SC

YMUN 2024

Yonsei Model United Nations

Chair Report.

Chair Seoyeon Yu
Chair Dong Yoon Lee

Updated 4 Dec 2023

Security Council (SC)

Chair Report

[Agenda A: Promoting the Disarmament and Non-Proliferation of Weapons of Mass Destruction]

Yonsei Model United Nations 2024

Chair(s): Seoyeon Yu

Student Officer : Dong Yoon Lee

About the United Nations

The United Nations is the largest intergovernmental organisation that was founded in 1945 after World War II. Consisting of 193 member states, the United Nations endeavours to sustain international peace, security and cooperation, guided by the United Nations Charter.

A replacement for the League of Nations, the United Nations has been the centre of discussion and euphony for multilateral issues such as general disarmament, international security, multilateral cooperation, international economy, human rights affairs and sustainable development. The United Nations is operated under six major organs - The Secretariat, General Assembly, Security Council, Economic and Social Council, Trusteeship Council and the International Court of Justice. The United Nations has also assigned other specialised agencies and rapporteurs in reach for international peace and security.

Sessions of committees pertaining to the United Nations carry arduous responsibilities of perpetuating peace and humanitarian rights. Delegates of member states thrive to represent their designated nation and to form an international consensus on a myriad of agendas.

Committee Introduction

The Security Council is the most powerful body of the United Nations responsible for preserving international peace and security. The council determines factors of aggression that threaten peace and works with its member states to settle disputes through peaceful methods. The

Council is also capable of taking more assertive actions such as imposing sanctions or utilising force, if deemed necessary. It has the sole authority to command peacekeeping operations for crises or conflict management. All Member States of the United Nations are legally bound by, and therefore have the duty to comply with the Council's decisions.

The UN Security Council, as the principal decision-making body of the United Nations, holds several unique characteristics. It comprises five permanent members (P5): the United States, China, France, Russia, and the United Kingdom, who possess exclusive veto power - the power to reject any decision made in the council. Ten nonpermanent members are elected from the UN General Assembly based on their contributions to international order, serving two-year nonconsecutive terms. The council's presidency rotates alphabetically among its members, each serving for one month, aiming to empower all members equally.

Veto power's origins date back to World War II, when victorious nations shaped the postwar political order. However, criticism arises from conflicting member state interests and frequent use of veto power, particularly by the US and Russia, causing delays in the council's response to major crises.

Agenda Introduction

Agenda A: Promoting the Disarmament and Non-Proliferation of Weapons of Mass Destruction

Weapons of mass destruction (WMD) are atomic, radioactive, chemical, and biological weapons that have the potential to cause large-scale destruction and harm a large number of people. The possession and proliferation of WMD poses significant danger toward global security. They can be used to terrorise people and cause economic damage. The atomic bombs dropped on Nagasaki and Hiroshima in Japan killed over 100,000 people, including innocent civilians, bringing fear to the people even until now. Another type of WMD, chemical weapons, can cause long-term health effects such as the failure of the central nervous system or adverse pregnancy outcomes. WMD’s immediate destruction of infrastructure leads to massive economic damage and WMD itself is costly to manage outside of times of conflict. Many of the WMD entities, including nuclear devices, biological pathogens, and radioactive material, are inexpensive to produce and easy to deploy, rendering them attractive options for many agents

and therefore posing a greater threat to people. Furthermore, due to the immense destructive potential inherent in WMDs, their possession is often regarded as the symbol of power and influence. In order to maintain their status on the global stage, nations tend to be highly reluctant in the process of disarmament, and many persist to invest in the further development of WMDs.

One type of the WMDs that the international community puts particular attention to is nuclear weapons. Nuclear weapons possess the destructive capacity to obliterate entire cities and leave lasting influences on the surrounding environment, even impacting generations to come. Due to the catastrophic effects they pose, the mere existence of nuclear weapons and technology can become a menacing threat. Though actual usage in warfare is rarely reported in history, there have been over 2000 nuclear tests conducted to date with a continuous development in nuclear technology. Efforts for the non-proliferation and disarmament of nuclear weapons have continued through acts such as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), but have failed to show meaningful progress.

Key Terms

Weapons of Mass Destruction (WMD)

WMDs are atomic, radioactive, chemical, and biological weapons that have the potential to cause large-scale destruction or harm a large number of people. In 1948, recognizing the significance and necessity to differentiate WMD from other regular weapons, the United Nations Commission on Conventional Armaments defined WMD as "atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons." This suggests other types of weapons can be included in the definition of WMD according to the progress and development of new types of weapons.

Major WMDs include chemical and biological weapons. Chemical weapons are liquids and gases that provide physical harm to their victims through methods such as poisoning, choking, or disrupting the nervous system. Often used chemical weapons include chlorine gas and mustard gas, both first used in WWI and later used again in the Iran-Iraq War. Biological weapons are those that contain toxins or infectious agents, leading to severe outbreaks of deadly

diseases in populated areas. The relatively easy process of preparing and using chemical and biological weapons have made them a tool not only for states but also for individual terrorist groups.

Non-proliferation

Non-proliferation means the prevention of an increase or spread of something. This term will be used to indicate the prevention of nations getting or possessing nuclear weapons or WMD for this committee. Often, non-proliferation is considered as the pre-step of disarmament. Before reducing the number of WMDs, it is important to stop the further development and expansion of it. The concept of Non-proliferation is embedded in many past treaties, such as NPT, which will be discussed later.

Disarmament

Reduction or withdrawal of military forces and weapons. This concept of disarmament was raised after World War II. Multilateral disarmament and arms limitation has long been a central goal of the UN to maintain international peace and security. Recognizing the importance of disarmament, the UN Disarmament and International Security Committee (DISEC) was formed to eliminate weapons, especially WMD. It gives high priority to eliminate nuclear weapons, destroy chemical weapons, and prohibit biological weapons. Due to the cost of abandoning weapons and the sophisticated power-relationship behind it, the process of disarmament is expected to be a long and difficult path for the international community to effectively take on.

Deterrence theory

Deterrence theory in terms of nuclear weapons posits that the possession of nuclear weapons implicitly dissuades other states from launching nuclear attacks by promising mutually assured destruction. This concept is important to understand as it accounts for the motivation behind why different nations would like to possess WMD.

Historical Background

The concept of WMD has existed for centuries, long before the very term was coined. For example, it is known that Hernando Cortes exposed smallpox to the Aztec population in 1518, which led to devastating effects. However, WMD only started to be officially put on active use during the two World Wars. During WWI, chemical weapons were used at a large scale for the first time. The German army utilised mustard gases, causing a high number of casualties, soon followed by France and Britain. In the interwar period, various countries started to develop their own biological and chemical weapons. In 1925, the Geneva Protocol was set to prohibit biological and chemical weapons in warfare, but failed to stop countries from conducting research or starting large-scale production of these weapons. WWII saw a larger number of WMDs introduced and being put to usage. Firebombings killed many people in major cities in a short period of time. Thousands died due to deliberate release of pathogens and toxins, a method well used by the Japanese against China.

As technology progressed, the concept of nuclear fission, a process of a nucleus of an atom of radioactive material dividing into separate nuclei that cause a release of energy, allowed the formation of nuclear weapons, which is one of the most threatening types of WMD. In fear of German development of nuclear technology during WWII, the US undertook the Manhattan Project to create an atomic bomb, directed by theoretical physicist J. Robert Oppenheimer. On August 6th and 9th of 1945, the United States dropped a B-29 bomber named Enola Gay, and a plutonium implosion bomb nicknamed Fat Man, respectively to Hiroshima and Nagasaki. The United States Department of Energy records that the bombing of Hiroshima led to "70,000" deaths due to initial "blast, heat, and radiation effects" and "200,000" subsequent deaths, considering long-term effects of bombing such as cancer, "radioactive fallout, and other after effects." After these bombings devastated Japan, Japan had no other choice than to sign the Potsdam Declaration issued by the United States, Great Britain, and China to publicise and acknowledge unconditional surrender. The development of nuclear weapons only signalled the intensification of WMD development. During the following Cold War, the US, Soviet Union, and several major powers invested themselves in building massive stockpiles of WMD containing nuclear bombs, artillery shells, and missile warheads. Apart from nuclear weapons,

they also amassed stockpiles of chemical and biological weapons. Efforts to reduce the production and usage of WMD has continued since then, but have failed to show significant progress. There have been numerous attempts to regulate the use of WMDs. Some early attempts of the international community to reach a consensus include the Nuclear Non-proliferation Treaty of 1968, the Biological Weapons Convention of 1972, and the Chemical Weapons Convention of 1993.

While recognizing the significant threat of WMDs, the possession of WMD was also viewed as of great strategic value by different nations, and they tried to develop their own system. Among the numerous conflicts over the possession of WMD, one prominent case was initiated by WMD: the invasion of Iraq in 2003. Several nations led by the US alleged Iraq of trying to develop WMD under Sadam Husein's control. In 2002, Richard Myers said the United States found that Iraq had a mobile laboratory to produce weapons. In the following year, President Bush said the United Kingdom had found out that Hussein was in search of uranium from Africa, which can be used to create WMD, while Iraq has not clarified the purpose of uranium yet, nor does Iraq not have nuclear usage for daily use. Soon after, Collin Powell, former secretary of the United States, stated that Iraq was trying to develop Bacillus anthracis, a form of bacteria, as a weapon of mass destruction. This rising possibility of an alleged weapon of mass destruction was the United States and its allies' primary rationale for invading Iraq. The global society later found out that the alleged WMD was at least partially fake and thus criticised its hasty action. This event gives a clear message that WMD inspection requires extra thoughtful attention, especially before implementing a forceful solution.

From a long-term historical perspective, different nations, especially authoritarian regimes, showed an attempt to develop WMD as it enabled them to maintain political power. Countering these efforts, countries and international organisations have made a consensus for global disarmament.

Status Quo

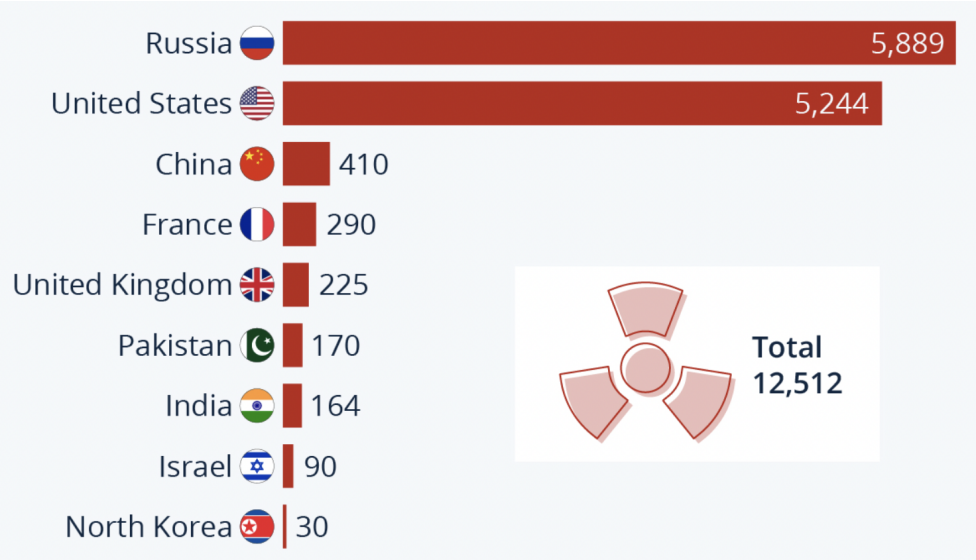

Figure 1: Estimated Global Nuclear Warhead Inventories of Countries Possessing Nuclear Arsenal, Statista 2023

Currently, a total of nine nations have access to nuclear weapons, namely Russia, the United States, China, France, the United Kingdom, Pakistan, India, Israel, and North Korea. One crucial point that should be taken into account is the motivation behind different countries' willingness to keep and develop WMD. Many states seem to consider nuclear weapons as a medium to enhance their prestige and influence in the international community. The idea of power provided by the possession of WMD has indeed been reflected in past trends, as states that have possessed WMD were more influential in deciding foreign policy matters, leading top-level international discussions as major powers. For example, during the postwar period, while the UK and France were behind Japan and West Germany in the economic aspect, they had greater influence and prestige in the international community due to their possession of WMD. The same idea was applied to China and India, with their possession of WMD guaranteeing them significant power status.

Not only does WMD provide an advanced and favourable position in terms of negotiation and foreign interaction, but possession of WMD guarantees national security. Such can be identified in Ukraine’s case. In 1992, Ukraine signed the Lisbon Protocol and joined the NPT as a non-nuclear weapon state. It decided to transfer former Soviet nuclear warheads to Russia and

committed itself to disarmament initiatives. While Ukraine's disarmament process after the Cold War was a laudable step for the cause of nonproliferation, critics have expressed concern that abandoning the nuclear program could be creating a significant weakness in the nation's security. The breakout of the ongoing Russo-Ukrainian War has once again proved the importance of maintaining national security, making people question if states are in the right environment to safely commit themselves to the disarmament process. Though there is indefinite evidence that the possession of nuclear weapons by Ukraine would have prevented the current conflict, it would be worthy to examine the role of WMD in terms of the progress of the war, namely identifying the background, rationale, and results of Ukraine abandoning WMD. In a broader sense, the committee should discuss not only measures to lead to the nonproliferation of nuclear weapons or WMD but should consider the measures that can make the environment favourable and safe for the nonproliferation of nuclear weapons.

Another aspect to focus on is the investigation method of alleged WMD. Considering the possibility of secret developments in WMD, the UN General Assembly established the Secretary General's Mechanism (UNSGM) through resolution A/42/37 C (1987). This mechanism looks for bacteriological weapons development by promptly investigating allegations of potential weapons use. If any member nations submits a report detailing such allegations to the Secretary-General, the Secretary-General is empowered to initiate an investigation objectively and scientifically by deploying a fact-finding team to the purported incident sites, and once this investigation is over, reports are sent back to all member nations. It is crucial to note that the UNSGM does not function as a permanent investigative body. Instead, Member States are regularly required to nominate experts and analytical laboratories. These entities are subsequently included in a roster and may be called upon to support a UNSGM investigation, all in accordance with the Guidelines and Procedures sanctioned by the General Assembly.

Qualified Experts	Expert Consultants	Analytical Laboratories
Qualified experts may be called upon to actively participate in any investigation team to conduct investigations into the alleged use of CBT weapons as requested by the Secretary-General. Their roles are outlined in the Guidelines and Procedures (A/44/561), paragraphs 64-75.	Expert consultants may be requested to advise and assist in the overall conduct and operation of the UNSGM, from planning and deployment to operation and reporting. Their roles are outlined in the Guidelines and Procedures (A/44/561), paragraphs 57-63.	Analytical laboratories may be requested to test for the presence of CBT agents. The role of designated analytical laboratories is outlined in the Guidelines and Procedures (A/44/561), paragraphs 76-80.

Figure 2: Nominations of Qualified Experts, Expert Consultants, and Analytical Laboratories, United Nations Office for Disarmament Affairs 2020

The diagram above illustrates the mechanism and components of the investigation team. One of the discussion points of the debate may be to discuss ways that can make this program comprehensive and more straightforward. One limitation of this program is that initiation of the program is the sole authority of the Secretary General of the United Nations, as well as the fact that investigation is often limited with the absence of all nations' full cooperation.

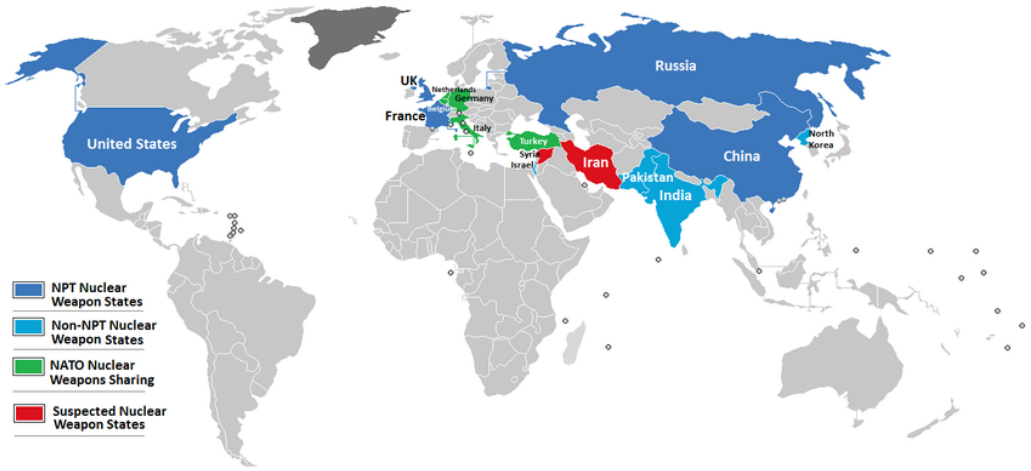

Figure 3: Map of Countries With Nuclear Weapons and Status of NPT, Researchgate 2010

The committee should also discuss ways to overcome the limitations of peaceful solutions, mainly the treaties. While it would be ideal for all nations to reach a consensus in a peaceful and agreeable way, it is often not achieved due to global politics behind them. This demonstrates the limitation of peaceful treaties as they are not in effect as long as they are signed. The diagram above illustrates the current status of some nations that are not signing the Nuclear Non-Proliferation Treaty (NPT). Thus, the committee should discuss ways to encourage the adoption of treaties and consider what is required to reach a consensus. If the cost of ultimate consensus seems unrealistic, the committee may want to approach the agenda with different perspectives. The concept of NPT will be further discussed in the below section.

Past Actions by Nations and Organisations

Security Council: Resolution 1540

Resolution 1540 was voted unanimously by member states of the Security Council. The resolution discusses and decides to implement the following measures: Calling nations to refuse to support non state actors that try to develop, produce, or transport WMD, agreeing to implement law regulation to prevent any group from developing, producing, transporting, or supporting creating WMD, calling nations to develop measures to effectively control the proliferation of WMD or their means of delivery by inspecting import/export systems, forming border control infrastructure, and securing existing WMD through direct governmental programs or providing financial assistance, deciding to form an inspection committee consisting of

expertise for a quick examination, clearly stating that the current resolution should not affect existing treaties such as the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention, the Biological and Toxin Weapons Convention, or responsibilities derived from the International Atomic Energy Agency or the Organization for the Prohibition of Chemical Weapons, providing assistance to the nations that might be lacking the proper infrastructure to implement the proposed solution, encouraging nations to participate in multilateral treaties and cooperations, deciding to remain seized of the matter and raise subsequent measures if necessary.

The resolution is significant in that it became the initial stepping stone to a series of subsequent resolutions related to WMD. For example, On 27 April 2006, the Security Council decided to extend the mandate of the inspection committee (1540 committee), which is written in operative clause four, by two more years with the adoption of resolution 1673. An additional instance involves the resolution 1810 passed by the Security Council in April 2008. This resolution extended the tenure of the 1540 committee by an additional three years and emphasised the ongoing enhancement of its role in aiding technical assistance. This included active involvement in coordinating offers and requests for assistance, thereby reinforcing its clearinghouse function. To measure their actions, the committee drafted a comprehensive review of Resolution 1540 and published it in 2010. Their revisit of resolution continued as they continuously renewed the duration of the committee, expanding the committee, as well as calling for progress checks.

The Biological Weapons Convention

The Biological Weapons Convention (BWC) refers to a treaty composed of 15 articles that was signed in April of 1972 for the purpose of banning the development, production, acquisition, transfer, stockpiling and use of WMD. States are encouraged to destroy biological weapons and stop the development of them. They are required to report alleged breaches of the BWC to the UNSC, cooperate in its investigation, and provide assistance to states in danger due to biological weapons. The BWC plays a big role in negotiation efforts regarding WMD proliferation and has succeeded in establishing a norm against biological weapons. Currently, it has 183 states-parties, including Palestine, and four signatories (Egypt, Haiti, Somalia, Syria, and Tanzania), while ten states have not signed the BWC yet. States of the BWC regularly meet to

pursue initiatives to strengthen the convention, and there have been eight Review Conferences since the first BWC. Despite being a legally binding document, the lack of an adequate mechanism for verifying compliance has resulted in a low level of adherence to this convention.

Treaty on the Non-Proliferation of Nuclear Weapons (NPT)

NPT, with its main objective to prevent the spread of nuclear weapons and their technology, was signed in April 1970 under the International Atomic Energy Agency (IAEA). In its eleven articles, states that have joined the NPT are prohibited from transferring nuclear weapons or any other nuclear explosive devices and are not allowed to gain control over nuclear weapons or explosive devices either directly or indirectly. While 191 states joined in with this treaty, some nations, namely India, Israel, Pakistan, and South Sudan, refused to sign it. One of the reasons why countries disagreed was due to NPT's statement of only recognizing China, France, the Russian Federation, the United Kingdom, and the United States as nuclear weapon states (NWS).

Stances of Major Countries and Non-Governmental Organisations (NGOs)

United States of America

Despite being the only country to have used a nuclear weapon in war, the United States is ironically committed to promoting the disarmament and non-proliferation of Weapons of Mass Destruction (WMDs). Recognizing the eradication of WMD as the cornerstone of global security, the United States has supported strengthening verification mechanisms and enhancing transparency in disarmament initiatives for a long time, having a record of initiating the invasion of Iraq. Currently, the United States is not only expressing concern about the possibility of Russia using WMD in the current invasion but also shows a willingness to actively respond. Joe Biden has stated that NATO would respond "in kind" if Russia uses weapons of mass destruction in Ukraine, affirming the nature of the response depends on the nature of the use."

Pakistan

Pakistan is one of the nations that has not signed the Treaty on the Prohibition of Nuclear Weapons. Pakistan has shown a unique perspective as it showed disapproving stances and raised a vote against it in an annual UN General Assembly resolution in 2018 and further resolutions since then. Pakistan clarified its stance at the United Nations meeting in October 2022. It expressed disapproval with the treaty and showed willingness to be free from the obligations arising from the treaty. Pakistan currently has approximately 170 nuclear weapons as a form of missiles and aircraft and seems to be continuing its process of weapon development. It is estimated that Pakistan spent an estimated US$1 billion to form nuclear weapons in 2022. Pakistan has been reluctant to actively cooperate with the international community in regards to weapon reduction, as shown by not participating in the negotiation of the treaty on the prohibition of nuclear weapons. This is also reflected in Pakistan's refusal to vote on the UN General Assembly resolution that established the official consensus for states to commence the negotiations in 2017 on a legally binding measure to ban nuclear weapons, ultimately aiming towards their total elimination.

Israel

Israel is known to possess nuclear weapons since the 1960s. However, Israel maintains a policy of nuclear opacity, which never openly admits the existence of its nuclear program. Israel is not a signatory to the BWC nor NPT. Israel is also widely refutable for their weapon manufacturing: "Israel Weapon Industries (IWI) manufactures small arms for the Israeli military and for export … [including] assault and sniper rifles, pistols, grenade launchers and the Uzi submachine gun." This is especially concerning as the trend of different nations importing weapons from Israel has increased due to recent war outbreaks and the increase of global tension.

India

India has opposed signing NPT because they perceive NPT discriminative as it only officially recognizes five nations (P5 nations) as nuclear weapon states. India views that the goal should be complete disarmament and elimination of WMD globally. Indira Gandhi, who was

Prime Minister of India, revealed their rationale for the decision: “India's refusal to sign the NPT was based on enlightened self-interest, and the considerations of national security ... nuclear weapon powers insist on their right to continue to manufacture more nuclear weapons … cannot be viewed with equanimity by non-nuclear countries.” While India possesses nuclear weapons, there remains a policy not to use them first, so to use them only as a means of defence.

China

China recently reaffirmed their stances marked by Sun Xiaobo’s (the Director-General of the Department of Arms Control of the Foreign Ministry of China) comment on the NPT Review Conference in August 2023: China’s policy is “not to be the first to use nuclear weapons at any time and under any circumstances” and “not to threaten to use nuclear weapons against non-nuclear-weapon states.” However, the current trend of China increasing its arsenal of operational nuclear warheads from an estimated 400 in 2021 to 500 as of May this year has grabbed global attention.

Russia

Russia is another nation that did not sign the Treaty on the Prohibition of Nuclear Weapons. Russia held a convention with the United States in 2011 called the New Start Treaty. The treaty limits both nations’ weapon capacities, such as a number of intercontinental ballistic missiles, submarine-launched ballistic missiles, deployed heavy bombers, and nuclear warheads, as well as their launchers. This treaty was initially set to last until February 2018 and was later extended to February 2026. Their treaty requires two nations to exchange their status of weapons twice a year. However, “the Russian Federation announced a unilateral and unjustified purported suspension of the treaty on February 28, 2023,” thus not providing 2023 March data. In response, the United States did not send data to Russia, but with an interest in transparency and to urge Russia, they revealed their data to the public.

Category of Data	United States of America	Russian Federation
Deployed ICBMs, Deployed SLBMs, and Deployed Heavy Bombers	**662**	**Not provided**
Warheads on Deployed ICBMs, on Deployed SLBMs, and Nuclear Warheads Counted for Deployed Heavy Bombers	**1419**	**Not provided**
Deployed and Non-deployed Launchers of ICBMs, Deployed and Non-deployed Launchers of SLBMs, and Deployed and Non-deployed Heavy Bombers	**800**	**Not provided**

Figure 4: Nuclear Weapon Status Based on New START Treaty, United States Department of State 2023

Considering the fact that Russia is a WMD-possessing country and Russia is currently at war, the committee should pay extra attention to the relevance between their war status and their WMD policies.

Organisation for the Prohibition of Chemical Weapons (OPCW)

OPCW, an organisation created in 1997, currently works with 193 member states to implement the Chemical Weapons Convention and prohibit the use of chemical weapons, encouraging the use of chemistry only for peace and prosperity. States following the Chemical Weapons Convention are also members of the OPCW. Currently, the Democratic People's Republic of Korea, Egypt, South Sudan, and Israel have not yet joined the OPCW. This organisation has a favourable view on the disarmament of WMD. One example of their interest in the area is to find safe ways to destroy chemical weapons while considering their environmental outcome. In its regular sessions, the organisation attempts to create and take measures that are deemed necessary to ensure state compliance on prohibiting chemical weapons.

International Campaign to Abolish Nuclear Weapons (ICAN)

ICAN is a coalition of partner organisations to promote people in the international community to encourage their governments to adhere to and implement the United Nations nuclear weapon ban treaty. ICAN makes partnerships with other nongovernmental organisations to reach the same goal of reinforcing nuclear weapon treaties. It has joined in implementing seven conferences on the objective of discussing detrimental humanitarian consequences from nuclear war. These efforts contributed to the UNGA adoption of a 2016 resolution to begin negotiation talks on an international legal treaty prohibiting nuclear weapons.

Possible Solutions

1. *Seeking for multilateral disarmament: Reaching consensus*

As illustrated above, global society had already put lots of effort and raised treaties to "peacefully" address the issue. However, there are limitations to approaching this agenda solely by treaties according to two major limitations demonstrated historically. First, the solution is not effective at all if it is not signed by all nations globally. To address this, it is necessary to carefully examine the rationale behind treaty disagreeing nations. Perhaps one opposing view of NPT is that it only officially recognizes P5 nations as WMD-possessing countries. Another view can be attributed to deterrence theory, as many nations believe that holding WMD indirectly prevents a nation from being targeted by a WMD attack or military attack. This view had recently gained attention once again as Russia initiated an invasion of Ukraine after Ukraine disposed of nuclear weapons. While this does not necessarily imply the relationship that disassembling WMD causes being targeted, multiple perspectives suggest that war could not have started if Ukraine decided to keep its WMD. Second is that a treaty can be broken at any time, especially when it only appeals to moral obligation. One way to motivate different nations might be to incentivize nations either with reward or punishment. However, the source of such incentives must be an important factor to be discussed in the committee. . Promising treaties can be made after considering these factors.

2. *Enhancing the inspection infrastructure*

The global society currently relies on the inspection system mentioned above to prevent and check whether global societies are following guidelines in terms of producing WMD. Although its system is based on the United Nations with expert teams, the committee can discuss ways to improve the current system. Some of the discussion points include finding measures to let the inspection team access all countries, optimising the inspection process, and considering a budget system.

3. *Considering the existence of veto power*

In the process of forming a resolution, the committee should consider the existence of veto power from P5 nations (the United States, China, France, Russia, and the United Kingdom). Veto power refers to the right of P5 nations to veto or deny the operative clauses of a resolution proposed by the committee. Thus, even when the 14 nations agree to the resolution, even one veto from any P5 nation can invalidate clauses. Therefore, when reaching a resolution, delegates must ensure that they consider veto power in order to propose a resolution that is to be reinforced. However, proposing a resolution that is vetoed still makes a record that it is raised and vetoed, showing the sponsoring nation's perspective or stances on the agenda, although it may not be implemented.

<u>Questions to Consider</u>

- Are there any ethical concerns the committee should discuss when addressing the issue?
- What measures can the committee implement to strengthen the verification mechanisms for disarmament agreements?
- How does emerging technology contribute to addressing the agenda?
- What were the limitations of past treaties? What is the reason why countries do not sign the peace treaties? How can this be mitigated?
- How can public awareness and education take a role in promoting the goals of disarmament and non-proliferation?

- What are organisations that work toward disarmament and non-proliferation? In what ways can the United Nations Security Council cooperate with those organisations?
- To what extent do intelligence-sharing mechanisms play a role in enhancing disarmament efforts?
- To what extent does a nation possessing WMD raise its political power status?
- How is a nuclear weapon or WMD regulated in different countries? What is ideal, if there are any, measures to inspect and regulate the formation of WMD?
- What measures should the committee take to prevent the illicit trafficking of WMD-related materials?

Bibliography

Armstrong, Martin, and Felix Richter. “Infographic: The Countries Holding the World’s Nuclear Arsenal.” *Statista Daily Data*, 4 Aug. 2023, www.statista.com/chart/8301/the-countries-holding-the-worlds-nuclear-arsenal/.

“Atomic Bomb: Nuclear Bomb, Hiroshima & Nagasaki - History.” *History.Com*, A&E Television Networks, www.history.com/topics/world-war-ii/atomic-bomb-history. Accessed 1 Dec. 2023.

“Biological Weapons Convention.” *United Nations Office for Disarmament Affairs*, disarmament.unoda.org/biological-weapons/. Accessed 1 Dec. 2023.

“Caat - Israel Weapon Industries (IWI).” *Campaign Against Arms Trade*, caat.org.uk/data/companies/israel-weapon-industries-iwi/. Accessed 1 Dec. 2023.

“China’s No First Use of Nuclear Weapons Policy: Change or False Alarm?” *Royal United Services Institute*, 13 Oct. 2023, www.rusi.org/explore-our-research/publications/commentary/chinas-no-first-use-nuclear-weapons-policy-change-or-false-alarm#:~:text=In%20August%202023%2C%20at%20the,use%20nuclear%20weapons%20against%20non%2D.

Christinawilkie. “Biden Says U.S. Would ‘respond’ to Russia If Putin Uses Chemical or Biological Weapons.” *CNBC*, CNBC, 11 Apr. 2022, www.cnbc.com/2022/03/24/biden-says-us-would-respond-to-russia-if-putin-uses-chemical-or-biological-weapons.html.

Epstein, William. “Why States Go -- And Don’t Go -- Nuclear.” *The Annals of the American Academy of Political and Social Science*, vol. 430, 1977, pp. 16–28. *JSTOR*, http://www.jstor.org/stable/1042354. Accessed 1 Dec. 2023.

"Fact Sheets & Briefs." *The Biological Weapons Convention (BWC) At A Glance | Arms Control Association*, www.armscontrol.org/factsheets/bwc#:~:text=It%20currently%20has%20183%20states,%2C%20South%20Sudan%20and%20Tuvalu. Accessed 1 Dec. 2023.

Feng, Emily. "New Pentagon Report Claims China Now Has over 500 Operational Nuclear Warheads." *NPR*, NPR, 19 Oct. 2023, www.npr.org/2023/10/19/1207156597/new-pentagon-report-claims-china-now-has-over-500-operational-nuclear-warheads#:~:text=1%2C%202019.-,The%20latest%20assessment%20from%20the%20defense%20department%20said%20China%20had,as%20of%20May%20this%20year.

"First Committee, 1) 25th Plenary Meeting (Resumed), 2) 26th Plenary Meeting - General Assembly, 77th Session | UN Web TV." *United Nations*, United Nations, webtv.un.org/en/asset/k16/k16anwggkc?kalturaStartTime=3968. Accessed 1 Dec. 2023.

Ghosh, Arundhati. "India and the Non-Proliferation Regime: Consistency or Change?" *Indian Foreign Affairs Journal*, vol. 1, no. 1, 2006, pp. 32–44. *JSTOR*, http://www.jstor.org/stable/45340543. Accessed 1 Dec. 2023.

"Israel." *The Nuclear Threat Initiative*, 15 Nov. 2023, www.nti.org/countries/israel/#:~:text=Although%20Israel%20has%20possessed%20nuclear,has%20never%20signed%20the%20NPT.

Kawai, Kazuo. "Mokusatsu, Japan's Response to the Potsdam Declaration." Pacific Historical Review, vol. 19, no. 4, 1950, pp. 409–14. JSTOR, https://doi.org/10.2307/3635822. Accessed 1 Dec. 2023.

Manhattan Project: The Atomic Bombing of Hiroshima, August 6, 1945, www.osti.gov/opennet/manhattan-project-history/Events/1945/hiroshima.htm. Accessed 1 Dec. 2023.

Map of Countries with Nuclear Weapons. NPT, Nuclear Nonproliferation ..., www.researchgate.net/figure/Map-of-countries-with-nuclear-weapons-NPT-nuclear-nonproliferation-treaty-Source_fig3_43535855. Accessed 1 Dec. 2023.

"Navigation and Service." *RKI*, www.rki.de/EN/Content/infections/biological/projects/UNSGM/UNSGM_node.html#:~:text=The%20United%20Nations%20Secretary%2DGeneral's%20Mechanism,-The%20United%20Nations&text=At%20the%20request%20of%20a,report%20to%20all%20Member%20States. Accessed 1 Dec. 2023.

"New START Treaty - United States Department of State." *U.S. Department of State*, U.S. Department of State, 1 June 2023, www.state.gov/new-start/#:~:text=Treaty%20Structure%3A%20The%20Treaty%20between,all%20Russian%20deployed%20intercontinental%2Drange.

"New START Treaty Aggregate Numbers of Strategic Offensive Arms - United States Department of State." *U.S. Department of State*, U.S. Department of State, 15 May 2023, www.state.gov/new-start-treaty-aggregate-numbers-of-strategic-offensive-arms-5/.

"Potsdam Declaration." *Encyclopædia Britannica*, Encyclopædia Britannica, inc., www.britannica.com/topic/Potsdam-Declaration. Accessed 1 Dec. 2023.

Rebehn, Michael. "The Long History of Weapons of Mass Destruction." *openDemocracy*, 7 Feb. 2003, www.opendemocracy.net/en/article_964jsp/.

"Russia." *ICAN*, www.icanw.org/russia. Accessed 1 Dec. 2023.

"Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM)." *United Nations Office for Disarmament Affairs*, disarmament.unoda.org/wmd/secretary-general-mechanism/. Accessed 1 Dec. 2023.

"UN Security Council Resolution 1540 (2004)." *United Nations Office for Disarmament Affairs*, disarmament.unoda.org/wmd/sc1540/. Accessed 1 Dec. 2023.

"Weapons of Mass Destruction." *Obo*, www.oxfordbibliographies.com/display/document/obo-9780199743292/obo-9780199743292-0221.xml#:~:text=The%20term%20%E2%80%9Cweapons%20of%20mass,effect%20to%20those%20of%20the. Accessed 1 Dec. 2023.

Security Council (SC)

Chair Report

[Agenda B: Measures to Combat Cyber Threats on the Security of Critical Infrastructure]

Yonsei Model United Nations 2024

Chair(s): Seoyeon Yu

Student Officer : Dong Yoon Lee

About the United Nations

The United Nations is the largest intergovernmental organisation that was founded in 1945 after World War II. Consisting of 193 member states, the United Nations endeavours to sustain international peace, security and cooperation, guided by the United Nations Charter.

A replacement for the League of Nations, the United Nations has been the centre of discussion and euphony for multilateral issues such as general disarmament, international security, multilateral cooperation, international economy, human rights affairs and sustainable development. The United Nations is operated under six major organs - The Secretariat, General Assembly, Security Council, Economic and Social Council, Trusteeship Council and the International Court of Justice. The United Nations has also assigned other specialised agencies and rapporteurs in reach for international peace and security.

Sessions of committees pertaining to the United Nations carry arduous responsibilities of perpetuating peace and humanitarian rights. Delegates of member states thrive to represent their designated nation and to form an international consensus on a myriad of agendas.

Committee Introduction

The Security Council is the most powerful body of the United Nations responsible for preserving international peace and security. The council determines factors of aggression that threaten peace and works with its member states to settle disputes through peaceful methods. The

Council is also capable of taking more assertive actions such as imposing sanctions or utilising force, if deemed necessary. It has the sole authority to command peacekeeping operations for crises or conflict management. All Member States of the United Nations are legally bound by, and therefore have the duty to comply with the Council's decisions.

The UN Security Council, as the principal decision-making body of the United Nations, holds several unique characteristics. It comprises five permanent members (P5): the United States, China, France, Russia, and the United Kingdom, who possess exclusive veto power - the power to reject any decision made in the council. Ten nonpermanent members are elected from the UN General Assembly based on their contributions to international order, serving two-year nonconsecutive terms. The council's presidency rotates alphabetically among its members, each serving for one month, aiming to empower all members equally.

Veto power's origins date back to World War II, when victorious nations shaped the postwar political order. However, criticism arises from conflicting member state interests and frequent use of veto power, particularly by the US and Russia, causing delays in the council's response to major crises.

Agenda Introduction

Agenda B: Measures to Combat Cyber Threats on the Security of Critical Infrastructure

With rapid developments in technology, cyber-attacks on critical infrastructure networks have become a growing concern. Cyberattacks are increasingly targeted on critical infrastructure, infrastructures considered as the backbone of the nation’s society, namely infrastructure related to the energy sector. By disrupting the systems that control vital sectors of the society, attackers can have a devastating impact on national economic stability, public health or safety, and security. Vital sectors such as the energy, transportation, or telecommunications sectors are the main targets of attackers, with facilities connected to electricity and financial services also being frequently exposed to attacks.

Unlike the past where critical infrastructure often operated in isolation, critical infrastructure has become much more intertwined, automated, and reliant upon connected

networks. As critical infrastructure systems are becoming increasingly dependent on information technology and interconnected to other infrastructure networks, they have become more vulnerable to cyberattacks. Systems in the power and electricity sector, for example, are usually interconnected to create a more efficient and robust energy grid. While such an interconnected form indeed yields significant benefits to the public, it simultaneously leaves the systems more open and susceptible to cyberattacks.

Given such transitions are occurring in the mode of operation, there is a rising importance on protecting critical infrastructure networks. An attack on these networks can impact every aspect of daily life and bring about catastrophic damage on public infrastructures as well. Delegates must carefully consider the gravity and complexity of the issue to come up with plausible solutions.

Key Terms

Critical Infrastructure

The specific terms of critical infrastructure is defined differently by region, but it generally refers to the systems and assets that are essential to a nation. Disruption in critical infrastructure may lead to threats on national security, public health, and the economy. In the digitalized age, critical infrastructure in the information sector consists of information and communications technology that are closely connected to other critical infrastructures and their operation. With a growing importance of critical infrastructures, states have been issuing specific frameworks on the protection of critical infrastructure. The European Commission classifies critical infrastructures to multiple sectors including energy, information and communications technology, financial systems, civil administration (such as government facilities and postal services), transportation systems, and the chemical industry. The President's Commission on Critical Infrastructure Protection (PCCIP) in the US has also classified critical infrastructures to eight sectors: telecommunications, transportation, electric power systems, finance, natural gas and oil, water supply, government services, and emergency services.

The interdependencies of critical infrastructures can be categorised to physical, geographic, cyber, and logical interdependencies. A physical interdependence exists when an

infrastructure is dependent on resources from other infrastructures. A geographic interdependence exists when infrastructures are located in close proximity, so that a disturbance in one can impact another infrastructure. A cyber interdependence exists when the infrastructures are dependent on a common information and communications system. When the connected systems or actions cannot be categorised into physical, geographic, or cyber, the infrastructures are said to be logically interdependent. Among these, the interdependency that makes critical infrastructures particularly vulnerable to cyber-attacks is the cyber interdependence, but all types of interdependency plays a role in magnifying the extent of harm posed by the attack.

Figure 1: Essential Critical Infrastructure Workers, CISA 2021

Information Technology (IT)

Information technology is the use of computers, services, software, hardware, infrastructures to cover functions including safeguarding data and information, managing communications networks, and resolving computer problems. IT is often used for business operations or for public goods instead of personal entertainment purposes. It has first evolved from the mid-20th century and has become a major part of our society's management and organisation systems overtime.

Energy Grid

The energy grid is composed of three separate sections of generation, transmission, and distribution. It is a system that transmits power generated at diverse facilities and distributes it to facilities, schools, individual homes, and more. Though varying at range, the electric grid is often synchronised and connected to other facilities.

Information and Communications Technology (ICT)

ICT is the infrastructure and the components that allow modern computing. Due to the nature of technologies to constantly evolve, there is no fixed universal definition of ICT. However, it generally includes all networking components, technological devices, related applications, or the combination of them. The ICT systems and tools attempt to enhance the process of information sharing and creation among people.

Information systems deal with the use of ICT to deliver knowledge. Its main components include computer hardware and software, databases, various networks, telecommunications, and processing systems. They are mostly interconnected to collect, process, and transmit digital information.

Historical Background

Cybersecurity may seem like a relatively new issue that rose only after the massive digitalization of the 21st century, but the history of cybersecurity dates back to the mid 20th century. In the beginning of the digital revolution, crimes have been targeted against the loosely managed control systems and networks, as many were not focused on strengthening their network protection systems. Most cyberattacks done in the 20th century were focused on individuals and private companies, but these expanded to target governmental systems and critical infrastructures overtime as attackers became increasingly adoptive and organised.

The first computer virus is known as the “Creeper Virus,” created by Bob Thomas of BBN Technologies for research purposes in 1971. The virus made people become aware of potential viruses that may cause critical damage to computer systems. In 1988, the first cyber

attack called the “Morris Worm” was distributed via the internet, before the release of the World Wide Web. The virus infected a large number of computer systems at different universities and institutions, including NASA. Going into the 90s, rapid technological developments gave rise to sophisticated communication technologies and networks more interconnected to each other through the internet. People were no longer limited by physical barriers; they could be connected to anywhere, anybody, wherever they were in the world. However, such developments were followed by the growth of cybercrime. In 1998, Max Butler, who worked as a security consultant for the FBI, hacked the US government websites before committing another illicit foray. A year later, the Melissa Virus spread across the internet, corrupting users’ document files and causing around $80 million worth of damages. Entering the 20th century, the attacks became more sophisticated and persistent, with many being sponsored by nation-states. The threatening evolution of cybercrime brought along new viruses and malicious techniques, damaging critical sectors of the digital society and the global economy. In response to increased cybercrimes, organisations have developed more security systems with the employment of cybersecurity professionals. A new field of ethical hacking also emerged, aimed to discover potential threats before a malicious cyberattack.

Individuals, private businesses and organisations are not the only targets of cybercrime, however. Governments and public critical infrastructures have also shown to be vulnerable to cyber attacks. In 2007, Estonia, government websites related to the media, banks, and government ministries were flooded by a series of denial-of-service (DoS) attacks. Though never admitting its involvement, the Russian government was blamed for these cyberattacks. The period was a time of political tensions between the two countries, and circumstantial evidence was pointing towards Russia. A similar cyberattack incident harming national security occurred in 2010, Iran. The Stuxnet computer worm, a well-designed digital weapon, attacked nuclear machines in the Natanz uranium enrichment facility, harming the Iranian nuclear programme. Though both countries never officially admitted their role in the incident, investigation suggested that the United States and Israel were responsible for designing and executing the Stuxnet computer worm. More recently, in 2021, the US Colonial Pipeline was targeted by the DarkSide Ransomware Group, a group of ransomware-as-a-service (RaaS) providers, leading to a shutdown of their entire operations. Because the Colonial Pipeline was responsible for a large part of the East Coast’s supply of gasoline and fuel, the attack led to a spike in gasoline prices

and forced a number of states to declare themselves in a state of emergency. As the Colonial Pipeline can be considered as critical infrastructure, the damage was even greater in scope and impact. After the attack, the US declared it would treat such cyberattacks or the use of ransomware on critical infrastructure as terrorism. Because it is necessary to have a deep understanding of the operations and configuration of the control systems to cause a cyber-attack damage on critical infrastructure, information systems over the internet were considered as the main targets of cybercrimes. However, the rapid growth of technology and the subsequent creation of malware capable of manipulating control systems have made attacks on critical infrastructure a reality, as seen in the case of Stuxnet.

Such increasing attacks on governments and critical infrastructures, particularly those expected to be sponsored by nation-states, have urged people to believe the world is entering a "cyberwar." Because of the difficulty to identify the attacker and the motive in cyberattacks, it is even more challenging to build an effective cyber-defense system. Today, the control equipment for critical infrastructure are becoming more interdependent and are based on standardised specifications, making them more vulnerable to cyber-attacks.

Status Quo

Critical infrastructures are at the centre of maintaining modern society. Because their functions are vital to a society's regular functioning, the protection of critical infrastructure have become national priorities globally. Recently, as attackers became more professional, critical information infrastructures have become major targets. Crimes usually consist of interruptions to the systems controlling the physical processes, resulting in damages on physical infrastructure and disruption of vital services. Threats held against critical infrastructures' control systems and related digital systems are evolving in sophistication and scope.

Critical infrastructures have become highly vulnerable to attacks due to their growing interdependence. They do not operate independently, instead being connected to other systems and networks. For a more convenient management, infrastructures are linked to multiple critical infrastructures and the services provided by them. Due to such characteristics, one critical infrastructure could serve as an access point for other systems, providing a high possibility for

the occurrence of cascading effects from cyber-attacks targeted towards a single infrastructure. For example, when the control over a telecommunications satellite *Galaxy 4* was lost, approximately 90% of all pagers were in blackout, with widespread transmission issues in television and radio networks. Due to its interdependence on other systems, it also resulted in a disruption of multiple banking and financial services such as machine transactions and card purchases. Though the cause still remains a mystery, this incident demonstrates the vulnerability of interdependence among networks run by technology.

The most critical systems such as water and energy, transportation, and communication are especially susceptible to cyberattacks due to the intimate connection between each sector. For example, a successful attack on electric power networks would result in outages in power generation and distribution, disrupting communications networks and supply of water as well. Most critical infrastructures are dependent on information systems, leading to a new research area of critical information infrastructure protection (CIIP). As seen by its dependence, this area is considered a cross-sector activity that should be viewed in a holistic perspective.

The number of successful cyberattacks on critical infrastructure have been on a steady rise over the past decade. In a 2016 report on critical infrastructure regarding 575 operators from 20 countries, 76% reported that cyberattacks on critical infrastructure have grown more sophisticated, and 44% said they have been targeted by malicious attacks. Many of these attacks are related to both IT networks and operational technology systems. Though OT systems are rarely vulnerable to attacks, due to the common IT network vulnerabilities, both systems have been the target of cybercrimes involving malware, particularly crypto-ransomware. There have already been reports of a number of ransomware attacks against critical infrastructure companies including various educational facilities and hospitals.

Cyberattacks on critical infrastructures have major economic implications and are the seeds of conflicts between nations. Cyberattacks on critical infrastructure can result in a significant economic stagnation, especially when targeted against power systems. In 2015, a Russian hacking group known as ‘Sandworm” caused a power cut in Ukraine, which cut off access to power for around 255,000 people. A power outage may last from just a few hours to several weeks, and if the outage continues for weeks, the economic effects would last for years. Because of such massive impacts posed by the interruption of power systems, they are placed in

high priority for critical infrastructure protection. Moreover, as recent cyberattacks on critical infrastructures are suspected to be backed by certain nation-states, cyberattacks may become a means for political exchange. This proposed cyber-war may lead to deepening conflicts among nations and interventions in other nations' affairs. After increases in expected cyberattacks on Ukraine after Russia's invasion, the US, Australia, Canada, New Zealand, and the UK have released a joint Cybersecurity Advisory (CSA) to warn target organisations of malicious cyber activity. The CSA provides an overview of state-sponsored cyber operations and cyber threat groups to help protect against potential cyber threats. Like this, in response to cyberattacks on critical infrastructure, especially those suspected to be government-supported, states have been putting effort to identify the attacker and cooperate with the international community to provide aid on enhancing cyberspace security.

Current trends in information technology no longer leave critical infrastructures safe from cyber-attacks, despite being separated from external networks like the internet. Attackers are developing a higher understanding of administrative operations and configurations of power systems. Furthermore, when also considering the potential conflict between nations rising from sponsored cyber-attacks, it is necessary to have a collaborative effort between private industries and sectors of the national government to sufficiently strengthen the protection system.

Past Actions by Nations and Organisations

The Budapest Convention (ETS No. 185)

Otherwise known as The Convention on Cybercrime, The Budapest Convention provides a legal framework that brings together international states and parties to cooperate with each other and share their experiences regarding cybercrime. When first opened in Budapest, Hungary, 2001, the treaty was negotiated by members of the Council of Europe, USA, Canada, Japan, and South Africa, but became open for any state to become accessioned. The convention requires states to criminalise offences ranging from interference to computers and illegal access to data and systems. States are also encouraged to set procedural law tools to work towards creating a system to efficiently investigate and protect from cybercrime. Most importantly, the convention aims to provide a medium for international cooperation.

Parties of the convention are members of the Cybercrime Programme Office of the Council of Europe (CPROC) and the Cybercrime Convention COmmittee (T-CY). The CPROC manages capacity building projects to assist member states to create necessary capacities for dealing with cybercrime and other cases involving electronic evidence. The T-CY allows members to facilitate the application of the treaty by sharing information or further developing the Budapest Convention through interpretation from Guidance Notes or additional protocols.

Figure 2: Sectors in the Budapest Convention, Council of Europe 2018

Moreover, the convention encourages international cooperation on cybercrime and electronic evidence through the 24/7 Network established under the treaty. The Network facilitates assistance among countries for investigations or proceedings regarding cyber crimes or for collection of evidence. States that have requested accession or have become acceded may receive technical assistance and resources. If a small country is unable to prepare the resources to negotiate agreements to gain electronic data, the partner countries in the Convention can provide immediate assistance once the country decides accession. Until now, the Budapest Convention remains the "most relevant binding international treaty on cybercrime and electronic evidence" with its large network of practitioners.

The UN Group of Governmental Experts report (UN GGE)

In 2004, the General Assembly established the GGE to examine ICT developments on national security and military affairs. The GGE comes together in their meetings and submits their report to the General Assembly. Since 2004, there have been three consensus reports (2010, 2013, 2015) made from six GGEs regarding the field of information and telecommunications in the context of international security proposals. The failure to produce a consensus report in the 2017 GGE seemed to mark the end of the GGE, but the 2019 Resolution 73/266 passed by the General Assembly established another GGE in an attempt to extend the process. The following 2021 GGE adopted a consensus report that reaffirmed serious ICT threats against critical infrastructure. The 2013 report has affirmed that international law including principles of state sovereignty and non-intervention applies in cyberspace. The following report adopted in 2015 further proposes a normative framework for state behaviour regarding cyber capabilities. Recognizing the increasing dangers of cyber conflicts in the future, the report makes 11 recommendations for new norms and principles, particularly suggesting the development of measures to create cooperative mechanisms between countries. In 2017, the GGE was unable to meet a consensus on state rights to respond to international ICT crimes and the applicability of international humanitarian law in cyberspace. The re-established GGE in 2021 then decided to emphasise state jurisdiction to establish the policies and necessary mechanisms to protect from ICT within their territories. It stated that the international humanitarian law is only applicable during situations of armed conflict. Mainly, through its series of reports, the GGE has outlined the global agenda and confirmed the application of international law to cyberspace. At its current situation, the GGE has uncertain future expectations regarding its continuation.

General Assembly Resolution 74/247 (2019)

In 2019, the UN General Assembly adopted a resolution to draft a comprehensive cybercrime treaty binding for all states. To this end, the resolution created the Ad Hoc intergovernmental committee, which was scheduled to hold its first sessions in 2022. The resolution was considered as a key step towards recognizing the need for an international consensus on cybercrime goals. States were incredibly divided on the vote, with many parties to the Budapest Convention going against the resolution. Opponents were concerned that the vague

treatment of cybercrime could leave spaces for potential abuse of human rights with an exclusion of civil society. Member states were also divided on fundamental issues such as defining what cybercrime is and how governments should take part in regulating the internet and enforcing data investigations. The latest session (6th) was held in September 2023, New York, and its concluding session is expected in February 2024.

Stances of Major Countries and Non-Governmental Organisations (NGOs)

North Atlantic Treaty Organization (NATO)

In the Strategic Concept adopted from the 2019 NATO Summit in Lisbon, NATO recognised that cyber attacks had the potential to threaten national prosperity, security, and stability. NATO and its Allies are attempting to strengthen their responses to malicious cyber activities. In 2016, the Allies have implemented a Cyber Defence Pledge to be committed to new goals to enhance cyberspace stability and defence systems with priority, including critical infrastructures. They are committed to actively counter the full range of cyber threats through collective actions. At the 2023 NATO Summit in Vilnius, the Allies attempted to enhance cyber defence by addressing significant malicious cyber activities through their launch of the NATO's Virtual Cyber Incident Support Capability (VCISC). Their new concept will integrate NATO's political, military, and technical defence levels and utilise the private sector as necessary.

NATO currently has the NATO Cyber Security Centre (NCSC) based at Supreme Headquarters Allied Command Europe (SHAPE) to protect NATO's networks through a centralised cyber defence system amidst a rapidly changing technological environment. Allies have enhanced their defences by sharing information and practices along with the conduct of cyber defence exercises. These regular exercises are targeted to integrate cyber defence elements and diverse considerations, enhancing capabilities for future cyber education and training. NATO is particularly focused on training for the maintenance and enhancement of NATO ICT systems as seen by the multinational and interdisciplinary cyber defence hub NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the NATO Communications and Information (NCI) Academy promoting training from different countries.

Apart from working amongst its allies, NATO also cooperates with the European Union (EU), the UN, the Organization for Security and Cooperation in Europe (OSCE), and others. It works on promoting cooperation in multiple areas including research, training, and exercises regarding cyber threats.

United States of America

The US government has consistently expressed concerns over cyber threats on essential systems including critical infrastructure. It defines critical infrastructure as "assets, systems, and networks that provide functions necessary for our way of life" and identifies 16 critical infrastructure sectors as subjects of focus. The Department of Homeland Security (DHS) is currently playing a major role in safeguarding critical infrastructure from cyberattacks. It is in charge of the overall federal effort to protect critical infrastructure from threats. In 2018, the Cybersecurity and Infrastructure Security Agency (CISA) was founded as an operational component of the DHS to oversee and enhance US cybersecurity efforts regarding cyber and physical infrastructure that people rely on daily. The CISA guides state, local, and industry partners in identifying and protecting critical infrastructure sectors. With its partners, CISA conducts cyber and physical security exercises to identify the most effective practices to improve the resilience of critical infrastructure. Exercises also help plan for the future and set up education efforts. A portfolio of these exercises, including cybersecurity scenarios and cyber-physical convergence scenarios are available online.

The US is also an active player in cooperating with other nations for the maintenance of cybersecurity. The US has actively negotiated protocols in the Budapest Convention and is currently a leading donor to the Council of Europe Cybercrime Program, which is responsible for providing advice and assistance to help expand and implement the Budapest Convention. However, it has strongly shown disapproval with the passing of a Russia-led cybercrime UNGA resolution, expressing concerns for limiting internet freedom. The US has long claimed that the internet is a platform outside state control. It has thus been reluctant in drafting fixed terms for a treaty regarding cybercrime and security.

Russia

Russia is an active player that has long been promoting a global cybercrime treaty to replace the Budapest Convention. Although it is a member of the Council of Europe, Russia has not yet joined the Budapest Convention. In recent years, Russia has significantly expanded its policies to enhance control over ICTs, particularly over privacy, internet content and infrastructure.

In 2019, Russia submitted and passed the UNGA resolution titled "Countering the Use of Information and Communications Technologies for Criminal Purposes" along with seven co-sponsors: China, Cambodia, Belarus, Myanmar, Nicaragua, North Korea, and Venezuela. It creates an expert group with the purpose of drafting terms of reference for a multilateral treaty. Noticeably, China and Cambodia have common grounds in employing more authoritative policies regarding technology regulation. Cambodia has also proposed a cybercrime law that could threaten surveillance of users including whistleblowers, indicating a potential restriction of free expression and reduction of individual privacy. Considering such, the resolution seems to be a step towards enhancing control over cyberspace in favour of the more authoritarian regimes' desires. The resolution has no mention of international human rights law being included in cyberspace.

Russia's support of the establishment of institutional mechanisms are largely seen as an attempt to legitimise its extensive domestic surveillance over the internet to suppress political dissent and enhance regime security.

China

China currently has policies that pose strict control over technological systems and internet platforms. The Chinese government has been attempting to use the idea of combating cybercrime as a justification for Internet censorship and regulation. It has joined Russia in leading the passage of the UNGA resolution to define terms for internet freedom. With Russia, it has criticised the Budapest Convention and the GGE for not being inclusive enough, instead gathering support for the Open-Ended Working Group (OEWG). As the OEWG is open to all member states, China and Russia are attempting to use support of governments in favour of an

authoritarian Internet to shape discussions on cybersecurity towards the direction they are pursuing.

Despite allegations of various countries about cyber activities attributed to Chinese actors, China has consistently denied accusations of being part of cyberattacks against critical infrastructure of other nations. It has argued that it is also a victim of cyber threats and expressed desire to cooperate with the international community to address cybersecurity challenges.

Possible Solutions

1. *Reaching a Consensus on Fundamental Terms Regarding Cybercrime*

There has not yet been a consensus among UN member states about the fundamental terms regarding cyberattacks. To accurately address the cyberattacks on critical infrastructures, there is a need for member states to make an agreement on what constitutes a cybercrime and what an overarching treaty would include. If cybercrimes are worded vaguely, laws can be used to target civil society actors such as whistleblowers, activists, and journalists, particularly in governments arguing that cybercrime includes disclosure of information violating a government policy. A lack of a clear consensus leads to a possibility of human rights infringement and arbitrary interpretations. Thus, terms should be clear and precise so that subjects can discern which actions are prohibited in order to adjust their behaviour accordingly. Ambiguous terms can also make it difficult to carry out investigations and accuse parties for violating international cyber law.

2. *Collaboration Between Firms and Governments*

Technological tools, information, and security conditions are constantly changing. Thus, it is difficult for governments to solely be in charge of setting regulatory tools and defence measures. There is a need for intensive strategic and operational collaboration between the government and related major firms. Through constant collaboration, exchange of information, and division of work can make way for a more efficient approach to tackle cyber attacks on critical infrastructure.

3. *Strengthening Cyber Defense Systems*

The most fundamental but important method to resolve issues of cyber attacks on critical infrastructure is to strengthen the national cyber defence systems. Governments should devote more resources to strengthen defence systems most vulnerable to attacks and draft plans for expected situations of a series of shutdowns possibly caused by the interconnection of critical infrastructure. Limiting data collection to a scope strictly necessary for a just purpose may also be a solution to reduce systems' vulnerability. Because states have differing capacities for defending against cyberattacks, it is crucial for the international community to cooperate with each other and provide assistance to those in need.

Questions to Consider

- How can countries verify attacks on critical infrastructure when many are reluctant to discuss or admit cyberattack capabilities?
- What is your country's stance regarding the creation of an international cybercrime law? Is it hesitant considering possible human rights infringement cases or is it in favour of stricter government control over the internet?
- Considering the continuation of the rapid development of technology and ICTs, how should the international community and individual member states respond to future advancing threats to critical infrastructure?

Bibliography

Alcaraz, Cristina, and Sherali Zeadally. “Critical Infrastructure Protection: Requirements and Challenges for the 21st Century.” *International Journal of Critical Infrastructure Protection*, vol. 8, 2015, pp. 53–66, https://doi.org/10.1016/j.ijcip.2014.12.002.

Brown, Deborah. “Cybercrime Is Dangerous, But a New UN Treaty Could Be Worse for Rights.” *Human Rights Watch*, Just Security, 13 Aug. 2021, www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.

Cabrera, Ed. “Protecting Critical Infrastructure From Cyberattack.” *Risk Management*, vol. 63, no. 8, Oct. 2016, https://www.proquest.com/openview/42970b7ca43d86aadb80b6b681fcf992/1?pq-origsite=gscholar&cbl=47271.

Cisco. “Addressing Critical Infrastructure Cyber Threats for State and Local Governments.” *Cisco*, Chertoff Group, 2015, www.cisco.com/c/dam/global/en_sg/assets/pdfs/govt_n_critical_infra_2169_cistcg_cisco_white_paper_v4-1.pdf.

Council of Europe. “The 24/7 Network Established Under the Convention on Cybercrime.” *Council of Europe*, www.coe.int/en/web/cybercrime/24/7-network-new-. Accessed 2 Dec. 2023.

Council of Europe. “The Budapest Convention on Cybercrime: Benefits and Impact in Practice.” *Council of Europe*, Cybercrime Convention Committee (T-CY), 13 July 2020, rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

"Critical Infrastructure Security and Resilience." *Cybersecurity and Infrastructure Security Agency CISA*, CISA, www.cisa.gov/topics/critical-infrastructure-security-and-resilience. Accessed 3 Dec. 2023.

"Cyber Attacks on Critical Infrastructure." *Allianz Commercial*, June 2016, commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

Gullo, Karen, and Katitza Rodriguez. "UN Cybercrime Draft Treaty Timeline." *Electronic Frontier Foundation*, 7 Apr. 2023, www.eff.org/deeplinks/2023/04/un-cybercrime-treaty-timeline#:~:text=November%2019,the%20EU%2C%20and%20other%20nations.

Lehto, Martti. "Cyber-Attacks Against Critical Infrastructure." *Computational Methods in Applied Sciences*, vol. 56, 2022, pp. 3–42, https://doi.org/10.1007/978-3-030-91293-2_1.

Lewis, James A. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Association*, June 2010, www.armscontrol.org/act/2010-06/multilateral-agreements-constrain-cyberconflict.

Moynihan, Harriet. "The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention." *Chatham House*, Dec. 2019, www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

Nato. "Cyber Defence." *NATO*, 14 Sept. 2023, www.nato.int/cps/en/natohq/topics_78170.htm.

NIAC The President's National Infrastructure Advisory Council. "Addressing Urgent Cyber Threats to Critical Infrastructure." *CISA*, Aug. 2017, www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

Noguchi, Mutsuo, and Hirofumi Ueda. “An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures.” *NEC Technical Journal*, vol. 12, 2017, https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html.

Office, U.S. Government Accountability. “Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure.” *US GAO*, 7 Feb. 2023, www.gao.gov/products/gao-23-106441.

Rodriguez, Katitza, and Meri Baghdasaryan. “UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope.” *Electronic Frontier Foundation*, 15 Feb. 2022, www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among.

Schmitt, Michael. “The Sixth GGE and International Law in Cyberspace.” *Just Security*, 10 June 2021, www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

Schneier, Bruce. “Cyberconflicts and National Security.” *UN Chronicle*, United Nations, Aug. 2013, www.un.org/en/chronicle/article/cyberconflicts-and-national-security.

Sherman, Justin, and Mark Raymond. “The U.N Passed a Russia-Backed Cybercrime Resolution. That’s Not Good News for Internet Freedom .” *The Washington Post*, 4 Dec. 2019, www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/.

“United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime.” *Office of Public Affairs*, US Department of Justice, 12 May 2022,

www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat.