DISEC (DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE)- A STUDY GUIDE

The Disarmament and International Security Committee was established in 1993. It is the First and one of the main committees of the General Assembly. The role of DISEC is outlined in Chapter IV, Article 11 of the United Nations Charter which states, "The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and may make recommendations with regard to such principles to the Members or to the Security Council or to both". As per this article, the mandate of DISEC is highlighted as, "to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources".

AGENDA 1 – CYBER WARFARE

DISCUSSION OF THE TOPIC

At the very onset, the Executive Board for the DISEC would like to inform the delegates of this committee that country specific research is imperative for effective participation during the conference. In order to participate in an appreciable manner, it is hence imperative for the delegates to research well in relation **to** their country. Delegates must find out whether their country has been a victim of cyber terrorism, past international actions their country has taken in relation to the agenda under discussion and what measures have been suggested by the country to prevent cyber-terrorism. In case their countries have not taken any major steps or are not major parties to this issue of cyber-terrorism, delegates are suggested to come up with their own stance and participate accordingly. Let us first understand the basic meaning of cyber terrorism.

➢ A Basic Insight into recent incident has highlighted the lack of consensus internationally on what defines a cyber-attack, an act of war in cyberspace, or cyber terrorism. Cyber war is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. Cyber terrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies. Within each of these categories, different motivations as well as overlapping intent and methods of various actors can complicate response options. Criminals, terrorists, and spies rely heavily on cyber-based technologies harmonize laws across countries as to what constitutes criminal activity in the to support organizational objectives.

Existent International Conventions Related to Cyber Crime:

➢ Council of Europe Convention on Cybercrime the Council of Europe Convention on Cybercrime is the first international treaty to attempt to cyber realm. This law enforcement treaty, also known as the Budapest Convention, requires signatories to adopt criminal laws against specified types of activities in cyberspace, to empower law enforcement agencies to investigate such activities, and to cooperate with other signatories.

➢ United Nations General Assembly Resolutions A series of U.N. General Assembly resolutions relating to cyber security have been adopted over the past 15 years. One resolution called for the convening of and a report from an international group of government experts from 15 nations, including the United States. The stated purpose of this process was to build "cooperation for a peaceful, secure, resilient and open Information and Communication Technology (ICT) environment" by agreeing upon "norms, rules and principles of responsible behaviour by States" and identifying confidence and capacity-building measures, including for the exchange of information. In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society (WSIS) to discuss information society opportunities and challenges. Delegates from 175 countries took part in the first summit, where they adopted a Declaration of Principles—a road map for achieving an open information society. An international treaty banning cyber warfare and/or information weapons has been proposed in the United Nations by Russian and German delegations. Preferring a normative approach over an arms control styled regime, the United States may wish to reserve its right to develop technologies for countermeasures and reconnaissance against potential cyber foes, particularly those acting outside the boundaries of a state system.

➢ International Telecommunications Regulations the International Telecommunication Union (ITU) regulates international telecommunications through binding treaties and regulations and nonbinding standards. Regulations prohibit interference with other nations' communication services and permit control of non-state telecommunications for security purposes. The regulations do not, however, expressly forbid military cyber-attacks. Also, ITU apparently has little enforcement authority.

➢ Other International Law Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cyber security; for example by prohibiting the disruption of air traffic control or other conduct that might jeopardize aviation safety. Bilaterally, mutual legal assistance treaties between countries may be applicable for cyber security forensic investigations and prosecution.

Questions to consider during research. It is imperative that the following five questions be answered by all delegates during their research process before the MUN:

➢ Does your nation have an effective framework to tackle cyber warfare?

➢Has your nation or any of its allies been a victim of cyber warfare in a big way?

➢ How open is the Internet in your country? Are various sites restricted in your nation? E.g. various social media sites are banned in China

➢Is your nation a signatory to any international conventions related to cyber security?

➢ Have any citizens of your country joined extremist organizations in the Middle East like the ISIS or Al Nusra?

Apart from this, research in relation to different aspects covered in the study guide and those that are specific to your country must also be carried out for effective participation during the MUN conference.

AGENDA 2- DENUCLEARIZATION OF ARMS

DISCUSSION OF THE TOPIC

The United Nations Charter, in its first article, defines that one of the purposes of the United Nations is "to maintain international peace and security". The promotion of a more peaceful world was the very reason the United Nations was created in the first place. The proliferations of Nuclear Weapons are a threat to world peace in every way, they are the most dangerous weapons on earth and the dangers from such weapons arise from their very existence. Fear of the bomb motivated the first atomic program and the allure of the bomb's power later propelled national leaders to start building their own arsenal, making them larger every time. In today's world, there are over 15,000 nuclear weapons in existence, enough to destroy the world many times over. Nonetheless, there are many barriers the International Community faces when trying to stop the proliferation and start the denuclearization of Nations across the world. States that already have Nuclear weapons keep investing in maintaining and expanding their nuclear arsenals while other States still try to acquire them, motivated by their perception of security or by the desire for symbols of power and control. Even though there are several treaties and conventions that attempt to stop the proliferation of those weapons, the UN

desperately needs to find a way to contain and decrease the number of nuclear arsenals worldwide effectively.

2019 estimated warhead inventories:

1. **RUSSIA-6490**
2. **USA-6185**
3. **FRANCE-300**
4. **CHINA-290**
5. **UK-200**
6. **PAKISTAN-160**
7. **INDIA-140**
8. **ISRAEL-90**
9. **NORTH KOREA-30**

Reference links- AGENDA 1 (for the delegates):

https://www.un.org/press/en/2014/gadis3512.doc.htm

https://www.unsystem.org/content/action-cybersecuritycybercrime

Reference links- AGENDA 2 (for the delegates):

https://www.armscontrol.org/ACT/2016_03/Features/Burying-the-Hatchet-The-Case-for-a-Normal-Nuclear-South-Asia

https://thebulletin.org/roundtable/how-to-reduce-south-asias-nuclear-dangers/

BIBLIOGRAPHY

https://www.aljazeera.com

https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat