The Doon School Model United Nations Conference 2018

BACKGROUND GUIDE

UNITED NATIONS SECURITY COUNCIL

CONTENTS

ABOUT DSMUN

The Doon School Model United Nations Conference is one of India's biggest and well-reputed high school MUN conferences. Since its inauguration in 2007, The Doon School Model United Nations Society has hosted an engaging, entertaining and intellectually stimulating conference annually, with each leaving behind a unique legacy. DSMUN has grown to be one of the key entries in every school's MUNning calendar. DSMUN has a history of attracting the best of both—the Indian and the international delegates—from the Pan-Asiatic Region. With each passing year, DSMUN has evolved and developed its programme, introducing new committees, creating singular crises situations and setting unorthodox agendas to challenge the delegates.

The Doon School, one of India's most reputed and prestigious institutions, is a member of the G20 Group of Schools, The Headmasters' and Headmistresses' Conference, The International Boys' Schools Coalition and the Round Square Conference. With its motto, "Knowledge Our Light", the School aims to mould its students into gentlemen of service and leaders for the future. Model United Nations is one of the largest and most popular activities in School, with over 200 students involved in it. The beautiful and serene 72 acre Chandbagh Estate, in which the school campus is set, and its heritage buildings, provide a scenic venue for the conference, ensuring that it will be an experience unlike any other MUN.

The DSMUN Secretariat is proud to host The 12th Doon School Model United Nations Conference from the 17th to the 19th of August, 2018. Popularly referred to as DSMUN '18, this year's conference intends to engage the delegates in 12 diverse committees, each of which will generate discussion on various contemporary and thought-provoking issues. There is also the promise of an opportunity to make new friends and create lifelong memories. We look forward to seeing you in Dehra Dun in August!

Crises to keep you on your toes, unforgettable memories, interesting new people to meet and an experience worth a lifetime—DSMUN '18 will have it all!

DSMUN'18

Ojas Kharabanda

Secretary General

Ritwik Saraf

President

Devang Laddha

Chairperson

Aryaman Kakkar

Paras Gupta

Deputy Chairpersons

THE DOON SCHOOL,
Mall Road,
Dehradun—248001,
UK, India
Phone: +919760013831
e-Mail: chair.sc@doonschool.com
dsmun@doonschool.com
www.dsmun18.com

THE DOON SCHOOL MODEL UNITED NATIONS

A LETTER FROM THE SECRETARY GENERAL

Dear Delegates,

It is an absolute privilege and honour for me to welcome you all to the 12th edition of The Doon School Model United Nations. What was once a small regional event has evolved and grown into an international conference with a repute and prestige that extends across borders. This year, we aim to raise the bar higher, with an invigorating mix of structured GA committees like the DISEC and Security Council to dynamic crisis committees like The Third Reich.

I am a veteran of the International Baccalaureate Diploma Programme, and take a keen interest in geopolitical developments across the world. I am extremely passionate about photography, and am the Editor-in-Chief of The Yearbook, which is one of the premier publications of our school. I have been involved for a considerable time in the MUNning world, and apart from winning multiple accolades, was the Vice-President of last year's conference. In a world that is becoming increasingly divisive and polarized, it is vital that we realise the special importance diplomacy and the simple willingness to hear each other out holds. Each committee is uniquely placed at a time and place to make a difference, but only if we approach each negotiation with peace as the goal will our time here be fruitful. I eagerly await your presence at Chandbagh.

Warm Regards,

Ojas Kharabanda

DSMUN'18

Ojas Kharabanda

Secretary General

Ritwik Saraf

President

Devang Laddha

Chairperson

Aryaman Kakkar

Paras Gupta

Deputy Chairpersons

THE DOON SCHOOL,
Mall Road,
Dehradun—248001,
UK, India
Phone: +919760013831
e-Mail: chair.sc@doonschool.com
dsmun@doonschool.com
www.dsmun18.com

THE DOON SCHOOL MODEL UNITED NATIONS

A LETTER FROM THE PRESIDENT

Dear Delegates,

I am extremely delighted to welcome you all to the 12th edition of the Doon School Model United Nations. Over the stretch of 12 years, DSMUN has earned itself a place among the most eagerly awaited MUNs in the whole of India; this year too, we have spared no effort in meeting these expectations.

With over 12 committees, including the GA committees of DISEC and SPECPOL as well as exciting crisis committees like Board of Control, East India Company, DSMUN promises to engage the delegates in a fierce tussle of rhetoric, negotiation and documentation- areas that have come to occupy an important place in an individual's holistic development. Further, DSMUN also provides an exciting opportunity for the delegates to meet and make unforgettable memories with people from all over the country!

I currently pursue the ISC curriculum., and after having served in the DSMUN secretariat for 3 years, I am privileged to be at its helm as the President in my last year in School. As the world continues to shrink to an even smaller place, the problems that torment humanity continue to expand. Time, therefore, warrants us to step up and collectively lead the human race to a better tomorrow. And to initiate this, we must begin from a young age itself.

Looking forward to meeting you in August,

Ritwik Saraf

DSMUN'18

Ojas Kharabanda

Secretary General

Ritwik Saraf

President

Devang Laddha

Chairperson

Aryaman Kakkar

Paras Gupta

Deputy Chairpersons

THE DOON SCHOOL,
Mall Road,
Dehradun—248001,
UK, India
Phone: +919760013831
e-Mail: chair.sc@doonschool.com
dsmun@doonschool.com
www.dsmun18.com

THE DOON SCHOOL MODEL UNITED NATIONS

A LETTER FROM THE CHAIRPERSON

Greetings delegates!

I take great pleasure in inviting you to the United Nations Security Council (UNSC) for the Doon School Model United Nations, 2018. The UNSC has been one of the most stimulating committees at DSMUN and this year we hope to ensure the same. This year, the UNSC shall be discussing two agendas:

1. Framework to deal with Failed States
2. Cyberwarfare

This Background Guide is to serve as your gateway for all research before committee. I would encourage you all to go through the entire guide and then use the references at the end as starting points for any further research. This is to give you direction as to what kind of discussion we are looking for in committee and how we want to go about it. To ensure great quality of debate and discussion, the countries for the UNSC have also been slightly modified. This guide by no means is sufficient research for committee, it merely is a starting point.

Moreover, as you surely know, the UNSC has slightly different rules of procedure than an ordinary GA committee. I hope that you all will thoroughly read up on the different rules for the UNSC. For any clarification, feel free to email me at any time and I will do my best to help you out. You are also required to know any past actions the UN has taken in the matters of these two agendas and how effective these policies have been. The Executive Board will be judging you on your research, your ability to lobby, your speeches and the solutions you propose.

I hope you all enjoy your experience at Chandbagh and hope to see you soon!

Warm Regards,

Devang Laddha

AGENDA 1: INTERVENTION IN FAILED STATES

Introduction

In the modern world there are several nations that are currently facing social, political and economic crises. These crises are caused by varied factors and have no set root, ranging from ethnic violence to corrupt authoritarian leaders and economic crises. However, they all have a similar outcome: the failure of the basic institutions. Institutions that secure the people's health, welfare and rights start deteriorating due to internal and external reasons, causing instability in the country. Due to this instability, governments often become dysfunctional and cannot support the rights of their own people. People see their rights abused on a daily basis: being sent to prison without fair trial, being raped and looted on a regular basis and having to fight to meet their basic needs, to name a few. Furthermore, these nations tend to become refuge for terrorist organizations as the lack of law and order makes these nations ideal for them.

The United Nation Security Council as the executive body of the United Nations aims to secure the rights of people across the world. Having the power to enforce economic sanctions, interfere in transportation and communication and call for ceasefire, UNSC aims to uphold the values of the United Nations and ensure peace within nations. However, historically the UNSC has had a bad track record of assisting nations embroiled in great crises. Due to the various conflicts of interest within the P5 Nations (Russia, US, UK, France and China), the decision making within the UN has been poor. This has led to the UN being involved in interventions that have gone awry and have not been able to help the people. Moreover, this intervention has also led to countries unilaterally intervening into other countries' affairs, breaching their sovereignty. These interventions have not always worked and have sometimes worsened the situation of countries, leading to more political and social turmoil.

In a world such as this, it is imperative that we find a solution to helping nations in need, where thousands are suffering. To deal with this, the first item on the agenda for this UNSC is to draft a resolution which would act as a guideline for nations while dealing with 'Failed States'.

The first requirement of the UNSC is to discuss what a failed state is. Delegates can use various criteria to show which countries classified as failed states. These criteria can be social (in terms of social tensions within a country), political (in terms of a lack of opposition or political infighting) or economic (in terms of corruption and inflation). In this guide, we have given some examples of what we consider to be failed states. This list by no means exclusive and delegates can discuss other failed states. As you will see, some nations that we have discussed have in the past been failed states, and may not currently be so. This is to give delegates an idea of the markers that can help identify failed states. Delegates are expected to thoroughly research failed states, both current and past, and understand the situations that have caused them to fail.

Moreover, delegates are expected to draft solutions that can help resolve issues that failed states face. They must recognize that the problems of a failed state not only affect the country's own citizens but also those of

neighbouring nations and other nations with whom they are trade partners. Throughout the guide, we have provided various questions that can guide delegates in terms of where discussion in committee will be going and what issues we look forward to being discussed. Delegates must also understand that the aim of the UNSC is not to merely end the crisis but to bring the nation back on its feet and secure the rights of the people.

Ultimately, the goal of the UN and the UNSC is to secure the rights of the people. People in failed states are vulnerable and their rights are abused on a regular basis. Delegates are to draft solutions to help these nations and their populace. Given below is a list of states that we consider to be failed states. This list is to serve as the starting point for your research for this agenda.

COUNTRIES

Cambodia– Khmer Rouge

Pol Pot was the leader of the communist Khmer Rouge government, which governed Cambodia from 1975 to 1979. During his four years of rule, approximately 1.5 to 2 million Cambodians died of starvation, execution, disease or overwork. Some regard this as one of the most barbaric and murderous eras in recent history. The Marxist leader tried to take Cambodia back to the Middle Ages, forcing millions of people from the cities to work on communal farms in the periphery of the country and this 'dramatic attempt' at social changes had a horrific cost.

On April 17 1975, the Khmer Rouge regime took power after winning the civil war which had caused mass destruction. As soon as they controlled the nation, the power bloc started transforming Cambodia into what they hoped to be an agrarian utopia. Former civil servants, doctors, teachers and other professionals were removed from their professions and were forced to toil in the field as a part of a 're-education' process. The cities were empty, private property was abolished along with money and religion. People were killed for wearing glasses or knowing a foreign language. In the years that followed, as Cambodia began the process of reopening to the international community, the full horrors of the regime became apparent. Those that complained about work or any change in the ideas were tortured in a detention center, such as the infamous S-21 and were then executed. This Cambodian genocide led to long-term effects on the nation and its citizens for many years to come.

This internal destruction continued till 1977, and in December 1978 the Vietnamese sent more troops along with arms across the border. Finally on January 7, 1979, they captured Phnom Penh and forced Pol Pot to flee back into the jungle. Throughout the 1980s, the Khmer Rouge received arms from China and political support from the United States who vehemently opposed Vietnam. But the Khmer Rouge's influence began to decrease following a 1991 ceasefire agreement, which finally led to the end of the movement.

Although this movement came to an end, its effects were disastrous. The people were still under fear and were scared to open their country up to the world. The Khmer Rouge saw the death of thousands and the abuse of even more. Basic human rights were not protected in any manner and the war, essentially, crippled Cambodia. Economically, the nation's GDP plummeted and reached an all-time low. Due to

the war, the agricultural sector suffered major setbacks leading to a full-blown agrarian crisis in 1979. Reviving the economy after the war was a massive task and took a lot of time.

Questions:

- How could diplomacy have been used to help the Cambodian crisis?
- How could the state of the people have been made better without a military intervention?
- If and what sanctions should have been put on the government, given the plight of the people who were already suffering?
- An invasion brought an end to this crisis, but was equally destructive. How do we prevent nations to take benefit of these vulnerable situations?

Chile – Pinochet Government

Augusto Pinochet was the president of Chile between 1973 and 1990. He ruled as a dictator, having overthrown the democratically-elected Marxist-leader President Salvador Allende in a coup d'état. His rule can been seen as a boon to Chile if one were to view it from an economic perspective, but as a bane if one were to look at the country's human rights record. Pinochet was appointed as the Commander in Chief in 1973 by President Allende. Only three weeks into the post, Pinochet played a crucial role in the CIA-sponsored coup against the leader. The aim of the coup was to "Liberate Chile from Marxist oppression". Having overthrown the democratic rule, the new military government consisted of the heads of the three-armed forces, known as the Junta. Pinochet, who was a Junta, banned all left-leaning political parties to function in Chile. In December 1974, Pinochet officially changed his title from the Supreme Chief of the nation to that of President of Chile. With his free market reforms and economic changes Chile earned a name in the World but this came with a cost. In 1980 a referendum was held to adopt a new constitution, and among its various features were proposals to increase Presidential power and allow Pinochet an additional eight years of rule. The new document was passed by 67% of the electorate, despite the criticism against it. Another referendum was held in 1988, which asked the people for another eight years in office. Prior to the referendum, in the face of international pressure, Pinochet had legalized other political parties in 1987. Later, the referendum for another 8 years of rule was rejected and it was followed by elections. Pinochet lost the seat of the President but remained Commander in Chief till 1998.

Due to his policies, public education and pensioning system were destroyed. Businessmen and many wage workers lost their livelihoods, leaving them to starve. These effects led to a poverty-stricken and unstable Chile. This crisis is different from the others as the economic conditions and the strength of the army augmented, yet humanitarian problems increased. Hence, we need to guide our interventions keeping in mind such differences.

Questions

- The concept of coup d'état has risen many times and we as committee need to come up with a strategy or a plan which would clearly define a situation of coup d'état so we can avoid false accusations.
- The process of eliminating all left wing members is extremely radical and inhuman. How would one convince a leader to give up on such a want?

Myanmar

The history of Myanmar, also called Burma, can be divided into fractions; the division is on the basis of political setup in that time frame. Post-independence U Nu became the Prime minister and led the nation till 1962, when he was ousted in a military coup led by Gen Ne Win. Gen abolished the federal system and inaugurated "The Burmese Way of Socialism", nationalizing the economy, banning independent newspapers and forming a single-party state. In 1974, a new constitution came into effect, transferring power from the armed forces to a People's assembly headed by Ne Win and other former military leaders. This form of government could not maintain law and order and soon the Opposition National Democratic Front, formed by regionally -based minority, mounted guerrilla insurgencies. This government followed the teachings of Nazism and abided by the concept of One Party, One leader. Due to such a dictatorial rule, the economy degraded and anti-government protests started. These protests led to fthe ormation of 'The State Law and order Restoration Council'. This council declared Martial Law and put thousands of people under arrests.

What followed post 1990 were direct implications of 'Thwarted Elections'. The general elections were won by Opposition National League of Democracy (NLD) but the results were ignored by the military. Aung San Suu Kyi was a member of NLD and played a vital role in protests against the government. Being a pro-democrat, she was constantly put under house arrest and was stripped off her fundamental rights. After this incident the country continuously remained in a political turmoil and the general public suffered. The major crisis revolved around the existence of Muslim minority and some ethnic groups. They were assaulted by the army and were not recognized as citizens. China and Russia vetoed a draft US resolution at the UN Security Council which aimed at urging Myanmar to stop persecuting minority and opposition groups.

In 2011, there was finally some sort of democracy that appeared with NLD taking part in the elections. It wasn't a complete democarcy because of the nature of the Prime ministerial-rule that followed. Her concept of religion and dictatorial actions have led to the Rohingya crisis. This shows how it is necessary for UNSC to not only tackle the crisis at hand but also reinstate peace in the nation, along with its political set up. If the latter is not performed, then we fail to perform our duties. What follows is a description of how the Rohingya crisis began and how Myanmar is not a democracy by spirit.

The Rohingya, numbered one million in Myanmar at the start of 2017, are one of the minorities in Myanmar. This is a Muslim sect with majority of the members living in Rakhine state. Descendants of Arab traders, they have

their own distinct language and culture. However, the Government of Myanmar, a Buddhist country, refuses to recognize them as its citizens and considers them illegal immigrants from Bangladesh. In the last few years, before the current crisis, Rohingya tribe members have made perilous journeys out of Myanmar to escape communal violence or alleged abuses by the security forces. The clash is between the Rohingya members and the Government of Myanmar. The clash is a fight of right to citizenship. The government and the police officials are assaulting the tribe, raping its women and murdering its kids. They have no option but to flee to Bangladesh, leading to a refugee crisis. The UN says that the Rohingya's situation is the "world's fastest growing refugee crisis". The need for aid is overwhelming. With the onset of monsoon coming closer, work has begun to relocate the refugee camps and to improve drainage channels. There is shortage of food and the medication facilities are not properly provided.

The world has shown verbal support; however, neither sanctions nor actions have been taken by any nation or body. The UNSC appealed to Myanmar to stop the violence but no sanctions have been imposed. In the opinion of UN's Human Rights Chief Zeid Ra'ad al-Hassan, "the act of genocide against Rohingya Muslims by state forces in Myanmar cannot be neglected". US and UK have all tried attempts to convince Myanmar to respect "The rule of law" but nothing could move the state's firm beliefs.

Myanmar's Rohingyas open up a different aspect of crisis- a conflict between religion and brutal actions due to religious beliefs of a nation. UN is bound to not interfere in internal matters of nations, yet this war seems to affect neighboring nations, majorly Bangladesh, and so we need to rely on sanctions to stop the crisis at hand.

Questions

- Buddhism is followed by many citizens, and going against their beliefs might lead to protest. How do we take steps and yet avoiding these repercussions?
- A fight between religions often leads to hindrance from other nations and groups. What are the steps that should be taken to avoid them?

Yemen

Claimed to be the country with the world's biggest man-made hunger crisis and cholera epidemic, Yemen has been under crisis since 2011. The Yemen conflict, like many others, started due to political instability. This is rather ironic, as the political transition that was supposed to bring stability to Yemen has, in fact, led to this civil war.

Followed by the Arab Spring uprising, the authoritarian president Ali Abdullah Saleh handed over his power to Abdrabbuh Mansour Hadi. Hadi himself proved to be incapable and struggled with problems like Al-Qaeda, corruption, unemployment and food insecurity. This gave the Houthi movement a chance to take advantage of the weak power and control Saana and other provinces. This movement won support of the Sunnis, giving the civil war a religious motive. The president fled to Aden during all this chaos making the country the centre of a political whirlpool. Three UN organised plans have failed and the situation is still not settled. Such chaotic situations are ideal for terrorist intervention, and so it happened. Jihadist militants from Al-Qaeda and the rival affiliates of the Islamic State group (IS) have wreaked havoc, killing thousands. Houthi

fighters have made efforts to take full control of the capital and have deemed Mr Saleh dead. To worsen the situation there have been instances of further division within the already existing rebel groups.

According to UN, more than 9245 people have been killed and 52,800 lay injured. UN Human Rights Council believes that civilians have been victims of 'breach of international humanitarian law'. There is scarcity of food and with the sudden outbreak of Cholera and lack of medical facilities, people feel helpless there. AQAP is considered the most dangerous branch of Al-Qaeda and ending this Civil war brings an end to this threat as well. This war is also to a certain extent a war between Shia-ruled Iran and Sunni-ruled Saudi Arabia. There has been questioning on why the UNSC has taken no action to restore peace and these questions should be answered as soon as possible cause any delay can threaten the lives of thousands of innocent people.

Questions:

- How do we stop the supply of arms and its routes?
- There is demand of power from all sides and external countries are looking for a chance to grab it. In such circumstances what are the steps to stop external intervention?
- Yemen lies in the middle of an oil route and this has caused trouble to trade, how do we go about posing restrictions on transportation?

Syria

Located in Western Asia, Syria has been officially under crisis since 15 March, 2011. Syria is currently in the midst of political instability, economic breakdown, a refugee crisis and religious conflict. The chain of events began in 2011 with the Arab Spring which fueled waves of pro-democracy protests across the country. The Syrian government under Bashar Al-Assad responded brutally, slaughtering hundreds. In July, defectors from the military formed 'The Free Syrian Army' with the aim of taking down the current government and establishing their own. These defectors started fighting with the government leading to violence erupting across the country, causing a civil war.

Most Syrians are Sunni Muslims, but Syria's security was under the members of Alawi sect, which gave way to rebel sectarian divisions. By June 2013, the UN said 90,000 people had been killed in this civil war and this figure kept augmenting. The major turn of events happened when foreign intervention took place. There became two distinct power groups with ulterior motives. The governments of Shia-majority Iran and Iraq coupled with Lebanon based Hezbollah have supported Assad's government, while Sunni majority countries, including Turkey, Qatar, and Saudi Arabia supported Anti-Assad rebels. This division of Syria into different administrations and rebel groups has caused decentralization of power, which in turn has led to no functioning judiciary and legislature. This absolute anarchy has led to severe war crimes taking place around Syria like murder, rape, blocking access to food and ceasing medical and health facilities by rebel groups as a method of war.

In August 2013, the war led to the Syrian government resorting to the use of chemical warfare against the rebels in Damascus- leading to collateral damage in the form of thousands of innocent Syrian lives lost. USA, along with UK and France, had threatened military

intervention. In April 2017, the US carried its first direct military action against Assad's forces, launching 59 Tomahawk cruise missiles at a Syrian air force base from which US officials believe a chemical attack on rebel groups had been launched. At the UN Security Council, Russia along with China have repeatedly vetoed western-backed strategy. The terrorist groups have taken advantage of these conditions and established rule in certain regions, these groups are termed as rebel groups.

The Islamic State (IS) has capitalised on the chaos and taken control of certain regions of Syria and Iraq, where it declared the creation of a "caliphate" in June 2014. This has caused a war within a war in Syria, as foreign military intervention now combats rebels and rival jihadists from the al-Qaeda-affiliated Nusra Front, as well as government and Kurdish forces.

The problem seems to be clear when we go through the facts and the effect of the crisis. According to UN, more than 11 million Syrians have been displaced, of which 5.3 million have tried to find some hope in neighbouring countries. The funds seem to be disappearing and lack of support from nations have aggravated the situation. Now we as a committee have certain powers, along which comes certain obligations. Syria should be a major example of dealing with failed states and our final guidelines should show how the diplomatic solutions have shown results.

Questions:

- How do we manage and control the Syrian displacing? Where do we find place from them to abide and how to convince neighbouring nations for their support?

- How to curb the growing terrorism and what directions are to be given to Counter-Terrorism Committee?
- The P-5 are divided and we are not able to reach any conclusion. How do we try and reach the same basis?
- The important factor is to reduce the number of deaths and call for evacuation from places, how do we go about these remedies?

Afghanistan

Lying between Saudi Arabia and India, Afghanistan has been the centre of terrorist activity and has been through years of unrest and destruction. During the cold war, Soviets had invaded Afghanistan in order to infuse communist ideas. This was heavily opposed by USA and this war dragged on for 10 years. Around 1990's Soviets gave up and left the nation, followed by withdrawal of USA forces leaving the country lawless and chaotic. The USA had funded a militant group known as the Taliban - providing them with military support to battle with the Soviets in Afghanistan. After the war ended the Taliban took control and the country soon came under strict Islamic laws. By 1996, Taliban took over the capital city of Kabul and this happened to be the time when Osama Bin Laden arrived in Afghanistan, having been ousted from Sudan. He set up training camps in Afghanistan with the help of his terrorist group, Al-Qaeda and planned 9/11 there. After the devastating attack, USA drove Bin Laden along with Al-Qaeda to the mountains and since then United States has had a permanent military presence in Afghanistan.

In March 2003, USA attacked Iraq with the objective of finding ammunitions held by the dictator Saddam Hussein. The effort went in vain as no weapons were found and it was said all over that this war was a mistake. This mistake was the tool by which Obama won his election in 2008 and said that real enemies were hiding in borders between Afghanistan and Pakistan. He sent brigades to Afghanistan, replaced the Governor General and took some serious military actions in that region.

Since then Afghanistan has been under political tensions and, moreover, has become the centre of terrorist activities. The latter is a threat not only to the nation but also to the world and bringing the end to this crisis will have a larger impact on the globe. Also, it is necessary to bring the nation back on its feet after the end of this era of terror. Recently the Trump administration has decided to keep US troops in Afghanistan to fight the Taliban and provide stability to the nation. However, due to this Afghan-US alliance Afghanistan has become dependent on US military aid and special forces to counter unrest and terrorist activity in their country, with the hope that this would cause long term political stability in their nation. With the possibility that the US could pull its troops out at any time with change in administration or due to certain emergencies, this reliance of Afghanistan on the US could cause further instability. The Taliban would take over the country leading to a possible civil war and further political instability. Thus, as members of the UNSC we must discuss the following questions in committee.

Questions

- Dealing with terrorist has always been tricky; how do we as a committee come up with a tactical strategy with the help of other nations?

- In general there have been times when people are misled. How do we control such situations?

Venezuela

The country is in the midst of political turmoil which is accompanied by hyperinflation and breakdown of the economy. The trouble is because the country is divided by different leaders and Venezuela is therefore a failed democracy. Venezuela is split into Chavistas, the followers of the socialist policies of President Hugo Chavez, former president of this broken democracy. After the end of the socialistic ruler in 2013, Nicolas Maduro, member of the United Socialist Party (PSUV), was elected the President and he swore to continue Mr Chavez's policies. These two leaders were celebrated by the Chavistas but the opposition, Democratic Unity Roundtable (MUD), feels that since the socialist party has come into power, the democratic institutions have been eroded and they saw a decline of their strong economy. This brought the rebel among the two groups on surface. One of the accusations made by the Chavistas is that the opposition are in the pay of the United States of America, a country which has poor relations with Venezuela. However, Mr Maduro has failed to inspire the Chavistas in the same way as their predecessor. A series of events has further heightened tensions between the two groups and this ultimately forced the Supreme Court to take actions. On 29th March the judiciary announced complete takeover of the opposition-controlled National Assembly. This verdict was strongly opposed, and was accused as an act of creating one-man rule under President Nicolas Maduro. This led to Supreme Court reverting its verdict. Due to the ongoing protests and rampage in the country, the President was forced to announce the creation of a constituent assembly to draft a constitution for Venezuela and blamed the opposition for falsely accusing the government of leading the nation into an "economic crisis". Mr Maduro believes that this body would 'neutralise' the political turmoil. The opposition did not buy this idea and developed a new notion that this was a step to delay the general elections 2018 and retain power. This conflict of power among the Supreme Court, Mr Munro's government and the opposition led to protests starting from the capital, Caracas, and eventually turning into a civil war.

Apart from hyperinflation, which is largely due to the black market, Venezuela finds itself stuck in an 'Economic War' including speculations and hoarding by opposition followers. Food shortage is due to the fluctuation in the prices of food due to black market. There has been a steep decline in the production of oil leading to problems in other countries. The focus has shifted from growth of the economy to paying back the debts, leading to poverty in the entire nation. There is lack of medication which in turn is leading to deaths at a large scale. In February 2018, Venezuela became the first nation with cryptocurrency, the Petro. 2016 was the year when Venezuela experienced highest-ever homicide rate at 91.8 homicides per 100,000 residents. There are people displacing to Colombia and Brazil, while some have left for the island of Curacao. Mercosur, an economic and political bloc comprising Argentina, Brazil, Paraguay, Uruguay, and Venezuela, removed Venezuela in 2016. Organisation of American States (OAS) recommended removal of Venezuela until Maduro's government resigns.

These international issues add fuel to the civil war of the enation and hence Venezuela requires immediate attention of the UNSC.

Questions:

- How do we deal with organisations such as OAS and Mercosur, which cause additional problems to the war?
- Reduction in production of oil has caused severe effects on other nations; how do we minimize these effects?
- The black market is playing a significant role in the civil war. How do we bring an end to it?

CONCLUSION

These examples cover all the aspects we need to resolve and are concerned about. This agenda can avoid a lot of crisis in future and more importantly will save life of millions. I would like to remind the delegates that we are working for humanity at large. I would request the delegates to understand the suffering that the citizens of failed nations are going through. The delegates need to put aside personal interests and work as one unit to achieve the common goal. Hope to have an intense debate on this topic with a common agenda in head.

REFERENCES AND FURTHER READING

Cambodia

- http://countrystudies.us/cambodia/61.htm
- http://www.bbc.com/news/world-asia-pacific-10684399
- https://www.aljazeera.com/indepth/features/2012/02/20122314155454169.html
- https://www.history.com/topics/the-khmer-rouge
- https://www.britannica.com/topic/Khmer-Rouge

Chile

- https://www.theguardian.com/world/1998/oct/20/pinochet.chile
- https://www.foreignaffairs.com/articles/chile/2014-05-22/what-really-happened-chile
- http://countrystudies.us/chile/67.htm
- http://countrystudies.us/chile/60.htm

Myanmar

- http://www.bbc.com/news/world-asia-pacific-12990563
- https://edition.cnn.com/2017/09/21/asia/myanmar-military-the-real-power/index.html
- https://www.cfr.org/backgrounder/rohingya-crisis
- https://news.sky.com/feature/rohingya-crisis-11121896
- http://www.bbc.com/news/world-asia-pacific-12992883

Yemen

- http://www.bbc.com/news/world-middle-east-29319423
- https://edition.cnn.com/2018/04/03/middleeast/yemen-worlds-worst-humanitarian-crisis-un-intl/index.html
- https://www.aljazeera.com/news/2018/01/yemen-worst-humanitarian-crisis-50-years-180105190332474.html
- https://www.nytimes.com/2018/03/27/opinion/letters/saudi-yemen.html

Syria

- http://www.bbc.com/news/world-middle-east-35806229
- https://edition.cnn.com/specials/middleeast/syria

Afghanistan

- https://waronwant.org/crisis-afghanistan
- https://www.britannica.com/event/Afghanistan-War
- http://www.bbc.com/news/world-south-asia-12024253
- http://www.foxnews.com/opinion/2017/08/02/afghanistan-in-crisis-why-is-region-still-hotbed-terrorism-and-violence.html

Venezuela

- https://www.opendemocracy.net/democraciaabierta/chris-carlson/crisis-in-venezuela-and-its-lessons-for-left
- http://www.bbc.com/news/world-latin-america-36319877
- https://www.cfr.org/backgrounder/venezuela-crisis
- https://www.aljazeera.com/indepth/features/2017/04/venezuela-happening-170412114045595.html

AGENDA 2: CYBER WARFARE

Introduction

In a world where we are making stellar advancements in the field of technology, it is becoming harder and harder to protect the advancements and seal off all vulnerabilities in the system. Hackers then take advantage of these vulnerabilities and use them as weapons in cyber wars. Cyber warfare is infiltrating and attacking a nation's network mainframe and through hacking, introduce rouge elements in a cyberspace to cause panic, corruption of online networks, and crippling of critical infrastructure. It is a means of war used by terrorist groups as well as nation states and has become increasingly popular over the last few decades because of its devastating effects spread out over a large region. It also acts as a convenient method of warfare as it can be used by anyone with a working knowledge of hacking and access to the Internet. Cyberwarfare is usually perpetrated by hackers in the military of a Nation-State or by a civilian hacker supported by the said Nation State. They then proceed to study the network and mainframe of their opponents to try to discern flaws and vulnerabilities in the design. Once found, they are exploited to temporarily or permanently disable an opponent or in turn, remand complete control of the system, cutting off the opponent's access entirely. Its capabilities can be used at the lowest tier to support traditional warfare and at the highest tier for information theft, sabotage, espionage, etc.

The nature of warfare has shifted from physical to online, seeing a deluge of state-sponsored cyber assaults on the West. The issue was put under the global spotlight in the month of April, when the UK and the US made an unprecedented joint statement blaming Russia for cyber-attacks on businesses and consumers. The announcement – which is the first time two nations have come together to show solidarity in this area – saw the National Cyber Security Centre (NCSC), US Department of Homeland Security and the FBI warn businesses and citizens that Russia is exploiting network infrastructure devices such as routers around the world. It is widely agreed that Russia is one of the most – if not the most – accomplished nations in the world in its ability to perform state sponsored attacks, disinformation and espionage. But China, North Korea and Iran are also known to have dedicated cyber arsenals that are of increasing threat to the West.

In April, the US and the UK governments hit out at state owned Chinese telecoms firm ZTE, with the NCSC writing to UK telecoms providers to warn that using the firm's equipment and services could pose a national security risk. There have also been multiple reports of cyber-attacks targeting the power stations and electrical grids. The US blamed Russia for a recent strike on its electrical grid, while the NCSC held the Kremlin responsible for several attempts to disrupt UK infrastructure. The damage can be considerable, but not all cyber-assaults focus on attacking systems directly. Many, especially those from Russia, aim to disrupt other nations for political gain through disinformation campaigns such as fake news.

The first requirement of the UNSC is to discuss what constitutes an actual cyberattack. Delegates may implement the usage of various criteria such as the disturbance caused in the networks of the victim, the amount of information stolen or siphoned off, the value of

the information at risk, the severity and scale of the cyber-attack itself etc. In this guide, we have given some examples of what we consider to be devastating cyber-attacks on organisations and on Nation-States. The attacks to be discussed are not limited to this list and are meant to help delegates identify the markers constituting a cyber-attack. Delegates are encouraged to do extensive research on cyber-attacks, both past and ongoing, and understand their function and causation.

Moreover, delegates are expected to draft solutions as to how we can deter such attacks and propose means by which we develop and implement extensive cyber-defensive capabilities which can stop the ever growing stockpile of offensive cyber weapons. We must also aim to protect the privacy of the people at risk of such attacks as during majority of cyber-attacks, copious amounts of sensitive data and private information are released in easily accessible public forums. Cyber warfare and its strategies are explained below to give you some foreknowledge. The list of important cyber-attacks and the countries with powerful cyber arsenals is to serve as a starting point for your research on this agenda.

TYPES OF CYBER WARFARE

Espionage

Drawing from the Cambridge Analytica case as well as from Edward Snowden of WikiLeaks, hackers can spy on government networks and glean restricted information that is not meant for public eyes. In this form of warfare, hackers gather information which is pivotal to their opponents and use it to directly attack the persons involved. Other means such as malware and spyware are malicious softwares by which hackers can obtain information without user knowledge. Such software transmits every bit of information, from files stored in personal computers to entire databases stored in a corporation's mainframe.

Sabotage

With the internet being an easily available and accessible commodity, many of the public services now have their operative systems and data banks stored and functioning online which include, among many others, water, electric power grids, and fuel infrastructures. Communication and military satellites along with computers divert a significant amount of online traffic and information which in turn makes them exploitable components of a bigger, more sophisticated system. These vulnerabilities can then be used to cripple civilian and military services of an entire nation state or be used to destroy an opponent's organisation. One of the frequently used attacks is the *'Denial-Of-Service'.* This form of sabotage is an attempt to block off all access to a system or network from its intended user. These are usually attempted on important web servers such as banks, credit card payment gateways, etc. These may not necessarily be computer-based attacks and can be physical attacks on communication lines as well.

Propaganda

Cyber propaganda is mainly use as a medium of psychological warfare, as means to influence the opinion of the general public. This includes the use of social media, the installation of fake news sites, and taking control over any form of information. This is mainly used to manipulate perceptions and perspectives in such a way that the audience affected reacts in a way desirable to the hacker propagating the information in the first place. This can be used to bring down a

person's faith or trust for a certain entity, for example, the nation's military, which would in turn create ripples of distrust within a community for their own military.

Questions:

- Is it possible to implement awareness programs within worldwide communities so as to inform and caution them against cyber attacks?
- Taking propaganda into account, are there checks we could perform for falsified or misleading cyber propaganda?
- Is it possible to take public utilities and system operations completely off the grid such that they cannot be tampered with?

USES OF CYBER WARFARE

Military

Currently, the National Atlantic Treaty Organization (NATO) holds a strong stance against cyber attacks. Member states created a cyber defense policy in 2008 after the 2007 attacks on Estonia. 33 NATO is a leader in creating international policy to protect against cyber attacks, and consenting members are already familiar with their successful defense strategies. However, they still lack procedure in reference to non-state actors. The International Court of Justice (ICJ) previously ruled on matters involving cyber networks. The type of interstate force prohibited expanded to "any use of force, regardless of the weapons employed." 34 This expands the traditional definition of a weapon to include using cyber means to inflict harm.

Civil

This mainly includes internet sabotage by hacking into the data communication lines and networks and web servers, client databases. Anything which is capable of accessing the internet is prone to cyber-attacks. Financial databases, electrical grids, and other public amenities with their systems online are also prone to cyber warfare. This can also be used to defraud individuals such as politicians by political or corporate sabotage and espionage.

Hacktivism

This is a tool used by hackers not to manipulate opinion or destroy for material gain, but to draw attention to their propaganda or to a serious issue at hand. Usually politically motivated, hackers hack into the network or system of the network and draw attention by well publicised disturbances in the hacked network. They are often portrayed as cyber-terrorists due to the use of blackmail, release of private information, and the huge disturbances they create on websites.

Private Sector

Cyber warfare in the private is sector is used for defensive more than offensive purposes. Hackers are mostly financially motivated to hack into the networks of international corporations and organisations so as to find information to be used for blackmail, corporate/industrial espionage and sabotage etc. But due to the millions of unsuccessful attempts of cyber warfare on the private sector on a daily basis, they usually pass unnoticed, are not reported in, and do not warrant media attention.

THREATS POSED BY CYBER WARFARE

New Domain of Warfare

In addition to the domains of land, air, sea, and subsea, warfare now also occupies cyberspace in

a very integral way. This harsh truth has many unwelcome consequences in terms of military laws and training facilities, materials, military operations, army personnel requirements and so on. Most importantly, it adds a significant challenge to the reality of simultaneous multi-domain warfare.

Extensive Coverage

In any case of cyber warfare, whether it is being used against military or corporations, civilians also come under the attack radius as attacking any resource affects anyone who uses it. For eg, a malware does not differentiate between a military computer and a civilian one. It infects every system software it comes in contact with, and can effectively shut it down which would result in the complete failure of critical healthcare systems among others, resulting in civilian casualties and loss of life.

Difficulty in Identification

In cyber warfare, it is considerably difficult to identify the entity or individual behind the attacks as your online presence can be masked from everyone while engaging in cyber warfare. This makes cyber weapons more dangerous as in real life we can trace who attacked first. However, in cyber warfare this is not possible due to the usage of proxies to mask online traffic. This leads to no accountability as the perpetrator has not been identified, either as a government agent or otherwise, which leads to no action being taken against said entity or individual. Without identification, deterrence and mutually assured destruction are no longer viable options to end the cyber war. This way, if a nation-state isn't going to be held accountable for its actions, they would not be afraid to use the worst weapons in their cyber arsenal to shut down power grids or critical industrial system,

leading to great physical damage to their opponent's factories and cities. This would also result in tremendous loss of civilian life.

No Distinction Between War and Peacetime

Since the inception of cyber warfare, the clear cut line between peacetime and wartime has become increasingly blurred due to technological advancements. These advancements have progressed in such a way that our offensive cyber weapons are way ahead of the curve while our defensive options are left in the dust. Taking into account the fact that we still cannot identify the attackers, this will further deteriorate deterrence for the same and increase warfare in cyberspace. If our defensive capabilities are far outdone by our offensive, we will have no choice but to engage in offensive warfare ourselves.

Questions:

- What measures should be taken to deter the use of cyber warfare during peacetime?
- Is there a need to install a committee/panel which decides to what extent and impact should cyber warfare be used?
- Should restrictions and sanctions be implemented upon countries who are overly engaged in cyber warfare?

THE WORST CYBER ATTACKS SO FAR

Operation Shady Rat

One of the ongoing cyber-attacks, Operation Shady Rat is aimed at government organisations and businesses in 14 countries worldwide and has even affected international entities such as the United Nations. It operates through the breaching of cyber networks and systems and stealing data from the computer on which they operate. Dmitri Alperovitch, a computer security industry executive who named the attack, led the search for the source of the act of cyber war. Due to an exponential increase in the number of attacks in the days before the 2008 Summer Olympic Games in China, software analysts arrived at the conclusion that the Chinese government was behind the attacks.

WannaCry

Wannacry was a ransomware that was released on the 12th of May 2017. It enveloped the entire cyberglobe, having devastating effects on millions of targets, including public utilities and large corporations. Surprisingly, the ransomware temporarily brought down National Health Service hospitals and other medical facilities in the UK, disrupting emergency rooms, detaining critical medical procedures and putting at risk thousands of British patients. Despite being so powerful, Wannacry had large and exploitable flaws, including functions that software analysts effectively used as a kill switch to turn it harmless and stop its spread.. US officials later concluded with "moderate confidence" that the ransomware was a North Korean government project gone awry that had been intended to raise revenue while wreaking havoc. In its entirety, WannaCry made away with almost 52 bitcoins, or about $130,000—which is trivial compared to past cases. WannaCry's extensive spread was mainly due to the leaked Shadow Brokers Windows vulnerabilities, EternalBlue. Microsoft had released the MS17-010 patch for the flaw in March, but most organisations hadn't updated it and were therefore vulnerable to the WannaCry infection.

Titan Rain

A code name given to a string of cyber-attacks in the early 2000s, Titan Rain infiltrated American computer systems, and was mainly targeting the major contractors of the Department of Defense department. These included some prestigious organisations such as Redstone Arsenal, NASA, and Lockheed Martin. The attacks were in the form of espionage through which the hackers were able to glean private data and sensitive information from the networks and the systems. Through investigations into the cyber-attacks, the Chinese government was found guilty of having ordered the attacks, a statement that the Chinese denied. Numerous other erratic attacks were targeted towards the British Ministry of Defense which further created some tension and caused strain in the foreign relations between China and the UK.

Macron Campaign Hack

During the final days of the run up to France's presidential runoff in May 2017, hackers leaked a huge cache of siphoned emails from the political party of the left-leaning forerunner and current President Emmanuel Macron. The leak was planned in such a way that it gave minimal time and restrained ability to respond, which was problematic since French presidential candidates are prohibited from making public announcements and speeches beginning two days before the final election. However, the Macron campaign did do a press release saying that the En Marche! party had been infiltrated, while warning the general population that not everything in the leaked emails was fact. An advantage that Macron possessed was that after observing the cyber-attack that deteriorated Hillary Clinton's political campaign, he had prepared for possible attacks. Investigators recovered proof that the Russian- government-linked hacker group called Fancy Bear did try to attack the Macron campaign earlier in March. Sometime after the email leak but before the elections, the Macron campaign said in a statement, "Intervening in the last hour of an official campaign, this operation clearly seeks to destabilize democracy, as already seen in the United States' last presidential campaign. We cannot tolerate that the vital interests of democracy are thus endangered."

The 2007 Estonia Cyber Attacks

On the 27th April, 2007, a continuous chain of cyber-attacks was targeted at Estonia on a scale never seen before. This act of cyber warfare froze the computer networks and systems in the Parliament of Estonia, government ministries, banks, and media outlets. This was a form of retaliation for the decision taken by the Estonian Government to relocate the Bronze Soldier of Tallin as well as the war graves in the capital. The first action taken by Estonia was to assign the blame on the Russian Kremlin, a blame which was later rescinded due to it being baseless. Following the incident, the Estonian government increased investments in the field of cyber-security and drafted up the Tallin Manual on the International Law Applicable to Cyber Warfare which outlines international laws on cyber warfare.

Google China hit by cyber attack (2009)

In mid-December 2009, Google's Chinese head office had found a security breach. Through this cyber-attack, hackers accessed numerous Google corporate servers and much sensitive data and intellectual property was stolen. Involving the Chinese government, Google

posted on a blog that it had "evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists". After further investigation, the company discovered that various Gmail accounts of users from the US, China, and Europe had been accessed without prior permission. As these emails belonged to advocates of human rights in China, the first and main suspect was the Chinese government as they had been ignoring human rights in China for years. The reason Google was in China was to extend its market through www.google.cn in 2006. However, after the cyber-attacks on their servers, Google reconsidered its stance in China and in the March of 2010, Google relocated its servers based in China for google.cn. They moved to Hong Kong so as to not get monitored by China's internet filtering policy.

Questions:

- Can cyber warfare continue as far as to ensure Mutually-Insured-Destruction (MAD)?
- How do we propose adequate defensive means if the current means are far outstripped by present offensive weapons?
- Are there non-cyber ways through which we can mitigate the exponential rise in cyber-attacks?

COUNTRIES WITH EXTENSIVE CYBER-OFFENSIVE CAPABILITIES

United States

2001-2015

Target: The World

From what was gleaned from the leaked documents by Edward Snowden, the NSA's capabilities are very extensive, and inform us about a humongous hacking operation aimed at undermining the Internet's infrastructure.

Outcome: A huge rise in global paranoia and a great reduction in cyber security for all.

2007: A ransomware called the Stuxnet was launched by the US to sabotage Iran's nuclear arsenal.

Outcome: The ransomware succeeded in temporarily setting back Iran's advancements on their nuclear program. The attack also defined cyber warfare at the time, making it a common means by which countries could launch cyber-attacks to end political disputes.

China

2009–2011: The Chinese were blamed for the cyber-attacks on Google, RSA Security, and other corporations from whom sensitive information and source code data was stolen.

Outcome: The hackers who infiltrated the network and systems of RSA Security made away with core data used in the company's two-factor authentication scheme favoured by governments and corporations.

2014: The Chinese infiltrated several databases and system networks used by the US Office of Personnel Management.

Outcome: The hacker's theft consisted of sensitive information such as Social Security numbers relating to more than 21 million people interviewed for government background checks.

United Kingdom

2009–2013: The UK breached the undersea cables of Google and Yahoo to steal unencrypted

traffic and data.
Outcome: After referring to the documents leaked by Edward Snowden, the UK not only accessed data of these companies but also that of major telecoms as well.

2012: The Communications Headquarters of the British Government infiltrated Belgium's networking systems to observe all cyber traffic passing through their routers.
Outcome: In spite of successfully breaching and accessing the network, the telecom wasn't able to clarify whether the hackers intercepted customer traffic.

Israel

2014: Israel had a sledge of allegations against them from the Russian government regarding their supposed infiltration into Russian security firm Kaspersky Lab to gather information on its research about nation-state attacks. It also attacked locations in Europe where the UN Security Council met to negotiate Iran's nuclear program.
Outcome: The hackers may have got data about Kaspersky's research.

2012: Israel was suspected of attacking the Iranian Oil Ministry and the National Iranian Oil Company with the Wiper attack.
Outcome: The malware wiped hard-drive data, then erased system files, causing the machines to crash and preventing them from rebooting. Iran insisted it had data backups.

North Korea

2014: Sony Pictures Entertainment was paralyzed by an attack. The US attributed the action to North Korea and applied additional economic sanctions against the country and specific officials.
Outcome: The attackers nabbed gigabytes of internal data and communications, which they later posted online.

2013: Computers in South Korea were struck by a logic bomb that caused data deletion and prevented rebooting. South Korea blamed North Korea for the attack but never produced solid evidence.
Outcome: Two broadcast media companies and at least three banks were affected.

Iran

2012: Iran allegedly launched a virus called Shamoon against oil conglomerate Saudi Aramco's computers. US officials blame Iran for the attack but have never produced evidence.
Outcome: Shamoon wiped data from some 30,000 machines and destroyed system files, preventing reboots.

2011–2012: Iran launched a series of denial-of-service attacks on US banks. Though Izz ad-Din al -Qassam Cyber Fighters took responsibility, US officials claimed Iran was retaliating for Stuxnet and UN sanctions.
Outcome: The attacks consumed resources, but no long-term damage was reported.

Russia

2014: Russia allegedly hacked the US State Department and the White House.
Outcome: The attackers had access to unclassified emails for President Obama as well as non-public details about his schedule.

2015: Russia reportedly hacked TV5Monde, a French-language broadcaster. A group calling itself the CyberCaliphate took credit, but French officials have pointed the finger at Russia.

Outcome: The hackers blacked out broadcasting for several hours and posted messages expressing support for ISIS to the TV channel's social media accounts.

Questions:

- Can we limit the use of Cyber warfare by Nation-States only to the respective militaries?
- Can we expect Nation-States to return previously stolen information and data taken from opposing Nation-States?
- Can Nation-States explore the possibility of sharing their cyber-capabilities, as done with their nuclear arsenal?

CONCLUSION

These example cover all of the aspects of cyber warfare we need to understand and resolve. This agenda is of utmost importance in an age where almost any information can be accessed on a server open to hundreds of millions of people. As peacekeepers of this generation of humanity, we need to develop modern ways to defend the people from the very same technology we have developed. We need to understand the fact that cyber warfare is one form of war which is being fought in our homes right now on our laptops and internet accessible devices and can affect us gravely as well. Hope to have a meaningful and heated debate on this issue with a united front in mind.

REFERENCES AND FURTHER READING

- http://knowledge.wharton.upenn.edu/article/the-secret-history-of-cyber-war/
- https://searchsecurity.techtarget.com/definition/cyberwarfare
- https://www.huffingtonpost.com/entry/david-petraeus-cyber-war_us_58da8731e4b0286e65b5f70e
- https://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#5b5b354f44ce
- http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/
- https://archive.nytimes.com/www.nytimes.com/cfr/world/slot1_20080227.html?_r=3
- https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/
- https://www.wired.com/story/2017-biggest-hacks-so-far/
- https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#62ec5aa61c78
- https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/

GUIDELINES FOR DELEGATES

Discussing other Failed States:

the number of nations that can be discussed in committee are not limited to the above list. Delegates are free to discuss other nations that they believe classify as failed states (whether currently or previously). However, delegates are required to first ask the Executive Board permission for discussing other states they seem pertinent to the discussion. This is to ensure that discussion remains on topic and does not deviate from the agenda. After getting confirmation from the Executive Board, the delegate may discuss the particular nation.

Foreign and Domestic Policy:

Delegates are expected to thoroughly read about their representative countries and know their domestic and foreign policy. All comments and statements made in committee should be in accordance to the various policies. Any statement made that violates the member nation's policy will be looked down upon and the delegate would be marked down heavily.

Pragmatic Solutions

Solutions proposed by delegates are also expected to be pragmatic and realistic rather than idealistic. Delegates must realize that the world they inhabit has a lot of problems and obstacles that need to be overcome. Thus, delegates should ensure that any solution proposed by them is realistic and pertinent in the real world.

Concrete Solutions

All solutions that are proposed by delegates need to be planned out and should be specific. Any vague proposal will be looked down upon and delegates are expected to work on how their solutions will work on the ground level. Extensive research must be done by delegates to make sure that their solutions have the necessary details any policy action requires.

Programmes

Delegates are required to research on previous and ongoing on-ground projects run in various organizations and governments. They should know about the working of these organizations and how much they have been able to accomplish. They are required to refer to these projects when making solutions.

POSITION PAPER GUIDELINES

Position papers are usually one to one-and-a-half pages in length. Your position paper should include a brief introduction followed by a comprehensive breakdown of your country's position on the topics that are being discussed by the committee. A good position paper will not only provide facts but also make proposals for resolutions.

A good position paper will include:

- A brief introduction to your country and its history concerning the topic and committee;
- How the issue affects your country;
- Your country's policies with respect to the issue and your country's justification for these policies;
- Quotes from your country's leaders about the issue;
- Statistics to back up your country's position on the issue;
- Actions taken by your government with regard to the issue;
- Conventions and resolutions that your country has signed or ratified;
- UN actions that your country supported or opposed;
- What your country believes should be done to address the issue;
- What your country would like to accomplish in the committee's resolution; and
- How the positions of other countries affect your country's position.

SAMPLE DRAFT RESOLUTION

Draft Resolution GA/3/1.1

General Assembly Third Committee

Authors: United States, Austria and Italy
Signatories: Greece, Tajikistan, Japan, Canada, Mali, the Netherlands and Gabon
Topic: "Strengthening UN coordination of humanitarian assistance in complex emergencies"

The General Assembly,
Reminding all nations of the celebration of the 50th anniversary of the *Universal Declaration of Human Rights*, which recognizes the inherent dignity, equality and inalienable rights of all global citizens, **[use commas to separate perambulatory clauses]**

Reaffirming its Resolution 33/1996 of 25 July 1996, which encourages Governments to work with UN bodies aimed at improving the coordination and effectiveness of humanitarian assistance,

Noting with satisfaction the past efforts of various relevant UN bodies and nongovernmental organizations,

Stressing the fact that the United Nations faces significant financial obstacles and is in need of reform, particularly in the humanitarian realm,

1. Encourages all relevant agencies of the United Nations to collaborate more closely with countries at the grassroots level to enhance the carrying out of relief efforts; **[use semicolons to separate operative clauses]**
2. Urges member states to comply with the goals of the UN Department of Humanitarian Affairs to streamline efforts of humanitarian aid;
3. Requests that all nations develop rapid deployment forces to better enhance the coordination of relief efforts of humanitarian assistance in complex emergencies;
4. Calls for the development of a United Nations Trust Fund that encourages voluntary donations from the private transnational sector to aid in funding the implementation of rapid deployment forces;
5. Stresses the continuing need for impartial and objective information on the political, economic and social situations and events of all countries;
6. Calls upon states to respond quickly and generously to consolidated appeals for humanitarian assistance;
7. Requests the expansion of preventive actions and assurance of post-conflict assistance through

PREAMBULATORY AND OPERATIVE CLAUSES

Preambulatory Clauses

The preamble of a draft resolution states the reasons for which the committee is addressing the topic and highlights past international action on the issue. Each clause begins with a present participle (called a perambulatory phrase) and ends with a comma. Perambulatory clauses can include:

- References to the UN Charter;
- Citations of past UN resolutions or treaties on the topic under discussion;
- Mentions of statements made by the Secretary-General or a relevant UN body or agency;
- Recognition of the efforts of regional or nongovernmental organizations in dealing with the issue; and
- General statements on the topic, its significance and its impact.

Affirming	Expecting	Having examined
Alarmed by	Emphasizing	Having received
Approving	Expecting	Keeping in min
Bearing in mind	Expressing it's appreciation	Noting with deep concern
Believing	Fulfilling	Nothing with satisfaction
Confident	Fully aware	Noting further
Contemplating	Emphasizing	Observing
Convinced	Expecting	Reaffirming
Declaring	Expressing it's appreciation	Realizing
Deeply concerned	Fulfilling	Recalling
Deeply conscious	Fully aware	Recognizing
Deeply convinced	Further deploring	Referring
Deeply Disturbed	Further recalling	Seeking
Deeply Regretting	Guided by	Taking into consideration
Desiring	Having adopted	Taking note
Emphasizing	Having considered	Viewing with appreciation

Operative Clauses

Operative clauses offer solutions to issues addressed earlier in a resolution through the perambulatory section. These clauses are action oriented and should include both an underlined verb at the beginning of your sentence followed by the proposed solution. Each clause should follow the following principals:

- Clause should be numbered;
- Each clause should support one another and continue to build your solution;
- Add details to your clauses in order to have a complete solution;
- Operative clauses are punctuated by a semicolon, with the exception of your last operative clause which should end with a period.

Accepts
Affirms
Approves
Authorizes
Calls
Calls upon
Condemns
Confirms
Congratulates
Considers
Declares accordingly
Deplores
Designates
Draws the attention
Emphasizes
Encourages
Endorses
Expresses its appreciation
Expresses its hope
Further invites
Deplores
Designates
Draws the attention
Emphasizes
Encourages
Endorses
Expresses its appreciation
Expresses its hope
Further invites
Further proclaims
Further reminds
Further recommends
Further requests
Further resolves
Has resolved
Notes
Proclaims
Reaffirms
Recommends
Regrets
Reminds
Requests
Solemnly affirms
Strongly condemns
Supports

Bibliography

Sample Draft Resolution: http://www.unausa.org/global-classrooms-model-un/how-to-participate/model-un-preparation/resolutions/sample-resolution#sthash.15LEikZY.dpuf
Preambulatory and Operative Clauses: http://www.unausa.org/global-classrooms-model-un/how-to-participate/model-un-preparation/resolutions/preambulatory-and-operative-

THE DOON SCHOOL,
Mall Road,
Dehradun—248001,
UK, India
Phone: +919760013831
e-Mail: chair.odc@doonschool.com
dsmun@doonschool.com
Website: www.dsmun.com