ZuMUN
THE ZURICH CONFERENCE

DISEC

Study Guide for Zurich Model United Nations

Written by Hafiza and Ioannis

April 28 – May 1, 2022

Zurich, Switzerland

ZuMUN
THE ZURICH CONFERENCE

Table of Contents

Letter from the Chairspersons

Dearest Delegates,

Welcome to the Zurich Model UN Disarmament & International Security (DISEC) Committee! We are honoured to chair this committee this year.

As chairs we both look forward to serving you in the Disarmament and International Security (DISEC) committee in the upcoming ZuMUN 2022. Both of us hope this study guide provides you with a good starting point for your research and a clear picture of what we are expecting to see in the resolutions that will be debated.

We strongly advise you to read this document thoroughly to define the policy of your country, so you can prepare a well-rounded and effective resolution on the topic.

That being said, we wish you best of luck and trust that we will have fruitful debates in the Committee.

For any question you may have, do not hesitate to contact us via email at: hafizasamath@gmail.com / giannosvelonias@gmail.com

Best Regards,

Hafiza & Ioannis

Introduction to the Committee

DISEC Committee constitutes the first committee of the General Assembly (GA), whose fundamental concerns are obviously the disarmament, the global challenges as well as menaces of peace affecting the international stability.

As a result, the main objective is the finding of solutions regarding security issues in an international frame. The committee is concerned with issues of worldwide relevance such as security and demilitarisation in all nations and areas, as well as ensuring that individuals across the world are safe.

This year, DISEC will be entrusted with answering ***two crucial issues*** of thematic importance to the committee. These issues should be examined in order to reimagine the globe in the current period and how the international community can work together to protect state sovereignty and self-determination. As you analyse and debate these issues, keep in mind the ultimate need for multilateral cooperation and a diverse range of viewpoints in order to achieve meaningful resolutions.

Topic A

Overview of Topic A: The Yemen Conflict

Yemen is located in the crossroads of Europe , Asia and Africa. Although geographically located in an incredibly strategic location, this nation is facing the world's worst humanitarian crisis. Yemen's political unrest started in the 60s which catapulted into a big blown up mess as a result of mingling by neighbouring nation(s). *This section will dwell further into the conflict that Yemen faces in different facets. All the different facets will be explained briefly so that it is not overwhelming to the readers.*

As many are aware, Yemen has never left the news at least from the beginning of 2010s. This is when the humanitarian crisis began. Yemen Civil War began in late 2014 , 2022 will witness Yemen's 7th year of this war. Even the COVID19 pandemic failed to put a halt to this war.

Yemen has found its way into conflict since the year 1962 when it's then ruler's demise. As a result of Saudi aggravation, the Civil War between Yemen royal supporters and Yemen republicans broke down. Here marks the start of geopolitical inter-mingling into Yemen. This is because the aforementioned royalists were backed by Saudi Arabia whereas the republicans were backed by Egypt.

Fast forward to the year 2011 when Yemen was heavily on the world news, the crisis further was heightened as a result of internal mismanagement by the ruling party. With the cost of living skyrocketing and grocery prices increasing, many are dying and on the verge of demise.

Political

The root cause of the Yemen conflict is political instability and crisis within. In the year 1948 when their first ruler; Imam Yahya, was assassinated , his son had to fight the feudalists to take over his father. This marks the regular fights to be in power for Yemen to stay an independent, self governing state.

In 1967, British withdrawal from South Yemen sparks power struggle between two Yemens in unifying and finding a common ground. Three decades later in 1990s Yemen was unified as one however internal clash between then leader of Yemen ; Saleh and his Vice birthed a critical situation for Yemen yet again.

In the 90s when Abdullah Salleh took over the leadership position of Yemen, Houssein Al-Houthi and his supporters paraded against him and his corruption antics. Houssein Al-Houthi's movement is called the Houthi movement / Houthi insurgency or "Houthi's" in mass media. In 2011 Salleh eventually gave up his position to his vice which then gave more hope to the Houthis and inter-mingling of international nations into Yemen's political scene.

Economic conflict

Abdullah Salleh and The Houthis conflict has greatly affected Yemen's economy. This goes further to show that disunity of a government affects its people and the betterment of the nation immensely.

The inflow of goods into the country has reduced as the years go by. This hampers sustainability of the nation as basic needs are to be met to live. With inadequate infrastructure as a result of war and monetary influx, even job creation and labour market is almost non-existent. Employment rate in Yemen as of 2020 is only 30%.

Yemen only depends on its rapidly decreasing oil and gas revenues. The COVID-19 pandemic had jolted down the economic wellbeing of the nation tremendously. As all nations around the globe struggle, Yemen had to stay flaccid with its slow recovery in producing its oil and ability to export has plummeted.

Yemen's currency exchange rate has deteriorated greatly, simultaneously diminishing purchasing power.

Social issues

Societal issues cover the humanitarian crisis. With the scarcity of food, struggling to produce and secure employment, and the struggling value of life in Yemen; to live a sustainable life is difficult to say the least.

Health care and educational institutions are struggling to mobilise as a result of economical instability in Yemen. Without education and healthcare an ordinary individual could not live nor survive.

Those that do afford education, health and employment are not paid. This is especially seen within the skilled workers such as doctors, teachers and civil workers. Many then leave the nation, further pushing Yemen into a brain drain society.

Historical Background

Yemen is one of the oldest civilisations on Earth. It became the hub of trade links. When great civilisation emerged, it then resulted in pre-Islamic kingdom taking over. For instance, the Ma'in Kingdom was successful because of frankincense and spice trading.

In the 10th century, the most popular and vast kingdom took over Yemen; Kingdom of Sabaa. Here, Queen Bilqis took over the northern part of Yemen and the far south of Yemen was taken over by the kingdoms of Qataban and Hadhramaut.

However Yemen prospered greatly under the Kingdom of Sabaa. The kingdom of Sabaa's greatness in conquering and prospering Yemen has given Yemen the name of " Happy/ Flourishing Arabia'' or "Arabia Felix'' in Latin.

Slowly but surely, when Egypt was occupied by the Romans, the Red Sea became largely used for trading as such yemen's caravan routes declined quickly resulting in hazy trading and wealth for this nation.

As Yemen struggled to sustain its wealth the kingdom weakened. Now, the Abyssinian Kingdom has taken over Yemen. Also, before the spread of Islam the Sassanids of Persia was able to occupy yemen too.

The concurring of multiple muslim caliphs in the rise of Islam was largely documented and known in the Islamic theology. With the start of Umayyad Dynasty and the end of Abbasid Caliphate taking over Yemen, Yemen then was able to establish its own grassroot Dynasty that was powerful enough to lead its nation alone. However , in the far north Zayydi imamite was slowly gaining power.

In the 16th century Portuguese merchants were regular traders in Egypt and were eyeing Yemen and once even unsuccessfully captured Yemen. Observing this, Egypt took advantage and seized Yemen. Eventually, Ottomans then captured Egypt itself and Yemen as well. Here, Yemen once again prospered economically. Yemen is known as the international coffee port under Ottomans rule.

However , from the 17th -19th century highlands of Yemen was left isolated from the rest of the world, this was when western europe was prospering and influencing the world with technological advancement. **As such, Southern Yemen was easily taken over by the British leaving the Northern part of Yemen to the Ottomans**. Both Ottomans and British then officially drew borders which then became known as north and south yemen.

North Yemen

When World War 1 ended, Ottomans were forced to leave Yemen, as such the Zayydi imamate took over **northern Yemen**. And so, for 4 decades two imams ruled here under an autocratic regime.

The Northern Yemenis from the 1940s witnessed modernisation of the world as they were left far behind in conjunction with the imamite regime and autocratic society. As such, the Free Yemen Movement was born, forcing a long revolution. Eventually, Yemen Arab Republic was established with a series of coup, assasination and failed assasination of the imams.

The 1960s marked a long civil war fueled by differences from within North Yemen itself. This marks the beginning of intermingling of neighbouring nations into North Yemen's political landscape. Here,anti-royalist were supported by Egypt whereas royalists were backed by Saudi Arabia and Jordan. However, eventually the people of North Yemen were given a say to choose their ruler/government.

Regardless, the civil war went on until Saudi Arabia severed ties with the royalist and now had successfully built a good relationship with Northern Yemen. Northern Yemen's President; Abdul Rahman al-Iryani then ended the long brawl between royalists and republicans which eventually led to a draft of a democratic constitution in 1970.

4 years later a coup resulted in the fall of the democratic government , now northern Yemen is ruled by the military. Almost 4 years of the military rule was brutal with two of its chiefs being murdered. In late 70s Abdullah Saleh took over tenureship and went on to lead Northern yemen until both North and south Yemen were united as one country under one ruler.

South Yemen

Aden which is the capital of modern Yemen was then known as **south yemen**. The British were sly enough to protect Southern Yemen from being taken over by the Ottoman back in the 19th century.

The British colony added 6 tiny states closer to Aden and eventually named them *Federation of South Arabia* in 1965. Two years later the British left Aden as a strong nationalist movement was building up. This nationalist movement is known as the "National Liberation Front."

As this is the only party that stood for South Yemen's liberation, it then successfully formed a government and South Yemen was then governed under a marxist ideology. A decade before unification of North and South Yemen, South Yemen was renamed to " People's Democratic Republic of Yemen"

Unification of North and South Yemen

The merging of both south and north Yemen was largely as a result of both leaders of these nations agreeing on economic stances. With the unification, Yemen was called " Republic of Yemen" and they were looking forward to a bright future as neighbouring countries and big foreign nations were assisting them financially.

However in the 90s Iraq taking over Kuwait affected Yemen's economic strength further pushing them into obscurity. The then government of Yemen's treatment towards Saudi Arabia's military presence in their sovereign state sparked a huge unrest in Yemen. This then pushed Yemen further backwards as political and economic unrest gradually catapulted for the entirety of its existence from then on till date.

Key Terms

Crossroads : a term used for when a road/ pathway is intertwined with 3 or more other roads /pathways.

Political unrest : a term used to describe the political situation in a nation that is not stable and often in a limbo of violence and cold fights.

Humanitarian crisis : a popular and widely used terminology to describe a human condition that is in dire need. When a country is facing a humanitarian crisis it means a country is struggling to have its people to live and survive.

Geopolitics : a term used to describe political relations between international regions.

Royalists : a term used to describe a large group of individuals that supports the royals and a monarchy.

Assasination : This term is used to refer to a killing of an extremely important figure, in this context ; a political figure.

Feudalism : A term used to describe the belief started in mediaeval societies in the Western part of Europe. Feudalism is when the bourgeois work for the nobles wherein in return the latter provides working class individuals with safety and land.

Brain drain : a term popularly used to describe skilled individuals leaving their homeland to pursue a career in their academic field.

Ma'in Kingdom : This kingdom belongs to the people of Minaean. They were inhabiting Northern Yemen and practised democracy in the 10th century.

Frankincense : Resin that comes from the Boswellia tree. Yemen, Eritrea and Somalia are the world's biggest supplier of frankincense. Frankincense was first found in Yemen in 10th century when it is seen as the most desirable and envied product which then led to the nation striving because of it.

Kingdom of Sabaa : The kingdom of Sabaa or Sheba ; as what its known in the bible is the most widely successful kingdom in the 8th century , solely because of its capture of modern

day Yemen. This kingdom is widely spoken in the Muslim, Jewish, Christian and Eutopian traditions.

Kingdoms of Qataban : Initially a part of the Kingdom of Sabaa, this kingdom was later replaced by Kingdom of Sabaa and went into obscurity.

Kingdom of Hadhramaut : This kingdom conquered Southern part of Yemen and later by Kingdom of Sabaa

Red Sea : Surrounded by desert in between Egypt and Saudi Arabia, it is the warmest sea in the world. Located in the sea roads of Europe, East Asia and Persian gulf, it has a heavy traffic on the daily.

Abyssinian Kingdom : The kingdom from Ethiopia that was founded in the 13th century and lost its existence in the 20th century.

Sassanids of Persia : Refers to the Sassanian Empire that conquered modern day Iran, Iraq, Egypt, Anatolia and Pakistan.

Caliphs : Known as the leader of a muslim community under the caliphate.

Imamite : An individual who is a part of the Shi'ah sect of Islam

Marxism : An ideology or a doctrine by Karl Max that argues for workers revolution and for communism to overturn capitalism.

Bloc Position

Blocs are separated in conjunction to the power each nations have in terms of economic capabilities and social life balance.

Western countries

Most of western countries are big and incredibly powerful nations who also have stakes in the ongoing crisis in Yemen.

France

According to the France government, it is one of the first few western nations to speak up publicly and to assist Yemen in its humanitarian needs in addition to vehemently supporting the sovereignty of Yemen as a nation. France has concurrently also established a foundation and allocated scholarships for Yemeni children to study in France back in the year 2017. This foundation was a joint effort from Hadramout Establishment for Human Development and the French Ministry for Europe and Foreign Affairs.

However despite the humanitarian efforts, France has also supplied arms and military equipment against Yemen. France is one of the last few countries who have delivered military arms against Yemen.

United States of America

The government of the USA has allocated hundreds of million US dollars for Yemen's humanitarian needs. In the year 2020, USA had allocated $630 million just for Yemen's humanitarian needs. USA also set up an organisation for smooth handling of the humanitarian efforts, this organisation is called U.S. Agency for International Development (USAID). USAID together with the State Department's Bureau of Population, Refugees, and Migration has worked hand in hand to assist Yemenis.

It must be noted when President Biden assumed office a lot of promises were made such as his promise to end the war in Yemen was not fulfilled. Saudi Arabia's persistent bombing of Yemen was backed by the USA in terms of military assistance and diplomacy efforts. The biden government has always been silent with Saudi's air raids of Yemen.

United Kingdom

The United Kingdom in the year 2021 decided to cut off its aid to Yemen. This means the aid from the UK is 50% less than the usual aid. The UK being one of the wealthiest nations was ambushed by various British Non-Governmental Organisations to reverse this decision.

It should further be noted that along with the USA, the UK has sent British troops to help Saudi soldiers. The UK also provides bombs and missiles for Saudi Arabia despite many other western nations such as Austria, Belgium, Germany, Finland, Netherlands, Norway, Sweden and Switzerland backing out from helping Saudi in Yemen.

Arab states of the Persian Gulf

With Saudi Arabia leading the war in Yemen for decades now, many countries in this region are also actively , directly or indirectly involved in the ongoing civil war in Yemen.

Saudi Arabia

Saudi Arabia's government boasts itself as being the single humanitarian donor for Yemen in its 2017 fact sheet published online. Its government emphasised that it has donated more than 2 billion USD for Yemen's development. It has apparently deposited a billion USD into Yemen's central bank.

However, Saudi is the one leading intervention and mingling into Yemen's sovereignty and land for far too long. Recently Saudi led electric cut and carpet bombing on Yemen is rampant and widely reported in the news worldwide. With the help of UK and USA made war weapons,

Saudi had led intervention and bombings in Yemen for years now. Saudi's military arms deals with the UK have actually prolonged war in Yemen.

United Arab Emirates

The UAE ever since the year 2015 has provided 6 Billion US Dollars in humanitarian assistance to Yemen. It has also helped largely in Yemen's medicinal supplies during the COVID-19 pandemic.

However, Canada has provided war weapons and arms to the UAE which has helped in fueling endless war in Yemen for the past year. The United Nations has also reported that the UAE is the main and important party involved in the war crimes committed in Yemen.

Iran

Iran's role in Yemen is largely to back the Houthis . Although Iran has also stepped in to assist Yemen whenever there is a need to in terms of humanitarian efforts.

But it should be noted that Iran's involvement in Yemen is largely to put itself within Shiite community in the Northern part of Yemen. This interest was strong even back in the 1980s. This year, there are vast allegations of Iran smuggling weapons to Houthis which does not sit right with Yemen's officials.

Points a Resolution Must Answer

1. How could member states come together in finding a common ground to attain peace?
2. What is the role of Non-Governmental Organisations in minimising the conflict?
3. Taking into account the ongoing conflict in Yemen and the worsening COVID-19 pandemic situation, how could appropriate steps be taken in achieving and finding a common ground?
4. What would regional and international collaboration look like and how could such collaboration be structured to maintain peace without harming innocent public?
5. What loopholes were there in previous legislations surrounding enabling usage of weapons ? How can DISEC close those loopholes?

Bibliography

"Employment to Population Ratio in Yemen" (Feb 16, 2022) *Fred Economic Data.* Retrieved From: https://fred.stlouisfed.org/series/SLEMPTOTLSPZSYEM

"History of Yemen: Heritage" (n,d) *Yemeni Community Association in Sandwell Limited.* Retrieved From: https://www.yca-sandwell.org.uk/history-of-yemen/

"France Diplomacy" (n.d) *France Government Website.* Retrieved from: https://www.diplomatie.gouv.fr/en/country-files/yemen/

"Ending the War in Yemen should be at the Forefront of Diplomacy for the French Government" (February 5, 2021) *Action Contre La Faim.* Retrieved From: https://www.actioncontrelafaim.org/en/press/ending-the-war-in-yemen-should-be-at-the-forefront-of-french-diplomacy/

"Biden Broken Promise on Yemen" (September 16, 2021) *Brookings.* Retrieved From: https://www.brookings.edu/blog/order-from-chaos/2021/09/16/bidens-broken-promise-on-yemen/

"US Relationship with Yemen" (n,d) *US Department of State.* Retrieved From: https://www.state.gov/u-s-relations-with-yemen/

Merat A. "'The Saudis couldn't do it without us': the UK's true role in Yemen's deadly war" (18 June, 2019) *The Guardian.* Retrieved From: https://www.theguardian.com/world/2019/jun/18/the-saudis-couldnt-do-it-without-us-the-uks-true-role-in-yemens-deadly-war

Humanitarian Aid to the People of Yemen (April, 2017) *Saudi Embassy.* Retrieved From: https://www.saudiembassy.net/sites/default/files/FactSheet_Humanitarian%20Aid%20Yemen%20Fact_April2017.pdf

Topic B

Overview of Topic 2: Cyber-Crime, Terrorism & Security

Since the beginning of the 21st century, technology has shown an increasingly rapid change in our daily lives. One could easily describe the Internet as an “invisible ruler”. Usually, technology in all its forms, including media, devices has played an important role in shaping human interaction and bringing new circumstances with innovative changes. and unknown challenges from every aspect. Therefore, it is clearly understood that technology is a topic of great importance, generating many heated debates regarding positive and negative influence. However, the goal here is to focus on what we can change to make cyberspace a better place for everyone.

A dark side of cyberspace is undoubtedly the subject of cyberattacks and cyberterrorism. A cyber attack is any type of attack attempted over the Internet or any computer network by a cybercriminal, in order to gain illegal access to electronic data stored on a computer or a network. The intent might be to inflict reputational damage or harm to a business or person, or theft of valuable data. Cyber attacks can target individuals, groups, organisations, or governments.’ There are many different forms of cyberattacks, from “simple” phishing to complex “Zero-day exploits,” which can be extremely difficult to prevent.

The purposes of cyber attacks, as we understand them, can actually range from simple bank robberies to cyber terrorism. As time goes by, it is understandable that cyberattacks will become increasingly complex and "sophisticated" even in the extremely near future due to the rapid development of technological progress. Therefore, this research guide should focus on the topic of cyber-crimes and the corresponding information in order to conduct further research related to preventing this type of terrorism and ways to promote cyber security.

Key terms

Network : A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

TCP/IP Protocol : TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network.

Cyberspace : Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyber Threat : A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

Cyber Crime : In general, cybercrime is defined as either a crime involving computing against a digital target or a crime in which a computing system is used to commit criminal offences.'

Virus : Technically, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

Cyberwar : Cyberwar (also called cyberwarfare or cyber warfare) constitutes war, which is conducted in and from computers and the networks connecting them, waged by states or their proxies against other states.

Phishing : The practice of tricking Internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly.

Worm : A worm is a type of malicious software (malware) that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path.

Cyber Terrorism : Cyber-terrorism involves the use of computers and/or related technology with the intention of causing harm or damage, in order to coerce a civilian population and influence policy of target government or otherwise affect its conduct.

Background Information

As internet access and other components of information technology have extended over the world, cybercrime has become more prevalent in global politics. Regarding the cybercrime and cyberterrorism, one of the most fundamental problems is the clear differentiation between the meanings of these two jargons. It is often difficult to distinguish between attacks on computer networks by terrorists and cybercrimes by hackers. While the United Nations does not have a permanent consensus on an international definition of a cyber-attack or cyber-terrorism, informal working definitions have been deemed to include all types of online criminal behaviour. A cyber-crime or attack must, in general, it usually covers all illegal activity on the Internet. Cyber terror aims to damage, compel, or frighten a people or state in order to achieve for example political goals. Indeed, cyber-terrorists have the same goal as in a real-life.

Cyber Crime

It is commonplace that cyber threats have been existing for the past few decades. It was the year of 1975, when Steve Wozniak and Steve Jobs invented the first personal computer. Since that, a plethora of cyber issues started arising with the help of hackers, people who strived gaining illegal access in order to have access to valuable information. The type of information could really range regarding the goal of the hackers, from personal profit to conduct terrorist acts.

The first ever cyber-attack including a computer is well known as the Morris Worm in 1988. Robert Tappan Morris, a graduate student at Cornell University, was responsible for the first worm. In 1999 another inconceivable incident occurred, when a teenager hacked the U.S. Department of Defence's (DOD) computers in a way that he managed to intercept internal significant emails, which contained valuable information. After that, using his access to the system of DOD, he also stole software from NASA. In the same year, Melissa's Virus constitutes a virus, which attacks Microsoft Word documents and automatically sends itself as an attachment through email. It sends emails to the top 50 individuals listed in an infected

device's Outlook email address box. The interesting fact about the last incident is that the creator of this respective malware did not even have any intention to harm computers.

Similarly, in 2009 hackers gained access to Google's computers and Gmail accounts belonging to Chinese human rights advocates, in an act of cyber espionage. Authorities revealed that several Gmail accounts belonging to people from other countries had been hacked after further inquiry. As the years were passing by, it was perceivable that cyber threats were possible to happen and how harmful such an action could be. Again, in the same year, Gonzales, a hacker from Miami, engaged in one of the largest fraud cases in US history. He was able to retrieve tens of millions of credits and debit card details from more than 250 different financial institutions. He had hacked into different firms' payment card networks. A new type of cyber-attack expanded across 150 nations in 2017, including European countries and Australia. Unless a ransom is paid, hackers would threaten to erase users' files and data.

Cyber Terrorism

Before getting into cyberterrorism in particular, it is critical to first get a comprehensive grasp of terrorism. Terrorism is a phrase that a lot of politicians and ordinary people use to describe a variety of situations. Nowadays, there are many definitions of "terrorism", making it difficult to establish a single, universal definition. However, before we can achieve an agreement, we must first define what we mean. The following definition of Security Council Resolution 1373 (2001) could describe quite analytically our respective term:

‘... criminal acts, including against civilians, committed with intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature.’

Indeed, unlike during the Cold War, when countries fought one another, now we have specialised autonomous organisations, each with its own set of goals, beliefs, and ambitions. Furthermore, when the old totalitarian European governments crumbled and Africa's decolonization became a reality, nationality movements emerged in the social and political spheres, demanding attention for their struggle against social groupings. With many assaults in Spain, the ETA (Euskadi Ta Askatasuna), a Basque terrorist and separatist organisation, and the Terra Lliure (Free Land), a Catalan terrorist and separatist group, began to develop a foothold in society. In Ireland, the IRA (Irish Republican Army) became the most well-known terrorist organization in Europe in the second part of the twentieth century. Finally, Italy was in a dangerous position for a long time with the Italian Mafias, who, fearful of intimidation, robbery, extortion, and murder, gained control of areas such as Sicily (Casa Nostra Mafia) and Calabria (Ndrangheta Mafia)

All of these organisations operated in several ways, with varied structures and techniques, but they all followed the same basic strategy of intimidation and violence. Terrorist organizations, however, have begun to deploy terror operations using fewer victims and more computing methods to achieve the same amount of harm, if not more, that the stale operation mode permitted since the end of the 1990s. As a result, all these led to the creation of new forms of terrorism such as cyberterrorism.

This new kind of terrorism is a potent weapon that has to be examined in UN committees because it has already caused far too much harm to be ignored. In recent years, cyberterrorism has demonstrated its power and capability, exposing a number of high-profile individuals, such as the hack into Hillary Clinton's campaign in the United States and the case of the hack into the French system exposing personal information about Emmanuel Macron in France. In addition, a number of terrorist attacks against Chinese authorities have occurred as a result of spy state activities.

Virtual assaults come from a variety of places, and no firm or machine is safe. In this sense, from a simple computer virus to a large-scale hack in a hospital, we are all exposed, despite

the fact that terrorists may simply exploit cyberspace to enhance fear and panic in a large population with just one "click." As a result, we do not simply have one sort of cyberterrorism, but a variety of attacks with one thing in common: the use of the virtual world as a weapon.

One concrete example occurred in the United States in 2008, when Chinese espionage launched a virtual terrorist strike on an American space program, causing a massive drop in American jets and raising fears that all US government secrets may be revealed.

Sabotage-induced terror is also not directed at the general public. The most recent and prevalent examples include virtual sabotage, which occurs when governments aim to undermine another country's system, such as what occurred between the United States and South Korea when the US government hacked Korean systems, preventing missile launches.

Opposition organisations might potentially use sabotage to bring down a particular regime. As a result, the important idea is to concentrate on domestic issues rather than exterior issues, since most of these events are related to military actions done by governments with low public support. This may be observed in a number of African countries, where regimes are unpopular despite heavy military operations against people.

Cyber assaults do not bring back virtual terrorism. Threats of cyberterrorist groups committing terrorism beyond the screen are one of the most prominent examples. However, the situation is exacerbated by the fact that this kind of terror has a large capacity for media coverage, and here is where we want to draw your attention. The explicit and repercussions are what make this group's purpose achievable, which is exacerbated by psychological horror, which, unlike the physical, is usually the major goal.

Nigerian groups such as Boko Haram and Ansaru exploited the internet to propagate fear and show the world their aggressions between 2009 and 2012. Nonetheless, this is a method to link up with other organisations, like Al-Qaeda, both intertextually and philosophically. As a result, we can clearly see that threats are often worse than terror, but they may also be used to develop contacts between terrorist organizations all over the world, which can lead to alliances or even disagreements. One of the responsibilities of all countries is to strive to

achieve a consensus on how to counteract online misinformation and prevent excessive media use. Even if it is not a threat to the broader public or a specific group, threats always include fear as one of their objectives. The threat issued by the Islamic State to the financiers of Facebook and Twitter through video was one notable example of threats spread over the internet. They are also regarded as threats if they appear in a video that depicts specific acts of violence, such as the Islamic State film decapitating an American journalist, rather than merely decapitating six guys in cold blood. This kind of behaviour is classified as virtual terrorism because it involves behaviours that explicitly induce fear and propagate terror over the internet. Because of its speed, accessibility, ease of sharing, and broad reputation, the internet may be a terrorist's first option for spreading terror.

To conclude, a hack of a company's internal system is not always a terrorist assault. We should remember that the majority of hacks are not terrorist acts, thus international organizations must pay close attention to whether they should be categorized under cyberterrorism or hacks, since the penalties must change based on the categorization. But how can we classify a digital assault as terrorism or a normal hack in this manner? In the context of terrorism, a hacker's major purpose is to promote fear and insecurity in the public. As a result, if a hacker hacks into a company's system to steal customer data in order to gain financial gain, he is not a terrorist, and his assault should not be treated as such.

Types of Cyber Attacks

Malware

Malware refers to a wide range of threats, including spyware, viruses, and worms. When a user opens a "planted" harmful link or email attachment, which is used to install malicious software within the system, malware exploits a vulnerability to infiltrate a network.

Phishing

Phishing attacks are quite frequent, and they entail sending a wide range of bogus emails to unwary individuals while posing as a trusted source. The fraudulent emails often seem to be legitimate, but they contain a link to a malicious file or script that allows attackers to gain

access to your device in order to control it or gather information, install malicious scripts/files, or extract data such as user information, financial information, and more.

Man-in-the-Middle (MitM)

MitM occurs when an attacker intercepts a two-way transaction and inserts itself in the middle. From there, cyber attackers can steal and manipulate data by disrupting data traffic. This form of attack typically can exploit network vulnerabilities, for instance an unsecured public internet network for inserting themselves between the visitor's device and the network. The problem with this type of attack is that it can get hardly detected due to the fact that the victim thinks the information is heading for a legitimate target. In addition to this phishing or malware attacks are often used to conduct MitM attacks.

Denial-of-Service (DOS) Attacks

DoS attacks work by flooding systems, servers, and/or networks with traffic that overloads resources and bandwidth. As a result, the system is unable to process and respond to legitimate requests.

Zero-Day Exploit

Zero-day exploits constitute a type of exploit of new and recently announced network vulnerabilities before a patch is released or implemented. Zero-day attackers will jump into the exposed vulnerability in an abbreviated period with no precautions.

Bloc Positions

It is perceivable that cybersecurity constitutes a topic of great significance, which generates a great deal of heated debate, giving rise to a plethora of different opinions and methods concerning the respective issue not only in a national but also in an international degree. Indeed, there are two main sides, where the one advocates that the responsibility of cyberspace should remain within the scope of one state, whilst the opponents claim that the international governance could play a vital role in enhancing the international cyber security.

It is quite interesting that a set of countries, including Australia, Indonesia, and India, were only concerned about the cyber-related topics, only after having suffered from major cyber-attacks. Other key characters in the debate include:

Russian Federation

Over the past few years, the Russian government has conducted a plethora of major cyberattacks aimed at foreign countries, intended to help, or harm a particular political candidate and has consistently demonstrated Russia's power. Starting in 2007, the Russians attacked the satellites of the former Soviet Union such as Estonia, Georgia, Ukraine, then expanded to Western countries such as the US and Germany.

Iran

Iran has been a victim as well as a perpetrator of cyber warfare. Israel and the United States targeted it in 2009 as part of their Olympic Games (Stuxnet) attempt to temporarily disable part of its nuclear facilities. Iran has also been a willing participant in the development of cyber capabilities to counter cyber-attacks and defend against them.

International Police (INTERPOL)

INTERPOL is committed to a global fight against cyberattacks and is a natural partner to any law enforcement agency seeking to investigate these crimes on a collaborative level. Its plans include operations and investigation support, cyber intelligence and analytics, digital forensics, innovation and research, capacity building, and national cybersecurity assessment.

North Atlantic Treaty Organization (NATO)

NATO and its Allies rely upon sturdy and resilient cyber defences so that you can gain collective protection, cooperation, disaster control and security. NATO signed a Technical Arrangement on cyber protection cooperation with the European Union (EU) in February 2016. Allies are committed to replacing data and statistics associated with coping with and getting better from cyber-attacks.

Commission of Crime Prevention and Criminal Justice

It was founded by the Economic and Social Council (ECOSOC) in 1992 and its main objective is to enhance international action against national and multinational crime. It also provides States with a forum to exchange expertise, experience and information in order to develop national and international strategies for dealing with criminal activities. Since cybercrime is a crime in itself, the United Nations (UN) agency responsible for combating this crime can work with other NGOs to ensure cybersecurity.

Democratic People's Republic of Korea (North Korea)

Even though DPRK does not constitute a major force in the UN, it could be the solution of future UN resolutions. North Korea is an important player in the field of cybersecurity. Indeed, being privileged for asymmetric cyberattacks to disrupt targeted and provocative activities to justify domestic considerations, North Korea was found responsible for the Sony Hack in 2014. In addition, domestic censorship and propaganda are widely used. North Korea is believed to be using cyber activity to increase state revenue, to some extent bypassing UN sanctions.

Points A Resolution Should Address

The first issue is related to the clear definition regarding cyberterrorism and the fundamental aspects of cybercrime. What, particularly, are the existing international tools and how successful are they? What are the key challenges to consider when examining existing cybercrime treaties and national law, and how can the resolution address them? Which is the best way to distinguish a 'simple' cyber attack from cyberterrorism?

The second point delegates should think about is how to strike a balance between cyber security and individual rights. Do demands for cyber security necessitate the surrender of a sizable portion of private enterprises' and users' previous liberties to state government control and oversight? A plethora of countries are plainly in favour of such oversight, while others say it is the polar opposite of what the Internet should accomplish.

The third topic that may be addressed is how to enhance present national and international actions implemented by states. Delegates are urged to consider measures both for their states and under an international frame.

The role of the United Nations is the fourth topic to discuss. Can member nations of the UN be required to set common Internet security and monitoring standards? Is it possible for UN Member States to agree on a common protocol for Internet usage and security?

Delegate's mini guide

It is commonplace to mention that you will not represent your own beliefs, but you will act on behalf of a country's interests, you are assigned to represent. As a result, it is important to study your country's policy, in order to acquire a better understanding on how to deal with the topic. Additionally, we would advise you to study the study guide, check the bibliography and the footnotes in order to acquire a more thorough understanding about things you find important. Moreover, even though there is already a section of definition of key-terms, do not hesitate also to search on your own, especially things with which you are not so familiar.

- Links for fundamental information for each country: https://www.cia.gov/the-world-factbook/countries/
- Furthermore, there is a plethora of UN Treaties, which you could check in order to get some ideas. For instance:
  https://undocs.org/A/RES/64/211.
  https://undocs.org/A/RES/70/237.

Bibliography

Poliveiraa. “Cybercrime Module 14 Key Issues: Cyberterrorism.” Cybercrime Module 14 Key Issues: Cyberterrorism, https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html.

“The History of Cybercrime: A Comprehensive Guide(2021).” Jigsaw Academy, 13 Feb. 2021, https://www.jigsawacademy.com/blogs/cyber-security/history-of-cybercrime/.

“United Nations, Main Body, Main Organs, General Assembly.” United Nations, United Nations, https://www.un.org/en/ga/first/index.shtml.

“Top 5 Most Notorious Attacks in the History of Cyber Warfare.” Fortinet, https://www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare.

Peterson, Andrea. “The Sony Pictures Hack, Explained.” The Washington Post, WP Company, 6 Dec. 2021, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

“Iran and Cyber Power.” Iran and Cyber Power | Center for Strategic and International Studies, 24 Feb. 2022, https://www.csis.org/analysis/iran-and-cyber-power.

Cyberwarfare and Cyberterrorism: In Brief. https://sgp.fas.org/crs/natsec/R43955.pdf.

“Chinese See Almost 1,000 Percent Increase in Cyber Attacks.” NBCNews.com, NBCUniversal News Group, 29 Nov. 2016, http://www.nbcnews.com/tech/tech-news/chinese-seealmost-1-000-percent-increase-cyber-attacks-n689466.

“Cybercrime.” INTERPOL, https://www.interpol.int/en/Crimes/Cybercrime.

Jinghua, Lyu. “What Are China's Cyber Capabilities and Intentions?” Carnegie Endowment for International Peace, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.
Nato. “Cyber Defence.” NATO, 4 Feb. 2022, http://www.nato.int/cps/en/natohq/topics_78170.htm.

“Ukraine Accuses Russia of Cyber-Attack on Two Banks and Its Defence Ministry.” The Guardian, Guardian News and Media, 16 Feb. 2022, https://www.theguardian.com/world/2022/feb/16/ukraine-accuses-russia-of-cyber-attack-on-two-banks-and-its-defence-ministry.