General Assembly

STUDY GUIDE

Haileybury Astana

Model United Nations

28 February - 1 March 2020

MUN REFUGEE CHALLENGE

Supporting UNHCR The UN Refugee Agency

KONRAD ADENAUER STIFTUNG

Dear Delegates,

Welcome to the first Haileybury Astana Model United Nations 2020 (HASMUN)! We are pleased to welcome you to the General Assembly. This year's chairs are:-------. ---

The agenda at hand is both vast and complex, and a successful discussion on it would entail the collective participation of all of you. It shall be your prerogative to decide the direction in which you want to take this committee. This agenda demands to be seen from more than one perspective, one that covers the issue of International Cybersecurity and the negative implications of government intervention, both in the context of economic, political and social problems nowadays. As the delegates of the General Assembly, you are expected and highly recommended to consider and actively discuss the multiple sides of the issue, while recognizing and following your state's policies and interests.

orce to maintain or restore international peace and security.

This Background Guide serves as an introduction to the topics for this committee. However, it is not intended to replace individual research. We encourage you to explore your Member State's policies in depth to further your knowledge on these topics. In preparation for the Conference, each delegation will submit a Position Paper by 11:59 p.m. (Nur-Sultan) on the 26th of February 2020.

We want to emphasize that any instances of sexual harassment or discrimination based on race, gender, sexual orientation, 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---------

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

Chairs----------

NATURE OF PROOF AND EVIDENCE

Documents from the following sources will be considered as credible proof for any allegations made in committee or statements that require verification.

Reuters: Appropriate Documents and articles from the Reuters News agency will be used to corroborate or refute controversial statements made in committee.

UN Document: Documents by all UN agencies will be considered as sufficient proof. Reports from all UN bodies including treaty based bodies will also be accepted.

Government Reports: Government Reports of a given country used to corroborate an allegation on the same aforementioned country will be accepted as proof.

INTRODUCTION TO THE COMMITTEE

Established in 1945 under the Charter of the United Nations1, the General Assembly occupies a central position as the chief deliberative, policymaking and representative organ of the United Nations. Comprising all 193 Members of the United Nations2, it provides a unique forum for multilateral discussion of the full spectrum of international issues covered by the Charter. It also plays a significant role in the process of standard-setting and the codification of international law3.

The Assembly is empowered to make recommendations to States on international issues within its competence. It has also initiated actions—political, economic, humanitarian, social and legal—which have benefited the lives of millions of people throughout the world. The landmark Millennium Declaration, adopted in 2000, and the 2005 World Summit Outcome Document, reflect the commitment of Member States:

- to reach specific goals to attain peace, security and disarmament along with development and poverty eradication;
- to safeguard human rights and promote the rule of law;
- to protect our common environment;
- to meet the special needs of Africa; and
- to strengthen the United Nations.

In September 2015, the Assembly agreed on a set of 17 Sustainable Development Goals, contained in the outcome document of the United Nations summit for the adoption of the post-2015 development agenda (resolution 70/1)4.

According to the Charter of the United Nations, the General Assembly may:

- Consider and approve the United Nations budget and establish the financial assessments of Member States;
- Elect the non-permanent members of the Security Council and the members of other United Nations councils and organs and, on the recommendation of the Security Council, appoint the Secretary-General;
- Consider and make recommendations on the general principles of cooperation for maintaining international peace and security, including disarmament;
- Discuss any question, relating to international peace and security and, except where a dispute or situation is currently being discussed by the Security Council, make recommendations on it;
- Discuss, with the same exception, and make recommendations on any questions within the scope of the Charter or affecting the powers and functions of any organ of the United Nations;
- Initiate studies and make recommendations to promote international political cooperation, the development and codification of international law, the realization of human rights and fundamental freedoms, and international collaboration in the economic, social, humanitarian, cultural, educational and health fields;
- Make recommendations for the peaceful settlement of any situation that might impair friendly relations among countries;
- Consider reports from the Security Council and other United Nations organs.

The Assembly may also take action in cases of a threat to the peace, breach of peace or act of aggression, when the Security Council has failed to act owing to the negative vote of a permanent member. In such instances, according to its "Uniting for peace" resolution of 3 November 1950, the Assembly may consider the matter immediately and recommend to its Members collective measures to maintain or restore international peace and security.

INTRODUCTION TO THE AGENDA

The exponential pace of technological change has shaken the very foundations of traditional security understanding. Over the past 50 years, international conflict has morphed into a shape beyond our wildest imaginations. Carl von Clausewitz, the father of modern warfare, once declared, „War is a mere continuation of policy by other means; War... is an act of violence to compel our opponent to fulfil our will"(Clausewitz). The „Fifth Domain" of warfare, cyberspace, and/or information warfare has given states and non-state actors new ways of achieving political ends through other means.

It is our mandate to oversee frameworks and solutions to issues that lead to a destabilization of peace and security to both individuals and states alike. Cyberspace has long been a blind-spot for the international system, where criminal and inter-state threats jeopardize the trust and readiness of collective security in both the developed and developing world. Over the past two years, actors such as China, the USA, the E.U., and Great Britain all shifted their view on cyberspace to include not only a matter of information security/C4-infrastructure but also the Fifth Domain of Warfare.

The problem with classifying cyber-attacks as a fifth domain of warfare is that cyberspace differs radically from other domains (land, sea, air, and space). A key tenant of international peace & security is deterrence, which involves parties to a potential conflict dissuading each other via credit mutual threats. In cyber, however, parties have the ability to strike with a certain degree of anonymity and deliver crippling blows without technically inflicting "kinetic" (or physical) violence. Cyber deterrence proponents like Nigel Inkster and the U.S. Department Homeland Security generally agree that states are vulnerable to attacks but tend to branch into two camps: those who argue for an offensive strategy in which leading countries assert dominance in cyberspace early on, and those who believe in defensive bandwagoning, which includes collaboration between states and the private sector. Other key theories discuss whether cyber operations should even be considered acts of war: John Stone (Cyberwar Will Take Place!) and Thomas Rid (Cyberwar Will Not Take Place) are at odds. The answers to questions dealing with how nations approach cyberspace determine how countries will pursue or prevent cyber-conflict.

DEFINITION OF KEY TERMS

Cyberspace: the internet considered as an imaginary area without limits where you can meet people and discover information about any subject.

Cybersecurity: things that are done to protect person organization, or country and their computer information against crime or attacks carried out using the internet.

Cybercrime: crime or illegal activity that is done using the internet.

Cyberterrorism: the use of the internet to damage or destroy computer systems for political or

other reasons.

Group of Governmental Experts (GGE): In GA resolution 73/266, the Secretary-General was requested to establish a Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. The GGE will also hold its first meeting in 2019 and is to submit its final report to the General Assembly in 2021.

Open Ended Working Group (OEWG): a particular group that works without definite limits, as a duration or amounts.

Warfare: the activity fighting war, often including weapons and methods that are used.

Deterrence: the action or the fact of deterring people from doing something.

Deter: to prevent someone from doing something or to make someone less enthusiastic about doing something by making it difficult for that person to do it or by threatening bad results if they do it.

Disarmament: the act of taking away or giving up weapons.

Endorsement: the act of saying that you approve of or support something or someone.

Integrity: the quality of being honest and having strong moral principles that you refuse to change

Cyberespionage: is the act of engaging in an attack or series of attacks that let an unauthorized user or users view classified material.

Surveillance: the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected.

GENERAL OVERVIEW

"The UN has taken a big step toward shaping an urgently needed international framework for legitimate and prosperous activities in cyberspace while offering the entire UN membership the tools to prevent a hasty militarization of the domain. Yet, this is only a beginning. Member states must make sure to undergird this framework with state practices fully in line with the general purpose criterion to make cyberspace "peaceful, secure, open and cooperative"

- Detlev Wolter

The First Committee5 of the UN General Assembly is one of the six main committees of the UN General Assembly (UNGA). It's where states address global challenges and threats to peace that affect the international community and seek ways to promote international security and disarmament.The UN General Assembly has been discussing the issue of information security since 1998, when the Russian Federation introduced a draft resolution on "Developments in the field of information and telecommunications in the context of international security" in the General Assembly (GA). Since then, member nations have been submitting reports about their thoughts on information security to the UN Secretary General. Mounting reports of disruptions and the increasing potential of cyber attacks disturbing the peace in the real world led countries to examine these challenges more seriously within the UN. More substantial work began at the UN when it constituted a Group of Governmental Experts (GGE) in 2004 to "examine the existing and potential threats from the cyber-sphere and possible cooperative measures to address them"6. Since then there have been three GGEs set up by the UN, gaining significant ground.

When it comes to cybersecurity-related issues, arguably the most important mechanism of the First Committee has been the GGEs. The first GGE on "Developments in the field of information and telecommunications in the context of international security" was set up in 2004. Through the GGEs, which are set up through the passing of a

resolution by UNGA member states, a group of member states selected by the UNSG nominate experts to hold discussions on the issues outlined in the mandate set out by the relevant resolution. If they all agree, the GGE produces a consensus report which is then presented at the General Assembly for endorsement by all member states.

While arguably it is important to maintain peace and international security in cyberspace, the debate arises on the means and methods of achieving this. The main argument might be whether state intervention justifies the granted access and usage of personal information, which might result in leakage of personal data. The possible use of personal information thus link to the violation of human rights. The committee is expected to raise the question of the relation of human rights and the possible solutions to avoid or minimize the violation of privacy and basic human rights, included in the Principles of Personal Data Protection and Privacy7.

Over the past decade, the international community has made clear that the international rules-based order should guide state behavior in cyberspace. UN member states have increasingly coalesced around an evolving framework of responsible state behavior in cyberspace (framework), which supports the international rules-based order, affirms the applicability of international law to state-on-state behavior, adherence to voluntary norms of responsible state behavior in peacetime, and the development and implementation of practical confidence building measures to help reduce the risk of conflict stemming from cyber incidents.

The promotion of peace and stability in cyberspace is important for human rights. Recent cyberattacks have resulted in the closure of hospitals, electrical grids and large industries, and even affected the integrity of democratic processes. These incidents – which directly affect the lives of ordinary citizens – show that the discussion of responsible state behaviour is closely linked to human rights. Without understanding and agreement between states on what responsible state behaviour looks like, cyberattacks could continue to undermine democratic institutions and even escalate into conflict. Engaging in these processes can provide an opportunity to promote measures like confidence-building measures (which can help to reduce the risk of escalation), and emphasise approaches that promote the stability and security of cyberspace – like principles of coordination and support for cybersecurity capacity

building, as well as measures which promote and protect human rights, including the right to privacy.

7Principles of Personal Data Protection and Privacy

https://www.unsystem.org/principles-personal-data-protection-and-privacy

TIMELINE OF KEY EVENTS

General timeline of economic sanctions in the world:

2004 The first Group of Governmental Experts (GGE) on "Developments in the field of information and telecommunications in the context of international security" was set up. Some of the achievements of the GGE: recommendation of a series of confidence-building measures and voluntary, non-binding norms8, agreement on the UN Charter and international law (including respect for human rights and fundamental freedoms) application to cyberspace9

October 2016 71st Session of the General Assembly First Committee10. The United Nations Institute for Disarmament Research (UNIDIR) held a side event on cyberspace and international peace and security during the session.

2018 the UN First Committee established two parallel processes to discuss responsible state behaviour in cyberspace – the UN GGE and the Open Ended Working Group (OEWG).

November 2018 Researchers discover that a Chinese cyberespionage group targeted a UK engineering company using techniques associated with Russia-linked groups in an attempt to avoid attribution

December 2018. Security researchers discover a cyber campaign carried out by a Russia-linked group targeting the government agencies of Ukraine as well as multiple NATO members

December 2018. The United States, in coordination with Australia, Canada, the UK, and New Zealand, accused China for conducting a 12-year campaign of cyber espionage targeting the IP and trade secrets of companies across 12 countries. The announcement was tied to the indictment of two Chinese hackers associated with the campaign.

February 2019. Norwegian software firm Visma revealed that it had been targeted by hackers from the Chinese Ministry of State Security who were attempting to steal trade secrets from the firm's clients.

February 2019. The UN International Civil Aviation Organizations revealed that in late 2016 it was compromised by China-linked hackers who used their access to spread malware to foreign government websites.

February 2019. Prior to the Vietnam summit of Kim Jong Un and Donald Trump, North Korean hackers were found to have targeted South Korean institutions in a phishing campaign using documents related to the diplomatic event as bait.

March 2019. The UN Security Council reported that North Korea has used state-sponsored hacking to evade international sanctions, stealing $670 million in foreign currency and cryptocurrency between 2015 and 2018.

March 2019. Iranian hackers targeted thousands of people at more than 200 oil-and-gas and heavy machinery companies across the world, stealing corporate secrets and wiping data from computers.

June 2019. Over the course of seven years, a Chinese espionage group hacked into ten international cellphone providers operating across thirty countries to track dissidents, officials, and suspected spies.

July 2019. Microsoft revealed that it had detected almost 800 cyberattacks over the past year targeting think tanks, NGOs, and other political organizations around the world, with the majority of attacks originating in Iran, North Korean, and Russia.

September 2019. Hackers with ties to the Russian government conducted a phishing campaign against the embassies and foreign affairs ministries of countries across Eastern Europe and Central Asia.

September 2019. Alleged Chinese hackers used mobile malware to target senior Tibetan lawmakers and individuals with ties to the Dalai Lama.

September 2019. North Korean hackers were revealed to have conducted a phishing campaign over the summer of 2019 targeted U.S. entities researching the North Korean nuclear program and economic sanctions against North Korea.

September 2019. Iranian hackers targeted more than 60 universities in the U.S., Australia, UK, Canada, Hong Kong, and Switzerland in an attempt to steal intellectual property.

October 2019. An Israeli cybersecurity firm was found to have sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in WhatsApp.

October 2019. A state-sponsored hacking campaign knocked offline more than 2,000 websites across Georgia, including government and court websites containing case materials and personal data.

October 2019. India announced that North Korean malware designed for data extraction had been identified in the networks of a nuclear power plant.

October 2019. Iranian hackers targeted more than 170 universities around the world between 2013 and 2017, stealing $3.4 billion worth of intellectual property and selling stolen data to Iranian customers.

October 2019. Chinese hackers engaged in a multi-year campaign between 2010 and 2015 to acquire intellectual property from foreign companies to support the development of the Chinese C919 airliner.

October 2019. A Chinese government-sponsored propaganda app with more than 100 million users was found to have been programmed to have a backdoor granting access to location data, messages, photos, and browsing history, as well as remotely activate audio recordings.

October 2019. The Moroccan government targeted two human rights activists using spyware purchased from Israel.

PREVIOUS UN DOCUMENTS RELATED TO THE AGENDA

- "Developments in the field of information and telecommunications in the context of international security", Report to the Secretary General, United Nations General Assembly, 58th Session, Addendum, A/58/373, September 17, 2003
- "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", Report to the Secretary General, United Nations General Assembly, 60th Session, Addendum, A/60/202, August 5, 2005
- Resolution 64/211, March 2010, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211
- Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunication in the Context of International Security, submitted to the UN General Assembly 68th Session, June 24, 2013, available athttp://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

QUESTIONS TO BE CONSIDERED

- How can we prevent privacy issues and information leakage throughout online platforms?
- Should companies and platforms be strictly regulated in terms of collecting personal data?
- At what point governments and organizations, including the UN, should intervene in the conflict?
- How can governmnets and organizations play a role in battling cyber terrorism and surveillance in the cyberspace?
- What will be the role of existing organizations regulating the cyberspace (including the GGEs, OEWG, etc.)?

SOME USEFUL RESEARCH LINKS

CSIS, List of Significant Cyber Incidents
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

UN, List of all previous UN Resolutions
https://www.un.org/en/sections/documents/general-assembly-resolutions/

ITU, List of UN Resolutions on Cybersecurity
https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

BIBLIOGRAPHY

- UN Resolutions related to Cybersecurityhttps://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx
- UN FIRST COMMITTEE PROCESSES ON RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACEhttps://www.gp-digital.org/un-first-committee-processes-on-responsible-state-behaviour-i n-cyberspace-a-briefing/
- Functions and Powers of the General Assemblyhttps://www.un.org/en/ga/about/background.shtml
- http://undocs.org/en/A/RES/70/1
- https://www.un.org/en/ga/about/background.shtml
- http://www.un.org/fr/member-states/index.html
- http://www.un.org/en/sections/un-charter/chapter-iv/index.html
- 2015 GGE report, 2015 GGE report A/70/174
- Principles of Personal Data Protection and Privacyhttps://www.unsystem.org/principles-personal-data-protection-and-privacy
- https://dictionary.cambridge.org
- GGE: https://www.un.org/disarmament/group-of-governmental-experts/
- Resolution adopted by the General Assembly on 22 December 2018:https://dig.watch/sites/default/files/Resolution%20A-RES-73-266%20-%20Advancing%
20responsible%20State%20behaviour%20in%20cyberspace%20in%20the%20context%2 0of%20international%20security.pdf