DIYAFAH INTERNATIONAL SCHOOL L.L.C

مدرسة ضيافة الدولية ذ.م.م

NURSERY حضانة

DISMUN 2025 | UNITED NATIONS SECURITY COUNCIL

STUDY GUIDE 2025

United Nations | Security Council

SECURITY COUNCIL
BACKGROUND GUIDE 2025

Dear Distinguished Delegates,

Welcome to the 2025 Diyafah International Model United Nations Conference (DISMUN-Abu Dhabi)! We are pleased to welcome you to the Security Council. This year's chair is ***Eden India Franks,*** who is currently in Year 13. This year's Deputy Chair is **Amina Irfan,** who is currently in Year 10.

The topic under discussion for the Security Council is:

Cyber Defence

The Security Council is comprised of five permanent members and ten non-permanent members. The five permanent members of the Security Council are China, France, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. Every year, the General Assembly elects five of the 10 non-permanent members for a two-year term.

We hope our delegates can utilize this background guide, as it introduces the topics for this committee. We urge you all to recognize that this guide is not meant to replace further research. We applaud and highly encourage in-depth research into your member state's policies and the use of the annotations to further your knowledge on these topics.

On the DISMUN webpage, you will find two resources that are essential to your preparation for the conference and as a reference during committee sessions. The DISMUN Handbook, explains each step in the delegation process from preconference research to the committee debate and resolution drafting processes. *Delegates should not discuss the topics or agenda with other members of their committee until the first committee session,* we urge our delegates to be respectful of this request.

In addition, review the mandatory DISMUN Conduct Expectations on the DISMUN website. They include the Conference dress code and other expectations of all attendees. DIS wants to emphasize that any instances of *discrimination based on race, gender, national origin, religion, age, or disability* will not be tolerated.

If you have any questions concerning your preparation for the committee or the Conference itself, please contact Communications.DISMUN@diyafahinternationalschool.com

We wish you all the best in your preparations and look forward to seeing you at the Conference!

Chair ***Eden India Franks***

Deputy Chair ***Amina Irfan***

Overview

Committee History

Introduction

Governance, and Structure

Membership

Presidency

Participation

Voting

Mandate, Functions, and Powers

Recent Sessions and Current Priorities

Conclusion

Committee Overview

Committee History

"One place where the world's nations can gather together, discuss common problems and find shared solutions."

Introduction

The **United Nations Security Council** is one of the six primary organs of the United Nations, mandated by the *Charter of the United Nations* to maintain international peace and security. The Council submits an annual report to the General Assembly.

After the devastating effects of two world wars, the international community decided to establish the United Nations (UN) (as an intergovernmental organization) with the primary responsibility of maintaining international peace and security, creating the conditions conducive to economic and social development, while advancing universal respect for *human rights*. The Security Council was established as one of its six principal organs and was given the primary responsibility to preserve *international peace and security*.

The Security Council held its first session on 17 January 1946, at Church House in London. After its first meeting, the Council relocated to its permanent residence at the UN Headquarters in New York City. At that time, five permanent members and six non-permanent members comprised the membership of the Council. However, over subsequent years, discussions regarding the structure of the Council began to take place. In 1965, the number of non-permanent members increased to ten, and although membership has not changed since, discussions regarding a change in configuration take place frequently.

Governance, and Structure

The Security Council is the only UN entity that has the power to adopt resolutions that are *binding* on Member States. In accordance with Article 25 of the *Charter of the United Nations* (1945), Member States are obliged to accept and carry out the Council's recommendations and decisions. The Security Council also has a variety of tools to address issues on its agenda. For example, the President of the Security Council may issue press statements or presidential statements to communicate the position of the Council. Although these other tools are not legally binding, they nonetheless bring attention to important issues and compel the members of the Security Council to make recommendations and resolve conflicts.

Membership

The Security Council is comprised of five permanent members and ten non-permanent members, now. The five permanent members of the Security Council are China, France, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. Every year, the General Assembly elects five of the 10 non-permanent members for a two-year term. Elections for non-permanent seats on the Council can be competitive, with countries expressing interest years in advance. Countries elected to serve on the Security Council are expected to represent the interests of their region; they usually have an influence at the international level and demonstrate leadership in specific areas of interest (to their foreign policy). Security Council elections for non-permanent members are held in June, six months before the term starts. This change allows Member States ample time to prepare for their new role.

Presidency

Each member of the Security Council holds the presidency of the Council for one month, rotating according to alphabetical order. Security Council meetings can be convened by the President upon the request of any Member State. Under Article 35 of the Charter, the President shall call a meeting if a dispute or situation requires the Council's attention. According to Rule 6 of the Provisional Rules of Procedure, all concerns that are brought to the attention of the Secretary-General are drafted in an agenda that is approved by the President of the Security Council.

Participation

Any Member State of the UN may attend the Council's meetings upon the invitation of the Council. Member States are invited if the Security Council is discussing an issue that directly concerns the interests of the Member State. Invited Member States do not have the right to vote but are allowed to submit proposals and draft resolutions. Furthermore, those Member States can inform the Council about a current crisis in their region. However, such proposals may be put to a vote only at the request of a member of the Council.

Voting

Every Member State of the Security Council has one vote. Votes on all matters require a majority of nine Member States. However, if one of the five permanent members of the Security Council votes "no" on a matter of substance, such as a draft resolution, the draft resolution does not pass. Despite the existence of this veto power, the Council has adopted many resolutions by consensus since the end of the Cold War and has been divided only on a very limited number of issues..

Mandate, Functions, and Powers

The mandate of the Security Council is to maintain international peace and security, as specified in the *Charter of the United Nations*. Chapters VI and VII of the Charter specifically concern the Security Council and the range of actions that can be taken when settling disputes. Chapter VI aims to achieve resolution of disputes by peaceful means, whereas Chapter VII explores further actions that can be taken. Any Member State is able to report a dispute to the Security Council; the role of the Council is to determine the severity of the dispute brought before the body and the impact of the dispute internationally. The Security Council is responsible for making recommendations to broker peace that take into considerations the previously attempted measures by the parties involved. Under Non-military actions that can be implemented include blockades or economic interruptions. In aggregate, the Charter provides the Security Council with the following set of powers to fulfill its mandate.

- **Sanctions:** Pursuant to Article 41 of the Charter, the Council can call its members to apply economic sanctions and other measures not involving the use of force to prevent or end violence. These include economic sanctions, financial penalties and restrictions, travel bans, severance of diplomatic relations, and blockades, among others. It may further mandate arms embargos, enforce disarmament, or initiate proceedings in the international justice system.

- **Diplomatic Tools:** The Council has a mandate to investigate any dispute or situation that might lead to aggressions between states or other non-state groups or within states' national territories. In order to do so, it may "recommend methods of adjusting such disputes or the terms of settlement; formulate plans for the establishment of a system to regulate armaments; determine the existence of a threat to the peace or act of aggression and recommend what action should be taken."

- **Military Action:** The Council may take military action against a state or other entity threatening international peace and security and may further decide on the deployment of troops or observers. The Security Council may also decide to initiate peacekeeping operations, as well as the extensions of their mandates and subsequent modification or withdrawal of any troops.

- **Partnerships:** The Council also cooperates with several international and regional organizations as well as non-governmental organizations (NGOs) to implement its decisions. Cooperation between the Security Council and UN-related organizations, such as the Organization for the Prohibition of Chemical Weapons and the International Atomic Energy Agency, is significant, but partnerships with independent intergovernmental organizations such as the North Atlantic Treaty Organization and the African Union are also of paramount importance for addressing a broad range of issues such as terrorism, disarmament, nuclear nonproliferation, and extreme violence from non-state actors, among others.

Conclusion

As the international community faces increasing asymmetrical threats from non-state actors and transnational organized crime, the Security Council has adapted to new working methods and broader and more open Discussions. But these situations also represent the systemic divides among Council members.80 This lacking capacity can be partially explained by the Council's controversial decision-making process, specifically the veto power of the five permanent members. However, as the Security Council represents the only body within the UN that has the power to adopt binding resolutions, it is still the entity of utmost importance for the maintenance of international peace and security.

Cyber Defence

Introduction to Cyber Defence

Cyber Defence refers to strategies, techniques, and policies designed to protect systems, networks, and data from cyber threats. As digital infrastructure becomes more integral to national and global security, cyber Defence has emerged as a priority in international diplomacy.

Key Terminology

- Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks.
- Cybercrime: Criminal activities carried out using computers and the internet, such as hacking, data theft, and ransomware.
- Cyber Warfare: The use of digital attacks by nation-states to damage or disrupt the infrastructure of another nation.
- Phishing: Fraudulent attempts to obtain sensitive information, often for malicious reasons, by disguising as a trustworthy entity.
- Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to systems.

Overview of Cyber Threats

- Hacking: Unauthorized access to data in a system or network.
- Ransomware: A type of malware that threatens to publish the victim's data or block access unless a ransom is paid.
- DDoS Attacks: Distributed Denial of Service, where multiple systems flood the bandwidth or resources of a targeted system.
- State-Sponsored Attacks: Cyber attacks funded or directed by governments to gather intelligence or disrupt adversary infrastructure.

Challenges to Global Cyber Defence

- Sovereignty and Jurisdiction: There is no global consensus on the boundaries of state jurisdiction in cyberspace.
- Attribution of Attacks: It is difficult to trace cyber attacks to their true origin, leading to challenges in holding perpetrators accountable.
- Lack of Regulation: The global cyberspace lacks a robust legal framework to govern state and non-state actors' behavior.

Case Studies

- WannaCry Ransomware Attack (2017): A global ransomware attack that affected hundreds of thousands of computers in over 150 countries.
- SolarWinds Hack (2020): A sophisticated cyber attack targeting U.S. government agencies and corporations, attributed to Russian operatives.
- Estonia Cyber Attacks (2007): One of the first large-scale state-sponsored cyberattacks, targeting the government of Estonia.

Cyber Defence Recent talks about the new strategic concept for NATO include discussions about cyber Defence. Cyber Defence being the anticipation and preparation for an attack on computers and computer networks. In this case, attacks on a large scale that may affect national security and the protection of information. In May of 2010, the 13th NATO Cyber Defence Workshop was held in Estonia and brought experts and allies in to discuss ways in which to protect against cyber attacks. As a military alliance, NATO's research in cyber Defence mechanisms is an investment in the protection of its Member States. Working with the Co-operative Cyber Defence Centre of Excellence (CCDCOE), the workshop discussed such topics as: International Cyber Security, remedies for cyber attack victims, cyber war and the legal parameters of cyber Defence. Additionally, this research includes defining and identifying cyber attacks and determining if they are state sponsored attacks.

At the workshop, Estonian Defence Minister, Jaak Aaviksoo addressed three key points regarding cyber threats, saying that "every NATO country needs to develop a national approach to cyber security that encompasses all important stakeholders." The second point to which Minister Aaviksoo highlighted that the private sector in NATO nations is where most of the infrastructure exists and that the majority of Internet users are companies and individuals and are therefore the most vulnerable to cyber attacks. And the last point he outlines was the need to develop partnerships, citing "prevention and cooperation" as keywords. In the same month of the workshop, NATO released "NATO 2020" – a comprehensive document that was compiled by the group of experts on a new strategic concept for NATO. The document outlines how "NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber Defence capabilities aimed at effective detection and deterrence."

NATO's policy on cyber Defence was approved in 2008 and sets up a consolidated approach to cyber Defence and responses. The policy also contains individual advice to Allies regarding protection to their national communication systems. The policy found its roots after a series of cyber attacks in Estonia took place in the Spring of 2007. Estonian public and private institutions were attacked, prompting NATO to take the matter more seriously.

Cyber Attacks? To fully understand cyber Defence, it is important to grasp the concept of a cyber crime. "Cybercrime is not a new phenomenon, rather an evolving one with respect to adoption of information technology for abusive criminal purposes." Ways that cyber criminals go about their crime varies, sometimes they "try to slip information out slowly, hidden in ordinary internet traffic. At other times they have tried to break in by leaving infected memory-sticks in the car park, hoping somebody would plug them into the network. Even unclassified e-mails can contain a wealth of useful information about projects under development."

In the United States, and other western nations, the threat is seen as high and dangerous. This new form of espionage jeopardizes the high-tech know-how of the West that could erode its economic lead or blunt its military edge. "Cyber-espionage is the biggest intelligence disaster since the loss of the nuclear secrets [in the late 1940s]," says Jim Lewis of the Centre for Strategic and International Studies, in Washington, DC.

Examples of cyber warfare

Several international occurrences of cyber warfare have scared nations with fears of catastrophic consequences. Additionally, "according to one of the speakers at the conference, identity theft has outpaced illegal drugs in dollar volume." The following profiles of cyber attacks are some examples as to the impact that is plausible.

Estonia

In April of 2007, Estonian websites – including parliament, banks, ministries and newspapers – were hit with denialof-service attacks, which disrupted web-based services and websites. "Denial of service attacks happen when thousands of computers are linked together using software or an agent called a 'botnet' to overwhelm a website with requests, essentially crashing the servers that host the website." It is suspected the attack was Russian-based and that it stemmed from Estonia's removal of a soviet war memorial from the city of Tallinn. Some of the sites even directed users to propaganda images and Soviet quotations. As a result of the attack, Estonia shut down the websites to the external world while they tried to fix the problem. The attack was likened, by the Estonian Defence ministry, to terrorist attacks – something to be taken seriously by a country whose government is "paperless" and practices web-based banking. It was fitting that NATO's Cyber Defence Workshop took place in Estonia, a nation that felt the impact of a cyber attack.

China vs. Google

For actions that took place in 2009, China is accused of wholesale espionage and of attacking the computers of major Western Defence contractors and reputedly taking classified details of the F-35 fighter – an

American aircraft. China is said to have used Google and other IT companies to infiltrate these sites. It is suspected, however, that the main objective of the Chinese attack was to gain access to email accounts of Chinese human rights activists. The incident, that is still under investigation, has prompted Google to question whether or not to drop service in China altogether.

North Korea hits the US?

In early 2010, The United States appointed its first military general to oversee cyber warfare. Keith Alexander is now the General of Cyber Command – the Pentagon's new venture designed to conduct virtual combat across global computer networks. Additionally, Air Force troops have also been reassigned from their posts in technical support, to join the force of cyber warfare. The appointment of this general and the emphasis on cyber Defence comes after a feeling of increased vulnerability felt by western nations. An example of a threat came in 2009 when an attack hit many government and private sites in the US and shut many government sites down. The attack "underscored how unevenly prepared the U.S. government is to block such multi-pronged assaults." The attack was linked to North Korea because of internet addresses that linked back to North Korea as well as similar attacks simultaneously hitting South Korea. Such an attack is believed to merely disrupt service while also potentially gaining confidential information. After such chaos, the U.S has taken precautionary measures to ensure safety, namely by appointing a military post to specialize in the matter.

NATO's Role

As a military alliance, NATO may or may not take on a key role in the construction of any future international law regime or enforcement regarding cyber security. With its inclusion of cyber Defence in its new strategic concept, NATO has demonstrated its commitment to combating and preventing cyber attacks. Being that cyber attacks are a newer threat to the international community, forms of cyber Defence are still in development and NATO's role will be shaped as the new strategic concept starts to take form. What do you think the exact role of NATO should be? Do you think NATO is doing enough to protect its Allies by including cyber Defence in its new strategic concept? What obstacles might NATO encounter by trying to protect against cyber attacks?

Key Stakeholders

- Nation-States: Countries are both defenders and potential attackers in cyber conflicts.
- Private Sector: Companies hold vast amounts of data and are often targets of cyber attacks. They also develop and deploy cybersecurity solutions.
- Hacktivists: Individuals or groups using hacking to promote political ends.
- International Organizations: The UN, ITU, NATO, and others play a vital role in shaping cyber Defence strategies and policies.

Role of International Organizations

- United Nations: The UN's Group of Governmental Experts on Developments in the Field of Information and Telecommunications has been crucial in outlining norms for responsible state behavior in cyberspace.
- International Telecommunication Union (ITU): A specialized agency within the UN that coordinates global cybersecurity efforts.
- NATO: Cyber Defence is a key component of NATO's Defence strategies, especially after recognizing cyberspace as an official domain of warfare.

Major Cyber Defence Initiatives and Policies

- General Data Protection Regulation (GDPR): The EU's regulation to protect individual data privacy, applicable globally.
- Budapest Convention on Cybercrime: The first international treaty to address internet and computer crime by coordinating national laws.

- Tallinn Manual: A guide on how international law applies to cyber warfare, developed by a group of experts.

Annotations

NATO, What is NATO’s new Strategic Concept?, 2009.
Ambassade de France, Discours du Président Sarkozy sur la France, la Defence européene et l’OTAN au 21ème siècle [Speech by President Sarkozy on France, European Defence and NATO in the 21st Century], 2009.
France Diplomatie, Colloque « la France, la défense européenne et l’OTAN au XXIème siècle » – Intervention de Bernard Kouchner [“France, European Defence and NATO in the 21st Century” Symposium – Speech by Bernard Kouchner], 2009.
NATO, Experts Discuss Intensifying Cyber Defence Cooperation, 2010.
NATO, Experts Discuss Intensifying Cyber Defence Cooperation, 2010.
NATO, Experts Discuss Intensifying Cyber Defence Cooperation, 2010.
NATO 2020, Assured Security; Dynamic Engagement, May 17, 2010, page 11.
NATO, Defending Against Cyber Attacks,
Encyclopedia of Cybercrime, Computer Crimes, p. 195-200.