Background Guide

# WSOMUN

GEMS Wellington Academy Model United Nations
March 22nd - 24th

## COMMITTEE: UNGA1 - DISEC

*Lead The Change…*

# Welcome Letter from the Secretary General

Distinguished delegates of the General Assembly First Committee,

It is my absolute honor to invite you to the second largest high school Model UN in the country; the first edition of the WSO Model United Nations conference held at the GEMS Wellington Academy - Dubai Silicon Oasis. I am beyond ecstatic and humbled to serve in the capacity of Secretary-General for this year's conference. In order to ensure that our conference's quality is of the highest caliber on an international scale, we have set up ideals and standards that orient us towards our goal while also providing us with the dedication necessary to make a difference. Our conference aims to engage and encourage the youth to participate and to share their ideas and beliefs about different and various global issues. The aim of our conference is to give students a unique experience where they are able to harbour their diplomatic skills and explore current affairs through a simulation of the United Nations. We strive to help students foster skills necessary for every day life, and provide education beyond the desk as practice is the best way to process theory.

Everything changes; but change itself is the only thing that doesn't. Remembering that nothing remains the same and even in the worst situation we face, we can and should rely on the fact that change is the constant. Throughout the conference, our aim is to develop solutions to issues which we currently face and widen our vision, while using the idea of change to our advantage. WSO Model united nations possesses an unique ability to bring forth students from diverse backgrounds to collectively work towards a cohesive and united goal. WSOMUN welcomes young leaders to portray onto a platform, values to be abided by, in order to create a change in the international community.

To this end, the members of the Secretariat have been working painstakingly, around the clock, to ensure that you enjoy every breath of this conference experience. I assure you that the final step of this journey will draw a higher academic and organizational line to satisfy all your expectations.

Looking forward to welcoming you this March!

With Best Regards,
**Varsha Venkatraman**
Secretary General
WSOMUN 2018

# Welcome Letter from the Dias

Honorable delegates,

It is my distinct pleasure to welcome you to the Disarmament and International Security Committee at the GEMS Wellington Academy Model United Nations. Prepare yourselves for days of heated yet fruitful debates and being challenged as a delegate. You will have the opportunity to meet students of diverse backgrounds and have an all-around amazing experience, both in and outside of committee.

My co-Director and I have written this background guide as a foundation for your position papers. Although this guide includes much information on the general topics, it is still very important to research your country and its stance on both cyber warfare and threat of bioterrorism and improvised explosive devices. we hope that the creativity and thoroughness of these topics will stimulate your research and encourage innovative debate during your committees.

We expect each and every one of you to be well read, going beyond the background guide and give your very most proficiently adept at this conference. It is also important to remember that each country, whether directly or indirectly involved, has value and ideas to add to resolutions throughout committee. Looking at your country's history and laws will help you understand how you might respond to both topics. As most GAs, there will unavoidably be some scheming and politicking throughout committee sessions. However, I would like to emphasize that this should never trump substantive excellence and respect for other delegates. Furthermore, I believe that active participation and collaboration in committee tends to be the most rewarding experience in Model UN. My aspiration for this committee is that we are able to discuss these issues profoundly while having a blast. This may be the largest committee some of you have ever participated in, but the opportunity provided in such a committee of further refining your debate skills, in addition to the fun nature of DISEC, will make this a committee to remember.

We are very passionate about each topic, so don't hesitate to reach out and ask us questions! As the executive committee members, we are here for you. We want this to be a fun learning experience and hope you all will be ready to carpe diem. We are all counting down the days until the conference!

**Chair:** Sidharth Pramod
**Co - Chair:** Siddharth Nair
**Co - Chair:** Advait Sai

# United Nations General Assembly 1:
# Disarmament and International Security Committee

The First Committee deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime.

It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva- based Conference on Disarmament. It is the only Main Committee of the General Assembly entitled to verbatim records coverage.

**Source:** http://www.un.org/en/ga/first/

# AGENDA 1

# Responding to the threat of bioterrorism and improvised explosive devices

## Introduction to the topic

Improvised Explosive devices are explosives which are not essentially used for military purposes. They have various modes to be triggered and are used as roadside bombs, and by suicide bombers. On the other hand, Biological Weapons mainly take advantage of the incapacity of humans to defend themselves from dangerous diseases, toxins, or viruses. These have been used by people from different countries during the war. This usage is termed as Biological Warfare. The Biological Weapons do not need any specific knowledge or any strategies for deploying the weapons effectively. They can kill 1000's of civilians in one attack. This simple usage of Biological weapons and Improvised Explosive devices has provided terrorists with a huge leap.

Several notable instances of the usage of Improvised Explosive Devices include The Manchester Arena Bombing on May 22nd, 2017 with 23 injuries including the bomber himself. In case of Biological Weapons, countries like The Syrian Arab Republic have used these methods to control protests against the government. Several conventions and agreements have been formed to prevent the stockpiling and increased production of biological weapons. One such convention includes the Chemical Weapons Convention(CWC) which had taken the initiative to extend the Geneva Protocol

to prevent the use and stockpiling of biological weapons. With regard to the usage of improvised explosive devices, due to the rapid increase in the usage of these types of devices, mainly due to its ability to kill several people at a time, there have been drastic changes in military priorities, tactics, and strategies. As a result, several countries are incurring enormous costs. These are extremely dangerous especially in countries like Afghanistan, Congo, Mali, Syria, and Somalia. These not only incur heavy costs for armies but also to several social organizations with the aim of reducing the threat to their own personnel. Hence, several countries have come together to prevent the problem of Improvised Explosive Devices and Stockpiling of several Biological Weapons.

## History of the topic

The Germans were the first to use biological weapons during the time of warfare to kill armies and a large number of people. These were later used by the Japanese as well, against the Chinese army. Since then, The Americans pressed on the French and The British to develop these weapons too. After the war, superpowers like The United States of America started developing these types of weapons to mainly counteract attacks from countries like Japan. Along with the USA, even the Soviet Union undertook several projects to develop biological weapons. This stockpiling of weapons included testing on animals, air tests, and tests on several volunteers. Currently, countries like Iraq, Iran, etc. are also stockpiling several biological weapons. Besides these governmental programmes, several non-governmental individuals and organizations have also got accessed to these weapons which have become a topic of major debate for several countries right now.

With regard to Improvised Explosive Devices(IED), they were used initially by the Irish Army with the help of agricultural fertilizers and other explosives like RDX, etc. Later they were widely used in The Iraq War. These included hiding these types of bombs behind traffic signals, etc. Several speculations include the development of these weapons with the help of leftover military ordnance.
Since then, terrorist organizations based in countries like Afghanistan, Pakistan, etc. have shown increased usage of these dangerous weapons.

## Discussion of the topic

Despite the signing of several Conventions and Agreements like The Chemical Weapons Convention(CWC) and the Biological Weapons Convention (BWC), there has been no proper limitation or action taken by these conventions. i.e. they have not executed their plans as such. Hence, several countries have initiated large-scale projects for the development of biological and chemical weapons. These countries include The United States of America, The Russian Federation, The People's Republic of China, etc. However, the main issue with this problem, currently, is that several nations do not abide by the conditions laid down by CWC or BWC. They violate some points in it to satisfy their own needs for the development of Biological Weapons. For example, The

Russian Federation does not provide much information about several major parts of their Biological Weapons Programme. First, they do not specify whether they have been used for peaceful purposes or not. Second, they do not provide enough reports and evidence of whether they have destroyed these weapons or not. These are clear violations of the BWC and are the main reasons for the current problem of stockpiling of biological weapons. Lastly, there are no proper countermeasures present to defend people or armies from these types of attacks in the future or the necessary information to determine a potential threat.

The problems associated with Improvised Explosive are becoming a huge matter of concern for the international world, because of the increased number of deaths around the world each year because of these explosives. Even when the terrorist organizations based in Afghanistan, etc. are wiped out by The United States of America, there would not be any massive reduction in the usage of these devices because of the fact that they are extremely easy to make. There has not been enough money spent on developing methods to counteract the problems associated with these devices. In addition, there is lack of important data required for the detection of an IED detonation well before time.

Hence, the Dias expects the delegates to be prepared with solutions and important points dealing mainly with the stockpiling of Biological Weapons and lack of any measures against the usage of Improvised Explosive Devices.

## Bloc Positions

With regard to the Topic Associated with the Improvised Explosive Devices, several countries share the same stance, i.e. to prevent the detonation of such dangerous devices in order to maintain international peace and security. However, the main distinction between different countries is how swiftly different countries are taking actions against these weapons. For example, since The United States of America has had the maximum number of casualties both outside America and inside America, they have been trying to determine different measures to counteract this problem. Another factor to be considered here is the effectiveness of these solutions. For instance, USA has been swift in taking action, but have not come up with effective solutions.

When considering the topic of Biological Warfare, delegates need to determine to what extent different countries abide by the BWC and CWC agreements. For instance, The Russian Federation does not provide any specific evidence of proper disposal of biological weapons. On the other hand, The Republic of India has not faced any accusations like that before.

Delegates need to be aware of these points during the conference in order to form proper blocs and intensify the debate.

## Questions to consider

1. What is your country's stance on these issues?
2. Does your country look favorably upon initiating programs that involve stockpiling of biological weapons?
3. Does your country have biological weapons?
4. If yes, do they abide by the Terms set up by International Agreements like BWC and CWC?
5. Has your country ever used biological weapons?
6. How many people have been killed because of Improvised Explosive Devices (Quantitatively)?
7. What type of solutions has your country come up with to combat these issues?
8. What type of solutions will you (as delegates) come up with to resolve these issues?

## Further Research

1. https://www.armscontrol.org/factsheets/cbwprolif
2. https://www.ncbi.nlm.nih.gov/pubmed/24436060
3. https://www.un.org/disarmament/convarms/ieds/
4. https://www.brookings.edu/articles/the-evolution-of-improvised-explosive-devices-ieds/

## Bibliography


1. "Countering The Threat of Improvised Explosive Devices." National Research Council of the National Academics, Web. 04 Mar. 2018.
2. McKenzie, K. (2001). The Rise of Asymmetric Threats: Priorities for Defense Planning. Quadrennial Defense Review. Retrieved December 13, 2006, from http://www.ndu.edu/inss/press/QDR_2001/sdcasch03.html.
3. Singer, Peter W. "The Evolution of Improvised Explosive Devices (IEDs)." Brookings. Brookings, 28 July 2016. Web. 04 Mar. 2018.
4. "Improvised Explosive Devices." North Atlantic Treaty Organization, 20 Nov. 2015. Web. 4 Mar. 2018.
5. "Improvised Explosive Devices (IEDs) – UNODA." United Nations. United Nations, n.d. Web. 04 Mar. 2018

# AGENDA 2

## Establishing Security Strategies for Countering Cyber Warfare in Digital Age

## Introduction to the topic

Cyber warfare can be defined as ‘the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes’.

While cyber warfare is nowhere near as detrimental as the problems usually discussed in the DISEC, it is imperative to note that this threat is a unique and difficult one to diffuse. What complicates the issue just like every other is that it is one with multiple stances: when some welcome cyber warfare for its method of attack due to the significantly fewer casualties there are others who don’t share the same opinion.

What makes cyber warfare a unique threat is its ability to throw a state into turmoil, thereby creating a dissent for the government among its citizens by ridding them of basic necessities to a large extent. The belligerent nature of cyber warfare knows no limits, it could breach the security of a state, manipulate and steal data and even access the nuclear launch codes resulting in havoc and destruction.

## History of the topic

Since the 1980s, various states such as: Estonia, Canada and Georgia, have fallen prey to cyber warfare. There have been serious incidences of hacking that have had the potential to have serious consequences like destruction and military disasters.

In April 2007, the Estonian Government was hacked by unknown foreign intruders, who were later identified to be of Russian origin. Later, in June, the email of the US Secretary of Defense was hacked and used to gain access to the government's data. In the following year, the U.S government was hacked by unknown intruders when in the process of electing a new President. These intruders hacked into the databases of both the Republican and the Democratic parties in the U.S to alter the outcome of the election.

In October, of the same year, the Chinese government reported that personal information from key Chinese governmental sectors was being stolen by foreign intruders. It was later diagnosed that that the intruders were of US and Taiwan origins.

In recent years, state actors have been alleged of attempting to steal military technology from foreign governments through cyber-attacks, many of which have been linked to China, Russia, the United States and the United Kingdom. With cybercrime being quite difficult to pinpoint, allegations have caused a rise in tensions and an increase in the number of attacks. Aside from the events involving state actors, the history of cyber warfare also includes the use of the same for corporate espionage, in an attempt to weaken rival companies.

Companies and state actors aren't the only targets of cyber-attacks. Nongovernmental organizations (NGOs), the United Nations, and other non-state actors have been known to experience cyber threats and attacks.

## Discussion of the topic

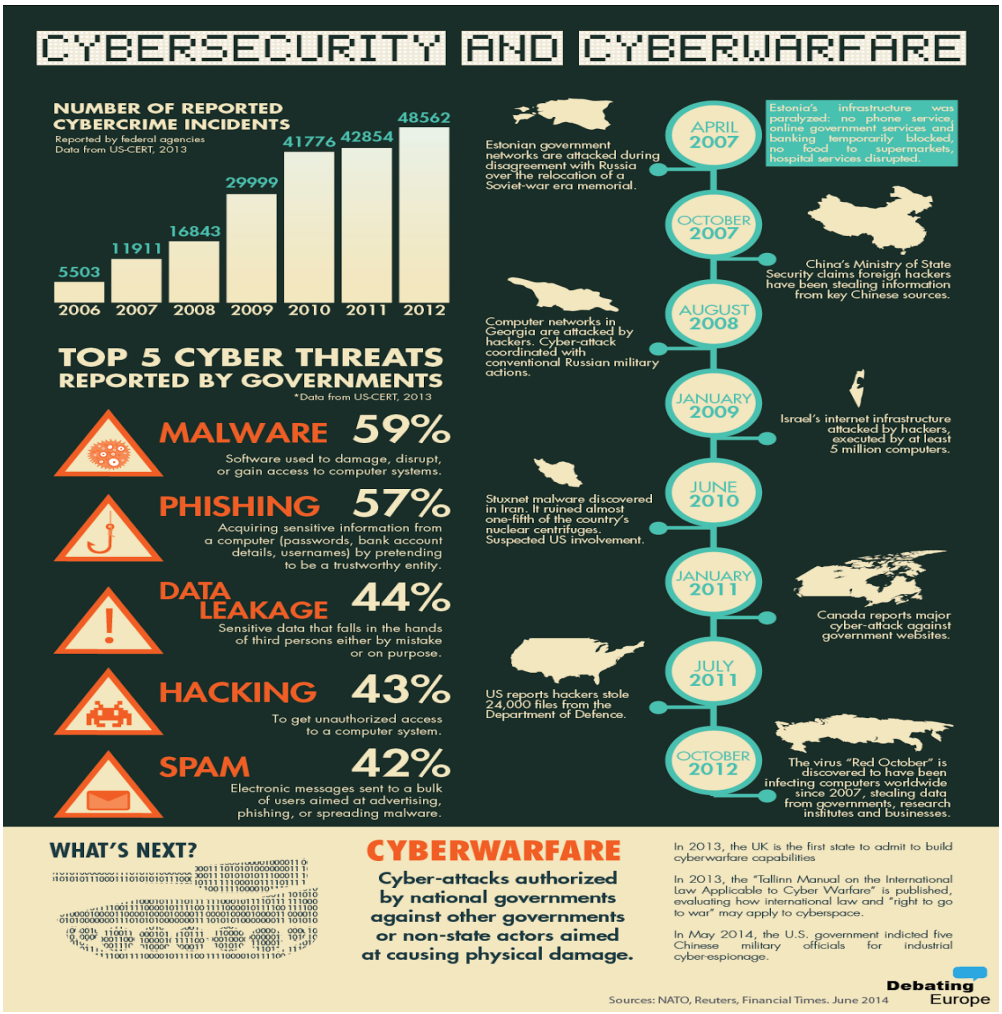
With the advent of the Internet, connectivity and online networking have proliferated across the globe. However, with an increase in the user base of the internet, there have been various non-state actors (NSAs) that have negatively influenced the users to act against governments, multinational companies and international organizations. These attacks often take place under complete anonymity and tracing the offenders becomes tough. Cyber terrorism has various aspects such as recruitment, incitement, finance and execution of sinister plans. These attacks are not just limited to terrorism and violence but also fraud and leaks of private data. While most of these hackings are conducted by non-state organizations, some state governments have also been accused of carrying out spying and illegal intelligence accumulating attacks. As reported by Sanger (2015), in 2013, the United States and the People's Republic of China accused each other of carrying out digital attacks

on the other. Unethical hacking and cyber-attacks have also been witnessed in many countries across the world for example; in 2010 a coded virus disordered the processing of Uranium in one of Iran's nuclear facilities. Owing to the wide accessibility of the internet, all countries and IOs are vulnerable to cyber-attacks, hacking and terrorism.


With both implicit ramifications such as leaks of sensitive and classified data and other, more explicit, consequences such as providing a platform on which to plan a terrorist attack, cyber-terrorism terrorism is an issue that concerns the entire international community including state governments, multinational companies and international organizations. International organizations such as the United Nations Office on Drugs and Crime (UNODC) have collaborated with the United Nations Counter-Terrorism Implementation Task Force in order to counter these cyber attacks. TOPIC 1 Establishing Security Strategies for Countering Cyber Warfare in Digital Age 9 The United Nations Counter Terrorism Strategy was adopted in 2006 by all member states to combat terrorism of different forms. However, a resolution that encompasses all aspects of terrorism has not yet been passed in the UN despite ongoing negotiations. According to the UNODC report, there have been various regional agreements such as the SAARC Convention on suppression of terrorism (1987), Arab Convention on Terrorism (1998), the European Union framework (2002) to combat terrorism, amongst various others. However, they have been largely unsuccessful in dealing with cyber-security issues.

## Bloc Positions

- Asia – Alleged to be the origin of most cyber-attacks, there is no clear position that it has. When countries like China have a dedicated part of their army that participates in the cyber-attacks there are countries like India that resort to cyber defense alone.




- Africa and Latin America – Africa and Latin America haven't been subject to any major cyber-attacks; however, countries in both these regions, taking into account their currently high vulnerability and their developing economic status, are looking to develop collective agreements and major policies in a step to be prepared.

- European Union (EU) and Northern Atlantic Treaty Organization (NATO) - The EU and the NATO have been leading blocs in trying to combat the threat of cyber warfare. Many of the countries within the same have adopted a collective security policy, which means that all the members follow the same set of regulations which allows easy monitoring of electronic services. In addition, the NATO and the EU have signed a Technical Arrangement on Cyber Defense.

## Questions to consider

1. How must Cyber Warfare be defined or how must its existing definition updated?
2. Should state sponsored cyber warfare be considered an act of war?
3. What measures must be taken to counter the same with respect to both state and non-state actors?
4. Must we accept cyber warfare as a component of modern conflict or must it be discouraged?
5. Must an international framework be established whose sole purpose is overlooking the same?
6. What actions must be taken to keep up with the technological advancements associated with cyber warfare?
7. Should countries be prevented from developing cyber warfare programs?

## Further Research

1. Cyber security and Cyber warfare-http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfarepreliminary-assessment-of-national-doctrine-and-organization-380.pdf

2. Making Sense of Cyberwar-https://www.belfercenter.org/publication/making-sense-cyberwar

3. The History of Cyber Attacks - a Timeline-https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

4. Cyber Warfare and International Law-http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

5. Cyber Resilience in the Digital Age-https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6

6. Threat Intelligence in the Age of Cyber Warfare- https://securityintelligence.com/threat-intelligence-in-the-age-of-cyber-warfare/