the General Assembly, the Disarmament and International Security (DISEC) committee for UCBMUN XXI. If you ask me where I am from, you will see me squirm around while I try to explain that I was born in Hyderabad, India, raised in Pittsburgh, and graduated high school back in Hyderabad. I am a sophomore pursuing a double major in Political Science and Economics. My interest for International Relations and debate cultivated from my first Model UN experience in ninth grade, and there has been no looking back since! This will be my second year on the dais for UCBMUN (I vice-chaired the SPECPOL committee for UCBMUN XX). Aside from Model UN, you can catch me curled up with a good mystery novel or at the closest ice cream parlor. I am also a huge Steelers fan, courtesy of growing up in Pittsburgh.

The two topics that have been selected for this committee are very real and demanding issues in today’s world. I believe that these topics allow for high quality debate and will require research on both the origins of the conflicts and the frequently updated current situation. Although I do not expect the committee to cease the civil war or prevent the spread of cyber warfare all in the span of three days, I do look forward to seeing all the innovative solutions and diplomacy that delegates have to exhibit over the course of the conference.

Please feel free to contact me if you have any questions regarding the committee, rules ofprocedure or the background guide. I look forward to seeing you all in the spring!

Best,
Mounika Yepuri

## Topic A: International Intervention in Civil War

### Background Information

Some sources state that the earliest conceptions of human rights started during the Enlightenment Age. During this period, the idea of liberty and equality were expressed in both the United States Declaration of Independence in 1776 and the French Declaration of the Rights of Man and of the Citizen in 1789. Despite these rules being codified by these institutions, the concept of equality was still not instilled in these scenarios, or at least the standards of equality that we hold to present day. It was not till the end of World War II that the world collectively agreed that there was a need for a system that states were accountable to. During the World War II, most of the atrocious crimes occurred courtesy of the great significance given to national sovereignty. This norm allowed Nazi Germany to commit heinous crimes that did not allow or encourage other states to intervene until a majority of the damage already happened. When the Allies claimed victory, they decided to create an international body that would focus on providing safety to the citizens of each state, and a body that would ensure national sovereignty would not trump the dignity of a human being. With this ideology, states came together to form the United Nations, and the permanent five member states of the Security Council – the USA, UK, Russian Federation, China, and France - reflected the interests and power dynamics of the international community. In 1948 the Universal Declaration Human Rights came into picture as a common standard of human rights that should be sustained by every state. It is important to remember that these human rights were codified with the mindset that these were the basic and minimum rights that states were responsible for providing, and that a few key players in world politics who set the floor for human rights wrote them. This will important to keep in mind when understanding how third party intervention is accepted or affects major conflicts within a state's sovereign borders.

*Definition and Legal Technicalities of Intervention*

International intervention has been a heavily debated topic, and most of the disagreements lie in the ambiguous definition and limitations of what is justifiable intervention. To understand some aspects of what prompts a state to intervene and justify it, it is important to recognize the prominence of understanding the term sovereignty and to what degree it affects geopolitics. The term was first notably used by Jean Bodin where he stated that, "Sovereignty is the supreme power of the State over citizens and subjects unrestrained by law." Although this idea has changed, some of the foundational philosophies of sovereignty have remained in our present international law literature. The Charter of the United Nations specifically states the prohibition of the organization and its members from intervening in domestic matters of a state; this can be specifically seen in Article 2 Clause 7. This clause can be summarized as a rule that a third-party or member state cannot intervene in any matters of a state to protect its sovereignty, unless it conflicts enforcing principle stated in Chapter VII of the charter. Chapter VII of the charter in summary allows the Security Council to take measures when it deems it necessary for member states to intervene in matters that are serious issues. It is interesting to note the last article in this chapter, Aritcle 51 which states: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security." Although this might seem ambiguous and conflicting with Article 2 Clause 7, it reflects the idea that measures that are necessary to maintain international peace and security are changing depending on the time and place of the situation. A common reason for intervention or the arguments that have been presented to the international community have centered on humanitarian issues. The conflict lies within the idea of how each state classifies basic human rights or what are major concerns and violations of the intentions of the UN Charter.

### *Human Rights Paradigm*

The rights paradigm follows the notion that individuals are the rights-holders, and these rights-holders have access to certain freedoms and liberties at birth that are considered as human rights.  Since the "universal" human rights that are accepted by many nations are only considered the minimum rights, there are "high-priority goals" that are aimed at raising the standards of living and entertaining the constantly changing norms and significance given to new socio-economic issues that is highlighted by each new generation. Consequently to ensure that these rights are maintained and can be checked upon, there exists the addressee who provides or protects the rights of the rights-holder. The addressee is usually referred to as the government or the institution that is responsible for the well being of the citizen. These are the individuals or organizations that are observed to ensure that human rights are maintained as well as a higher authority for rights-holders to hold confidence that their human dignity is being upheld. There are also the backup addresses, which consist of the international community. When the addressee, usually a state government, cannot maintain basic human rights that is universally accepted, the international community is morally and sometimes legally required to step up and sustain the rights of these individuals. We can see this idea codified in Chapter VII as discussed. Human Rights can also be seen as two categories: Moral (Natural) Rights or Legal (Positive) Rights. Examples of moral rights can stem from religious beliefs, ethical systems, UN declarations, and even the UDHR; whereas legal rights are usually seen in constitutions, statutes, and judicial case laws.  Many parties argue how moral principles can be seen as universal human rights when moral systems vary from state to state, community to community and individual to individual.  Most of these moral rights under the Universal documentation are common ideas that are accepted in most cultures and moral systems such as thou shalt not kill, thou shalt not commit adultery, and thou shalt not steal. In other scenarios there are justified moral rights, which are principles that can be justified in treating universally such as everyone is entitled to enough food to sustain them and decent shelter. Political Science author Jack Donnelly makes an interesting argument for the rights paradigm stating that despite being of Western origin the Rights Paradigm is applicable across the world as one of the best approach to realizing human dignity because it is an approach that is suited for the 21st century and fluctuating standards.  The rights paradigm mainly focuses on three factors: the rights holder, the addressee, and the rights themselves, which are all again in the limelight and compose the UN Declaration of Human Rights.

*UN Declaration of Human Rights*

Adopted by the United Nations General Assembly on December 10, 1948, the United Nations Declaration of Human Rights is a document consisting of thirty articles, which have been explained about, in other international treaties and agreements. The document contains a set of norms that is believed to dictate basic human rights that every citizen is to share as their birthright. However it is important to note that these ideas are not shared universally despite the namesake. The Arab Charter on Human Rights, which was adopted by the Council of the League of Arab States, has many articles coinciding with the UN Charter, the Universal Declaration of Human Rights, the International Covenants on Human Rights, and the Cairo Declaration on Human Rights in Islam. Although these documents share fundamental concepts that humans are special and deserve certain specific access to certain objects and abilities, differences can be recognized in aspects of customary law and religious ideologies. This can be seen when the document was first introduced and many Muslim-majority countries signed onto the document; however, certain countries like Saudi Arabia where the head of the state has to comply with Shari'a Law and the Qur'an arguing that it went against Islamic beliefs and traditions. These states criticized the UDHR for being western ideals that were being imposed on non-western states and for not respecting the cultural values under this Islamic rule. This brings up the question whether expecting other nations to share the same values as those who had the most power at the end of World War II is justified, or if non-Western nations should view human rights as a humane norm rather than Western norms?

**Case Studies**

To fully understand the difficulty of all that encompasses international intervention in civil war, it is important to look into the history of this topic and the various case studies throughout time that are related to this topic. These case studies have several similarities and differences that should be highlighted when comprehending what has been and what has not been efficient in previous years. With this being said, it is crucial to account for the differences in scenarios and contextual information that makes each case study and in general civil war unique.

*Somali Civil War*

Rebels captured the capital of Somalia, Mogadishu, in 1991, which forced the dictator of 21 years to flee.[1] The state was left for two warring clans to fight, which ensued conflict, which resulted in the death of thousands of Somali lives. There were further civilian casualties as the conflict went on due to the civil war which gave way to starvation and disease. Images and accounts of these depressing stories were circulated across the world, which led to the immediate transport of American troops and resources to Somalia; however, this brought conflict between the rebels and American troops, 18 of these troops who lost their lives when helicopters were shot down by the Somali rebels. The US almost immediately retreated from the area leaving Somalia to fend for them again.

Simultaneously the UN tried staging intervention as well, more widely known with UNOSOM I, UNITAF, and UNOSOM II. United Nations Operation in Somalia I was engaged in Somali politics from 1991 when the first civil war first began. This mission was extremely ineffective; despite having a ceasefire in place, the war continued and relief operations were at great risk. This forced the UN to abandon their mission. Then came the Unified Task Force which was a collaboration of the UN and USA to

[1] http://jor705.wixsite.com/somalicivilwar/timeline

curb the war. However, peacekeepers and relief operations were once again dangerously targeted and these operations could not gain the trust of the civilian population in Somalia which made all their efforts ineffective. Following the dissolution of UNITAF, UNOSOM II was sent to replace the task force.

UNOSOM II's main purpose was to not change the political climate of Somalia, but to help with nation building, which included disarmament, establishing legislative institutions, and restoring infrastructure. When investigating a depot belonging to a war-load, Mohamed Farrah Aidid who was vying for the presidential position, Pakistani representatives arrived in Somalia to complete their investigation. However, this angered the Somali protestors who in turn killed many of the Pakistani officials. This led to the UNSC allowing all necessary measures to be taken against the rebelling forces, which broke out war again and led to more civilian and troopers' lives. This further severed the relationship between the troops and peacekeepers and the Somali population. With the Battle of Mogadishu, UNOSOM II was ceased with the immediate retreat of American soldiers after the mentioned loss of 18 soldiers and their bodies being dragged across the land by the rebels. Somalia was later declared a failed state and the international community's intervention in this civil war was seen as a large failure in its purpose and was discredited for the numerous loss of lives that resulted as a consequence of the war because of the preemptive and consistent international action.

*The Rwandan Genocide*

Approximately 800,000 Rwandan citizens were killed in the span of 100 days in 1994 with most of the targeted victims being Tutsis and perpetrators being the Hutus. Rwanda has always witnessed an unstable and violent relationship with the Tutsis and Hutus, but this conflict was at a much larger scale and the blood bath increased at an exponential rate. Shooting down of the plane carrying President Juvenal Habyarimana, who died from the crash, triggered this genocide. He identified himself as Hutu and this aroused conflict between the Hutus and Tutsis with each ethnic group accusing the other for the assassination. Although there was no concrete evidence of the true identity of the perpetrators, violence escalated quickly, even more than the normal violence between the two ethnic groups.

In fear of repeating the same history of intervention in Somalia, many states did not step in to help the conflict. The US administration admitted that the country did not too much to help ease the genocide or curb the conflict of the civil war. It was also seen that states such as the US and the UN were hesitant in sending peacekeepers and actually withdrew some of them due to their previous experience in Somalia.[2] Moreover, the international community is bound by the Geneva Conventions to intervene when a conflict is termed as genocide, which made several nations hesitant to even acknowledge the reality of the situation.

Belgium was a colonial power stationed in Rwanda and had deep ties with them even after decolonization especially with their efforts with the United Nations Assistance Mission for Rwanda (UNAMIR).[3] Although the state warned the international community that it was necessary to strengthen UNAMIR, nothing was done to which Belgium was hit a great loss when Rwandan Prime Minister and her husband were assassinated along with Belgian soldiers. They essentially retreated from their efforts with Rwanda and UNAMIR, which resulted in further chaos in Rwanda. This spiraled out of control and Rwanda felt the consequences.

Simultaneously Canada was also making efforts, with the limited information that they received, to curb the magnitude of this conflict and enforce the sentiments of the Arusha Accords; however, they could not be fully effective due to the halfhearted information they received. Canada did, however, in the aftermath establish the International Convention on the Prevention and Punishment of the Crime on Genocide.

Most nations including the United Nations Security Council admitted that their inability to provide adequate and timely reinforcements worsened the situation to the point that was unimaginable to the international community, which is almost the opposite of the case of Somalia.

The dais would like to point out that though it is clear this was a genocide, this was also a civil war and in this case there was no clear boundary at what point civil war and genocide were distinguished, but it resulted in the same result where nothing was done to protect the citizens and resources by the international community.

*Syrian Civil War*

The Syrian Civil war is a conflict that arose from the mistreatment of civilians by the al-Assad family. Hafez al-Assad ruled from 1970-2000 and following his death, his son Bashar, took up his position from 2000 to present day. It is suspected the protests first broke out in Daraa in March 2011 after a group of children and teenagers were arrested for making political graffiti. Many

[2] Powers, “Bystanders to Genocide”
[3] Valentino, “The True Costs of Humanitarian Intervention”

were killed when the security forces of al-Assad cracked down on these protests and rebellion acts.[4] To address the political unrest in the country, the state promises several changes to the government to appease the citizens, but within a week, Bashar al-Assad addresses the nation acknowledging that he does not plan on keeping this promise, and the state of emergency remains intact.

The international community, such as the United States, reacted by imposing sanctions on Bashar and some of his associates. The US furthers its role by establishing economic sanctions on Syria as a whole, and is quickly joined by the European Union to prevent further damage to the citizens and violations of fundamental human right norms. Within a couple of months, the emergency state was repealed due to number of decrees that were instated. On the other side, the Russian Federation and the Republic of China veto a resolution that would allow the international community to immediately intervene and stop the Assad administration. The next organization to join in the condemning of the Assad regime is the Arab League imposes economic sanctions on Syria as well as suspends their membership to the organization. In March 2012, the Syrian government agrees to UN special envoy,

[4] http://www.cnn.com/2013/08/27/world/meast/syria-civil-war-ast-facts/

Kofi Annan's proposal to establish a ceasefire and provide Syrian citizens with humanitarian aid, release detainees, and establish a forum to discuss both sides of the conflict. After several attempts at negotiating peace and establishing dialogue between the several parties participating in this conflict, we arrive at 2016 where there have been several losses of lives and damage including the UN halting its operations in Syria due to the severe nature of the state with four different main factions of fighting groups including: Kurdish forces, other opposition, ISIS, and the Assad Regime.

The Rebels

There have been several groups composed of militants, exiled dissidents, activists, and political groups that are against the Ba'athist government, but with vast ideological differences.[5] The National Coalition for Syrian Revolutionary and Opposition Forces was first formed in November 2012 to gain international recognition as the Syrian Arab Republic's sole representative. This was created as a response to the complaints of the ineffectiveness of Syrian National Council. This coalition also had the support of the rebel Supreme Military Council of the Free Syrian Army. They were successful in gaining this recognition, first by the Gulf Co-operation Council and then by France, United Kingdom, European Union, and the US. However, they were unable to cope with alleged international pressures and stepped down. Moreover, it was not able to address Human Rights violations due to lack of funding and conflicts in different standards and norms of human rights with the international community. This information shows the inability for any group to establish a legitimate government against the Assad government. Although the recognized government has committed several heinous acts, it is important to remember that the rebels, including ISIS and several other revolutionary groups have equally done harm to this torn state. Armed groups have carried out destructive attacks in the Aleppo City causing the loss of several residents, with many times having a loss of more children than any other demographic category. Therefore, when thinking about this issue, it is important to realize that there is no clear solution to this issue, rather focusing on the least damaging solution possible.

There was a temporary ceasefire that collapsed quickly after it was established, but there has been speculation that more ceasefire attempts are on the way. However, the large number of Syrian refugees and the inability of the entire international community to shelter these

[5] http://www.bbc.com/news/world-middle-east-15798218

refugees has become a serious problem. There is also the issue of Syrian resources and institutions being damaged at an alarming rate. Most of the international intervention so far has not been efficient enough to have any hope of the conflict ending soon[6]

**Questions to Consider:**

1. International intervention is currently justified in cases of humanitarian aid. Should it be justified in other cases? If so, which cases can justify intervention?
2. What is legitimate intervention? Define what is legitimate and sanctions? At what point does it become a proxy war?
3. Should international intervention be justified when legal or positive rights are violated, or is international intervention only justified when moral rights are violated?
4. To what extent do documents such as the Universal Declaration of Human Rights touch upon the universality of rights and human dignity?
5. What lessons can be taken from previous case studies when implementing effective intervention?
6. How does the current arrangement of the Security Council, the organ of the United Nations that can sanction international intervention, affect the justification of intervention?

[6] https://petapixel.com/assets/uploads/2016/08/1534719_770900156314367_7626115611761532406_o.jpg

## Topic B: Cyber Warfare

### Statement of the Issue

Cyber warfare has become increasingly prominent in the list of threats to the international community due to the ever-increasing global dependence on technology. From controlling your household devices to handling all financial and sensitive information, technology has found its place as an integral part in most households. Although this has added to the convenience of each individual, it has also increased the threat of hacking, stolen identities, and other features. Spanning out of the domestic realm, globally there has been recently been many large-scale cyber attacks on member states as well. These not only affect the Governmental realm, but also the civilian realm such as attacks to the electrical power grids and components of the tertiary sector.

“Cyber War” has been commonly coined as the actions made by nation states against other nation states’ computers and networks to disrupt or damage the purposes of these technological assets. [7] However it is important to note that not only other nation states, but also non-state actors can make cyber attacks. Moreover, many times the definition of war penned down by Carl von Clausewitz says, ‘War is thus an act of force to compel our enemy to do our will.’[8] Similar in most political and international scenarios, the definition of cyber warfare has an air of

[7] Clarke, Richard A. *Cyber War*, HarperCollins (2010)

[8] The Third World? In the Cyberspace. Cyber Warfare in the Middle East.

ambiguity and openness to interpretation. As an effort to bridge this gap, the North Atlantic Treaty Organization had a meeting to discuss the emerging threat of cyber warfare. However, it was concluded that, “There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organisations, despite prevalence in mainstream media and Mohamed Farrah Aidid in national and international organisational statements.”[9] Instead they established what nation states interpreted in regards to each cyber term. However varying interpretations are only of member states that are party to NATO, which constitutes a very small portion of all of the member states. This exhibits the large gap when understanding this new realm of warfare from state to state. This can also contribute to the lack of adequate regulations and procedures to address cyber warfare.

From espionage to power grid attacks, cyber warfare has become a prominent issue without enough collective international action against this emerging and very powerful weapon. The further struggle about cyber attacks is that their impact can go unnoticed for long periods of times. Drone strikes are immediately visible; however, it takes an extensive amount of time longer to feel the impact or identify a hacker stealing important information that can threaten the security and stability of a state. This also cries as a large breach of sovereignty as foreign sources interfere among domestic issues that can be handled by the governing state.

**Background Information**

To gain a better perspective of how cyber attacks occur and their effect on respective states’ sovereignty, it is important to learn about how this technology came to be a potent weapon for war.

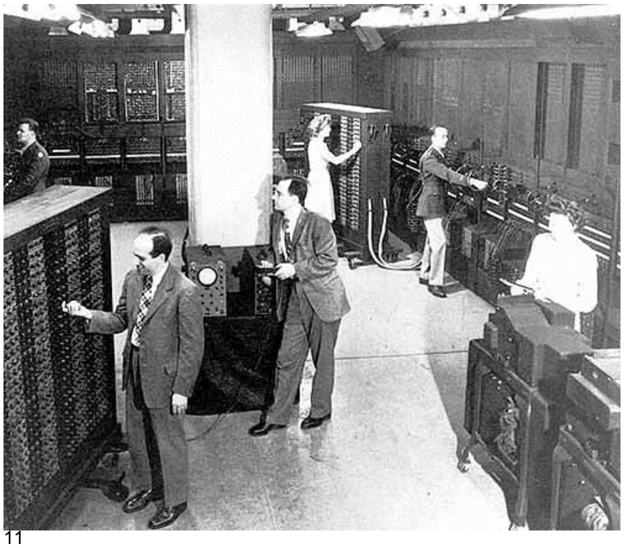
*The Beginning of an Era: History of Computers and Internet*

Just as most inventions, the computer was born out of the necessity for a quicker way of crunching and computing statistics and numbers. After much progress from the initial computer-free computing, two professors created a machine what is known to be the grandfather for digital computers. This device, known as the Electronic Numerical Integrator and Calculator, filled up a 20’ by 40’ space with approximately 18000 vacuum tubes.[10] Once again feeding off the innate human characteristic for convenience, progress was made to remove

[9] https://ccdcoe.org/cyber-definitions.html

[10] http://www.livescience.com/20718-computer-history.html

the vacuums and decrease the space and size of this machine.



11

Eventually in 1953 Grace Hopper formed COBOL, the first computer language. In this same year, Thomas Johnson Watson Sr. creates the IBM 701 EDPM as a way for the UN to secure information on the Korean government during the war.[12] A decade later, the world was witness to the first prototype of the modern computer. This was a big step in the technological world because this invention was no longer only purposely for scientists and academicians, but also user friendly for the general population. Soon after the floppy disk and Ethernet were created for the purposes of sharing and receiving information in a more efficient manner.[13]

The first glimpses of the Internet were in the form of Advanced Researched Projects Agency Network (ARPANET), an early packet switching network, which was used for the purpose of being able to use data on different computers that share the same network.[14] It is important to note that the ARPANET was funded by the US government and mainly studied by military scientists and engineers to establish a form of more efficient and safer communication.[15] The boom in technological advances in the late 1900s resulted in modern day telecommunication systems, which allowed both the general population and military to address issues of large lapses in communication. This essentially made it easier and quicker for the military to communicate among each other, but with advances in this technology and the knowledge of this technology, other states and groups began to learn to hack into these systems.

According to NATO's public database, the first instances of Cyber attacks that got worldwide attention was the Morris worm created and executed by Robert Tapan Morris. In an experiment to gauge how large the Internet was, he essential set out this virus to slow down computers to the

[11] http://encyclopedia2.thefreedictionary.com/Electronic+Numerical+Integrator+Analyzer+and+Computer

[12] IBID

[13] IBID

[14] Internationalizing the Internet: The Co-evolution of Influence and Technology

[15] IBID

extent of being completely useless. [16] Despite this being one of the earlier major attacks, cyber warfare did not surface again as a serious threat and a weapon until the 2000s with the Titan Rain and Estonian cyber attacks.

**Relevant Case Studies**

The Titan Rain, Estonia Cyber Attacks, and Stuxnet case studies should provide a brief introduction to the recent entry of cyber warfare into our modern realm of international conflict. These examples will provide you with information on how these cases developed and emphasize the difficulty of taking international action against these attacks majorly due to the lack of clear legal ramifications to combat and condemn these actions. It is important to note that there is several other cases that are not mentioned involving issues of cyber security, but these case studies only focus on those attacks that affect the governmental facilities.

*Titan Rain*

Shawn Carpenter was your average software employee, who went out of his way to complete a task successfully. That was what he set out to do when his employer, Sandia Corporations, assigned him a special task in the summer of 2003. He realized that some of the attacks one of the parent companies was facing originated from the same group of individuals located in China. He further investigated to come upon the news that these attacks were also affecting the internal networks of the U.S. Army Base, Fort Dix, and etc.[17] Additional study unveiled that other attacks were from a machine in South Korea. After having access to the internal networking of this machine, he realized that there were hundreds of documents of extreme importance and top security clearance. This caused a stir within the U.S. government as many of their top national secrets and strategies were exposed and compromised. Consequently the U.S. government started directly interacting with Shawn to gather more information and combat the Chinese attacks. These Chinese attacks were codenamed Titan Rain.

Titan Rain put further pressure on the already strained U.S.-China relations, with both countries being perpetually suspicious of each other. A large part of cyber attacks is making sure to not have a paper trail or evidence of the hack or attack. This provides the group or state plausibility to deny the actions, and to neither confirm nor deny responsibility for the attacks.

[16] http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

[17] Surviving Cyberwar

Consequently, states may employ the help of individuals or groups that are independent of the government to perpetuate these attacks, which makes it nearly impossible to pin the blame and consequences on the responsible actors. This case study was just the start of an every increasing dependence on technology for security and strategic defense, such as in the case of the Estonian cyber attacks.

*Estonian Cyber Attacks*

The Estonian Penal Code accounts for cyber attacks profusely; the country has included consequences for any cyber related misconduct under Damage to Property with more specific subdivisions of Fraud, Unlawful Use and Petty Offences against Property. It also has sections under Offenses Against Intellectual Property and Offenses Against State Power, which mainly focus on acts of terrorism.[18] This clearly exhibits how the nation has covered most of the legal fronts to deal with these technological attacks. During these 2007 attacks, Estonia largely placed the blame on the Russian government. The evidence they presented was several of the attacks originating from Russian state computer servers, which the Russian government adamantly denied involvement.[19] Moreover, these attacks allegedly began after the Estonia went ahead with moving a Soviet war memorial in Tallinn out of the city, a decision that the Kremlin did not approve. The NATO got heavily involved to alleviate the incessant attacks the country was facing and went on to say, "In the 21st century it's not just about tanks and artillery."[20] The attack hit Estonia harder than most nations because in 2007 it was one of the handpicked governments that had most of their government related activities were based online. Some of these activities include banking, e-government, and even electing their officials on online mediums.

It was claimed that these attacks were a denial-of service attack. Denial- of Service Attack or DoS is defined as:

> **In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services**

[18] Estonian Penal Code (translated to English)
[19] http://news.bbc.co.uk/2/hi/europe/6665145.stm
[20] IBID

**that rely on the affected computer.**[21]

One of the most common ways of a DoS attack is to overload a servers network, effectively slowing and shutting down the server's ability to process requests from users who are trying to access a certain site. When one types in an URL, they send a request to the servers to access the page; however, if these attackers flood the requests, then the server cannot process regular requests and inadvertently denying accessibility to the user.[22] Suppose if most of your government is run on websites such as these, and suddenly all these servers are unable to process requests of citizens and residents of Estonia; in some scenarios, it was even difficult for government officials to read emails or access the bank.[23] This essentially brings the nation to a halt in government affairs and, as seen in this example, a dangerous attack.

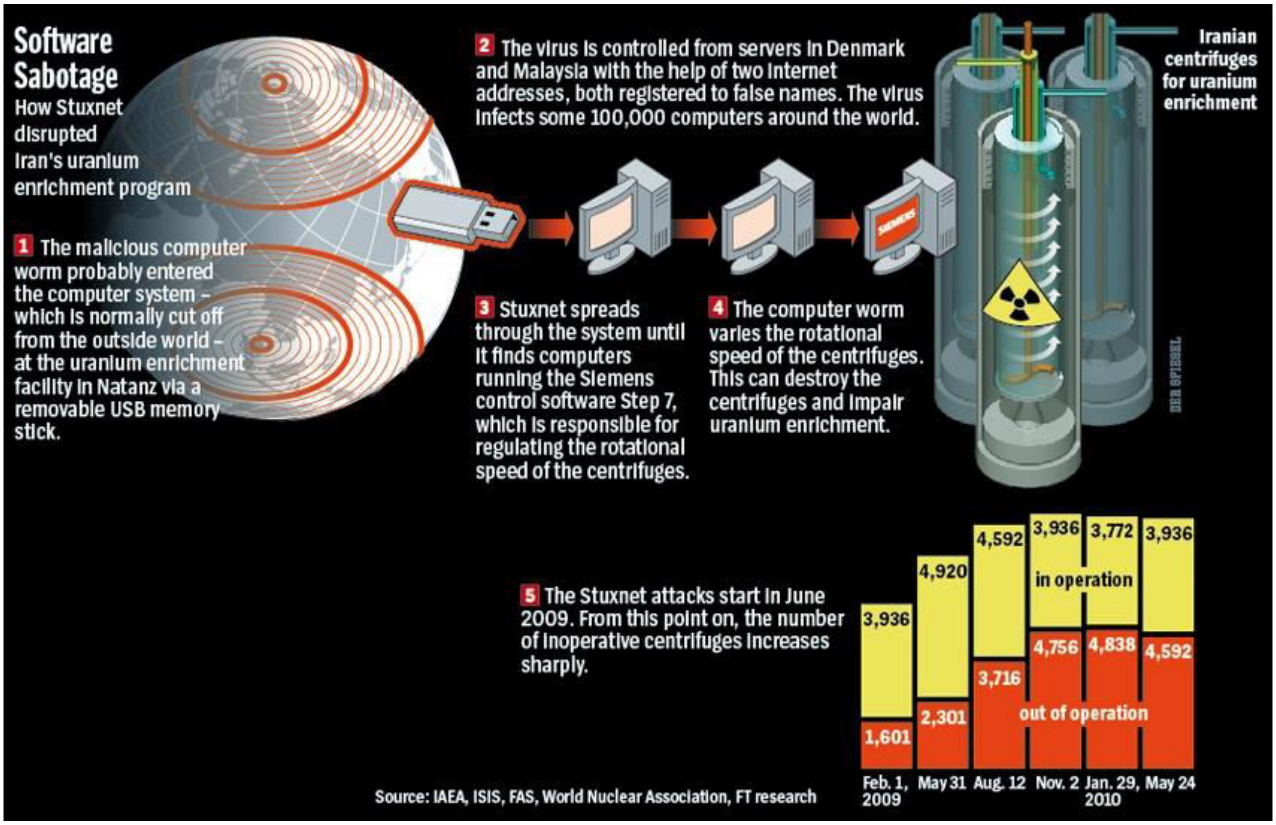
The political motive behind this was moving the Bronze Soldier. Estonia viewed this as a representation of Soviet occupation; moreover, many nationals wanted moved or completely destroyed since the fall of the Soviet Union. This move not only caused a stir in the cyber world, but also on home ground, Estonia witnessed one of its worst periods of unrest. Ethnic Russians that resided in the country let out two days of extremely violent riots, which proved fatal for one man and injuring almost 153 people.[24]

After two weeks of the cyber attacks, Estonia was finally freed from these cyber assaults. Although there was high suspicion on the Russian government and most convinced it was indeed Russia, there was no concrete evidence of this occurring and even the involvement of the state or just individuals using the state's network. One individual admitted his guilt and was convicted, but that was the most that could be done. At this time, Estonia labeled these attacks similar to terrorist attacks and requested NATO to combat these attacks; however, there was never a cyber attack like this and the alliance was not ready to take on this war. There were too many lapses in technological knowledge and equipment to confidently combat the attacks, so the Estonian case study was an alarm for most governments and defense systems to start focusing on cyber technology as a means of warfare, the next generation of combative resources.[25]

[21] https://www.us-cert.gov/ncas/tips/ST04-015
[22] IBID
[23] http://news.bbc.co.uk/2/hi/europe/6665145.stm
[24] http://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/
[25] http://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/

*Stuxnet*

Stuxnet was the name given to the computer worm that significantly damaged the Iranian nuclear program. Interestingly, the worm's software was designed to self-erase in 2012, making it difficult to create further damage and hiding the origins of the worm, which have still been unclear since no organization to this date has taken responsibility for the attack; however, the US and Israel are highly suspected of working together to co-create this cyber weapon.


Software Sabotage
How Stuxnet disrupted Iran's uranium enrichment program
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.
2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.
3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.
SIEMENS
Iranian centrifuges for uranium enrichment
DER SPIEGEL
5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.
3,936
1,601
4,920
2,301
4,592
3,716
3,936
4,756
3,772
4,838
3,936
4,592
in operation
out of operation
Feb. 1, 2009
May 31
Aug. 12
Nov. 2
Jan. 29, 2010
May 24
Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

The worm was first discovered due to the significant loss of centrifuges in the Iranian nuclear program. The nuclear facilities in Iran are located outside of Natanz; the centrifuges located in these facilities have systems that have a lifespan of 10 years.[26] Initial reports by the IAEA showed no activities or damage that would arouse suspicion of foul play or cyber attack; however, after further analysis of the statistics behind the loss of centrifuges, the organization realized that Iran was losing their centrifuges at an exponential rate, which was abnormal for the technology being used. It is important to note that it is

[26] Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon

not under the IAEA mandate to investigate failed equipment or question why Iran had to replace their centrifuge machines. Therefore the IAEA could not uncover the truth that someone or some organization released a destructive virus onto their computers. It was revealed to be an extremely complex software that later was coined as the first digital weapon.[27] Iran has adamantly denied any intentions of using nuclear facilities for anything other than peaceful purposes, but the state has failed to comply with international regulations on nuclear proliferation several times. As a response to Stuxnet, Iran expanded its cyber facilities and capabilities to avoid similar situations in the future. Just as the whereabouts of the origins of Stuxnet and the perpetuators behind hit, there has been a lot of speculation of Iran's new and improved cyber program attacking Western nations to avenge Stuxnet. Without concrete evidence and more regulations on how to attempt to combat cyber security breaches, the international community is in grave danger of succumbing to a large-scale cyber war, especially with many nations equipped with the latest technologies and research capabilities and the rise of tensions in several geo-political regions.

## International Efforts to Combat Cyber Attacks and Definitions

In this section, we will discuss some of the attempts made by the international community to combat cyber warfare. One of the first notable propositions was the resolution put forth by the Russian Federation's delegation to the DISEC in 1999, which was adopted without a vote, on the "Developments in the field of information and telecommunications in the context of international security."[28] This brief document was a transition to what would become a pressing issue almost a decade later and what we are dealing with today in modern society. The document can largely be summarized to request nations to not allow advances in cyber technology to conflict with the main purpose of stability within the international security realm, develop the member states' understanding of this concept of cyber technology and its role in the international community, and transparency by submitting reports to the General Assembly. [29]

### *Groups of Governmental Experts*

Post the adoption of Resolution 53/70 there was the creation of four additional Groups of Governmental Experts

[27] IBID

[28] http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70

[29] IBID

(GGEs) that were responsible in analyzing all threats related to the cyber-sphere and propose solutions to tackle these issues.[30] The first group was established in 2004 but all of the members could not agree on two main policy issues. The first difference was the inability to have consensus on how much to emphasize the emergence of ICTs as a threat to national securities and military affairs, especially on the attention that should be allocated to threats due to "State exploitation of ICTs for military and national security purposes."[31] Following this attempt, a second group of GGEs were created which was able to produce a successful report, which highlighted upon encouraging discussion among member states on matters regarding norms of ICTs, their role in conflict, building their foundation in less-developed countries, and exchange of ICT research and development.[32] An important development was made with the GGE 2012/2013 where a report was established that agreed that international norms and regulations stated by the UN Charter were applicable to the cyber sphere including aspects of upholding sovereignty, human rights and fundamental freedoms, and the UN acting as a mediator among member states when conflict arises or as an advisor. [33] It is important to note that, although, there has been encouragement in dialogues of cyber security, it does not completely solidify the role of the UN in cyber-security affairs, especially in those scenarios, which cannot be applicable to inspection under international law that was envisioned for more traditional forms of warfare.

*Sovereignty*

If the server for a host site or data storing service is located outside a country, the data travels to the server's of the host country. At this point, the government of this country can obtain or view this information since the data is within its country's borders; however, no state would be willing to give permission to other states to view their confidential data. At what point is sovereignty violated when technically data is owned by one state but it is physically within the borders of another? It is important for delegates to explore the relationship between ownership of cyber data and sovereignty of that state. Furthermore, under Customary International Law, self-defense in cyber attacks should based on the principle of *Jus in bello,* which means the attacked nation has the right to defend

[30] https://www.un.org/disarmament/topics/informationsecurity/

[31] https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

[32] https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

[33] IBID

themselves based on necessity and proportionality.

**Questions to Consider for Resolution Writing:**

1. How should the United Nations and the international community develop the definition of Cyber War? How can the UN account for regulations and clauses that were created for more traditional forms of warfare to cyber warfare?
2. How can the UN build capacity to combat cyber warfare and take preventive steps to impede high-level threats to international security? How can the international community curb the excessive usage of ICT for espionage strategies?
3. How can existing laws and norms such as the UN Charter be applied to cyber warfare? How can the international community update these laws to take into account the increasing usage of ICTs in modern warfare? How is proportionality measured in cyber war?
4. Should countries with cyber technology capacities support and develop countries that are under-developed in the cyber-sphere?
5. What laws can be in place to ensure the national security of a country when under cyber-attack from international organizations and agencies?
6. How does the UN further ensure that member states comply with the norms of cyber security and do not use proxies for using cyber attack against other nations?

**Note From the Dais:**

Parts of Topic B went into technicalities and contextual information to help delegates have a better understanding of the complexity of this topic; however, we would like to see debate be more central to what effects cyber warfare has on International Law, regulations, norms, and foreign relations and how to govern offenses made in this comparatively newer sphere in our world today.