STUDY GUIDE

United Nations Security Council

Cyberspace Dynamics in the AI Era: Tackling Threats to International Peace and Security

President
Anna Golikova
annagolikova2107@gmail.com

President
Apostolos Symeonidis
apostolossymeo@gmail.com

Revised By: Simrit Mann, Kristian Walters

WELCOME NOTE

Esteemed Delegates,

It is our pleasure to officially welcome you all to the Security Council of GIMUN 2021.This Study Guide can be used as a compass to indicate how to organise and conduct your research, not only for the topic but also for your country's policy. The Security Council is considered to be one of the most challenging, as well as exciting and rewarding committees of the conference and we are looking forward to dealing with these challenges and experiencing the thrill of debate together.

The topic for this year's Security Council is "Cyberspace Dynamics in the AI Era: Tackling Threats to International Peace and Security". When we chose this topic, we wanted to challenge you, the delegates, to tackle complicated and multifaceted situations and issues that would require you to think outside the box. "Cyber Warfare Threats to Peace" is a complex and multidimensional matter which will play a determining role in the shaping of global power dynamics. Despite the information that this Study Guide will provide you with, we strongly encourage you to conduct your own personal research, both on the topic and on your personal country's position.
We are certain that you will provide us with structured, well written position papers and a constructive debate during the conference. We expect delegates to be respectful, devoted, and eager to make the most out of this experience, but most importantly, we want you to enjoy yourselves and share our passion and love for debating. During your experience, we will be at your disposal for any possible remarks and inquiries that may arise.

We are looking forward to seeing you all.
Best Wishes,
Apostolos, Anna & Ibrahim

CONTENTS

1. DESCRIPTION OF THE SECURITY COUNCIL

1.1 ABOUT THE SECURITY COUNCIL

The United Nations Security Council is one of the six principal organs of the United Nations, Article 7 of the Charter of the United Nations (UNC). Its main goal is the maintenance of international peace and security under chapters V and VII.[1]

The council is composed of fifteen members. Five of them are permanent (commonly known as 'the P5'): the People's Republic of China, the French Republic, the Russian Federation, the United Kingdom and the United States of America. The P5 members of the United Nations Security Council have veto power, meaning that if present, any substantial decision to be taken can be blocked if any of the 5 permanent members disagrees and exercises their veto power. The other ten members of the Council are non-permanent. The non-permanent members are elected by the United Nations General Assembly, taking into consideration the chosen states' contribution to the actions of the United Nations and the need for an equitable geographical distribution for a term of two years.[2] The current non-permanent members are: Estonia, India, Ireland, Kenya, Mexico, Niger, Norway, Saint Vincent and the Grenadines, Tunisia, and Vietnam.[3]

Under Section VII of the Charter of the United Nations, the United Nations Security Council takes the lead in investigating any dispute or situation which might lead to international friction or cause turbulence in the global dynamics as well as in determining the existence of a threat to peace. Its first measure to deal with possible imbalances is to recommend methods of adjusting such disputes or establish the terms of settlement using peaceful means. Furthermore, the Council is entitled to call on Members to apply economic sanctions and other measures not involving the use of force to stop aggression. If non-military measures do not bring high-yielding results, the Security Council can take military action against an aggressor. Lastly, it is rightfully permitted to recommend to the General Assembly the appointment of the Secretary-General[4] and, together with the Assembly, elect the Judges of the International Court of Justice (ICJ).

The Security Council is the most powerful body within the United Nations system, as it is the only organ able to take measures that are legally binding for all 193 United Nations member states under Article 25 of the Charter of the United Nations. In light of this, the Council can take several actions in case of turmoil in the global scenery. It can decide upon the existence of a threat to peace and ways to resolve the emerging problem and call upon the parties involved to maintain a specific

[1] "United Nations Security Council |." United Nations. United Nations. Accessed March 15, 2020. https://www.un.org/securitycouncil/.

[2] "Current Members Security Council." United Nations. United Nations. Accessed March 15, 2020. https://www.un.org/securitycouncil/content/current-members.

[3] "Current Members Security Council." United Nations. United Nations. Accessed March 15, 2020. https://www.un.org/securitycouncil/content/current-members.

[4] "FAQ Security Council." United Nations. United Nations. Accessed March 15, 2020. https://www.un.org/securitycouncil/content/faq#threat.

position. Amidst others, the Council can adduce the signing of agreements, provide guidelines and principles to ensure that the arrangement is fair and precise, entertain mediation processes between parties and launch specific missions and envoys. In cases of aggravation, the United Nations Security Council has the authority to ask for ceasefire and deploy military observers or peacekeeping forces. The authority of the Council also encompasses the adoption of measures, such as economic sanctions, embargoes, rupture of diplomatic relations, blockades and collective military action under the prerequisites set by the Charter of the United Nations. The Security Council's actions are not only the result of the cooperation with single United Nations member states, but it can also coordinate its actions with those of regional organisations such as the League of Arab States, the African Union, North Atlantic Treaty Organisation (NATO), or the European Union, to achieve their main goal which is international security and safety.[5]

In case the Council is not able to pass a resolution, the committee is still able to publish a Presidential Statement. These statements address the topic and contain official recommendations given by the Council but are not legally binding in any way.[6]

1.2 Mandate and Instruments

The mandate of the Security Council is laid down in Article 24 of the Charter:

In order to ensure prompt and effective action by the United Nations, its members confer on the Security Council, primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf.

The decisions shall be made by an affirmative vote of nine members, considering the concurring votes of the permanent members. The right to veto is one of the most significant features of the Security Council. Article 27(3) of the Charter states that all substantive decisions of the Council must be made with the "concurring votes of the permanent members". Permanent members use the veto to protect their national interests or to highlight a certain decision of particular importance to a state. The veto has been recorded 293 times since 1946 when the USSR cast the first veto on a draft resolution regarding the withdrawal of foreign troops from Lebanon and Syria.

1.3 Functions

The primary responsibility of the Security Council is the maintenance of peace and security. It is important to note that it is the only United Nations body with the power to make legally binding decisions. The functions of the Security Council are outlined in Chapters VI-XII of the Charter of the United Nations. Thus, Article 39 of the Chapter VII indicates that:

[5] CFR Staff. The UN Security Council. (2018, September 24). Retrieved from https://www.cfr.org/backgrounder/unsecurity-council.

[6] "UNSD - Methodology." United Nations. United Nations. Accessed March 15, 2020. https://unstats.un.org/unsd/methodology/m49/.

The Security Council shall determine the existence of any threat to the peace, breach of peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42 to maintain or restore international peace and security.[7]

Members of the UN, as is stated in Article 25, are obliged to accept and execute the decisions of the Security Council.

1.4 Recent History

In the XXI century, the Security Council is increasingly facing criticism and this issue has been on the agenda of the General Assembly for several years. It is widely accepted that the geopolitical situation has changed since the establishment of the United Nations in 1945. At that time, the world population was slightly less than 2 billion and now 7 billion people live on the planet.[8] In 1945 more than half of today's United Nations member states were not fully independent. Nowadays, after the admission of South Sudan, there are 193 members in the United Nations. In the XX century, wars were fought mainly by states and between states. However, in the modern world, conflicts have significantly transformed. In the XXI century, the world faced an increase in non-international conflicts. The new reality shows that conflict is increasingly becoming hybrid. Countries use not only conventional weapons, but also modern technologies to assert their power. Recent conflicts have shown that countries are ready to use cyber weapons to gain advantage. This forces us to rethink the concepts and approaches that were previously adopted.[9]

1.5 Introduction to the Topic:

Cyberspace has undergone rapid development in the last decade; bringing with it great possibilities, chances and risks. A 2011 Norton study has shown that in the preceding year, roughly one million users fell victim to cybercrime events. The combination of all possible global security leaks might have created a rift between citizens and their government. This begs the question of whether there is a need for an implementation of rules for data protection and privacy in the internet, improving the international response to cyberwarfare.[10]

Similarly, data protection in the internet should be regarded as a major component for achieving international peace. Malware from other territories disrupt international peace, as it might hamper with security problems – ranging from governmental institutions to private organisations. International leaks might interfere with peace relations between the nations, while cyberspace could be seen as the new battleground for terrorism.[11] Cyberwarfare potentially infringes

[7] UN Charter https://www.un.org/en/sections/un-charter/un-charter-full-text/ (date of access: 06.02.2021)2

[8] UN Department of Economic and Social Affairs, 'World Population 2012 Wall Chart' (date of access: 06.02.2021)

[9]Perception of Security https://www.havc.se/res/SelectedMaterial/20142224ilperceptionsofsecurity.pdf (date of access: 06.02.2021)

[10] Cybersecurity: a global issue demanding a global approach https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html (date of access: 06.02.2021)

[11] https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity (date of access:07.02.2021)

international law and, thus, disrupts international bonds between countries. Furthermore, a resolution by the Inter-Parliamentary Union acknowledges that "the use of the Internet by terrorists or terrorist organizations for illegal activities, in particular to raise funds, enlist members or publish ideas inciting people to violence and hatred" is needed to be addressed quickly. The concern has inspired former Secretary-General of the United Nations Ban Ki-moon to assemble 15 experts[12] from different countries to discuss the underlying problems addressing cybersecurity and cyberspace.[13] To this date, although the use of the internet has been proposed as a human right by the United Nations Special Rapporteur, the only article abstractly referring to cyberspace or cybersecurity by the United Nations is Article 51 in the Charter of the United Nations, which reads:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[14]

In order to establish a safe space for both governmental and non-governmental users, cooperation between United Nations countries could ensure a quick response to any threats regarding cyberspace. Although several Member States are still lacking an urgent cybersecurity plan, it should be the United Nations' utmost urgency to address the matter adequately and swiftly.

2.1 Historical background and Past Resolutions

In the Report of the High-Level Panel of Experts on Information and Communication Technology (ICT; for technologies that provide access to information through telecommunications, it is tied with the term "information technology (IT)", however it focuses primarily on communication technologies; it includes the Internet, wireless networks, cell phones, and other communication mediums[15]) in 2000, the United Nations recognised the importance of ICT. The Report highlighted the benefits of ICT for countries that are ready to harness their potential, and highlighted the urgent need for an international ICT action plan. In 2002, the United Nations adopted Resolution 57/295, entitled "Information and Communication Technologies for Development." The resolution reaffirmed the desire to develop a unified ICT strategy.[16] One of the most recent documents on our agenda is Resolution 73/27, adopted by the General Assembly on 5 December 2018, which states

[12] https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity (date of access:07.02.2021)

[13] https://www.un.org/sg/en/formersg/ban.shtml (date of access: 07.02.2021)

[14] https://legal.un.org/repertory/art51.shtml (date of access: 07.02.2021)

[15] https://techterms.com/definition/ict (date of access: 07.02.2021)

[16] https://unctad.org/system/files/official-document/ares57d295_en.pdf (date of access: 07.02.2021)

that: "The UN should play a leading role in encouraging dialogue among Member States to develop a common understanding and attitude towards ICT security". [17]

One of the most important agreements in the field of information space is the Budapest Convention on 23 November 2001. It was adopted by the Council of Europe. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing mainly with copyright infringement, computer fraud, child pornography, hate crimes, and network security violations.[18]

Also, as conditions and guarantees, the Convention requires the provision for the proper protection of human rights and freedoms, including the rights arising in accordance with the obligations under the European Convention on Human Rights (1950), the International Covenant on Civil and Political Rights (1996), as well as other relevant international instruments in the field of human rights, and should include the principle of proportionality.

International clubs of states pay attention to the problems in the information field. In 2000, G8 Heads of State and Government drafted the Okinawa Charter for the Global Information Society.[19]

Despite the fact that the United Nations and the world community recognised the significance of cyberspace and the possibility of the emergence of threats associated with its vulnerability, it has not yet been possible to reach a joint agreement on cybercrime. In 2019, Russia presented the document "Countering the use of information and communication technologies (ICT) for criminal purposes." Resolution A/C.3/74/L.11 decided to establish an ad hoc open-ended intergovernmental committee of experts representing all regions to develop a comprehensive international convention against the unlawful use of ICT. The adoption of this resolution reaffirms the urgency of the problem while emphasising that progress in this area develops slowly. [20]

2.2 Cybersecurity in the AI Era

Artificial intelligence (AI) is a wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence.[21] The use of AI can significantly benefit cybersecurity as automated techniques will be capable of detecting cyber threats. Moreover, AI can help develop prevention and recovery strategies. However, further advancement in AI can give way to new types of cyber threats. AI can also hack a system's vulnerability much faster and efficiently than a human. Moreover, it can be used to disguise attacks so effectively that one might never know that their network or device has been affected.[22] AI creates

[17] Resolution 73/27 https://undocs.org/A/RES/73/27 (date of access: 07.02.2021)

[18] Budapest Convention https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (date of access: 07.02.2021)

[19] The Okinawa Charter on Global Information Society https://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf (date of access: 07.02.2021)

[20] https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/187 (date of access: 07.02.2021)

[21] https://builtin.com/artificial-intelligence

[22] https://www.entrepreneur.com/article/339509

new solutions, but also creates new problems that we could not face at the dawn of the Internet and cybersecurity in the beginning of the 21st century. Future cyberwarfare will inevitably be linked to the development of AI and therefore we need to understand the nature of technological change and cyberspace's characteristics.

2.3 Features of Cyberspace

Ottis and Lorents from the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence based in Tallinn, Estonia, defines cyberspace as "a time-dependent set of interconnected information systems and the human users that interact with these ICT systems" (Ottis & Lorents, 2010). It is important to note that we often face the problem of attribution with ICT sector. According to political scientist H. Lin, there are currently no effective evidentiary standards in international politics that could confirm which subject committed the attack.[23] Cybercriminals can carry out attacks from anywhere in the world, and in many cases, identifying the suspect is an unsolvable task.

An important characteristic of cyberattacks and cybercrimes is unpredictability. Criminals do not only go unnoticed, they can also attack at any moment. These unpredictable attacks have also led to rapid technological development. In recent years, the number of Distributed Denial of Service (DDoS) attacks carried out on a computer system in order to make it difficult for system users to access it has increased significantly. They also create a situation that requires actors to be ready to protect the network from various attacks. This is the case for both classified and unclassified attacks.

The Information Technology field is characterized by its technological complexity. However, this field is also known for a major problem: the fragmentation of leadership. Decision-making in the ICT sector involves several actors, IT specialists and representatives of the administrative apparatus. This creates difficulties in the decision-making process, because managers, and non-information security specialists, make the decisions. Cybersecurity specialists are employees with professional ICT skills. This category includes both top-level specialists (developers and analysts of computer systems, programmers, computer specialists, electronics engineers, communication and instrument engineers) and mid-level specialists (electronics and telecommunications technicians, radio and telecommunications equipment technicians and operators). Although they have the requisite technological knowledge, they do not make key policy decisions that are approved by politicians and administration officials.

2.4 Cybersecurity Threats

When we talk about threats in the field of information security, it is essential to note that we are talking primarily about artificial threats that directly depend on a person's implementation and are divided into intentional and unintentional. ICT crime is a deliberate threat. The form of cyber threats (threats in the field of ICT) differs significantly from traditional threats to strategic security, and in

[23] https://cyber.harvard.edu/cybersecurity/sites/cybersecurity/images/Lin-Cyber_Conflict_and_National_Security_2012.pdf (date of access: 07.02.2021)

many aspects this type of threat still remains unexplored.[24] Countries and their citizens around the world are becoming increasingly vulnerable to cyber threats: in the first half of 2020 alone, the number of cyber attacks increased by almost a quarter.

Information security threat's classification:

- Distribution of inappropriate and dangerous content
- Information leak
- Data loss
- Fraud
- Cyberterrorism
- Cyberwarfare

Thus, each cyberthreat (threats in the ICT sector) can vary significantly from traditional threats to strategic security, and in many aspects, this type of threat is still unexplored.

2.5 Cyber Warfare as a Part of Global Hybrid Warfare

In order to combat cyberwarfare, it is important to examine it through the scope of a broader concept – hybrid warfare. Hybrid warfare is a concept in political strategy which blends conventional methods of warfare with other tactics, such as media interference and propaganda (fake news), political warfare and cyberwarfare.

Cyberwarfare can often act as a supplement to conventional military tactics. A cyberattack may have the necessary capability to disrupt an energy network or any infrastructure that is vital to the other party. Therefore, the parallel use of cyberwarfare by an aggressor may ease the passage of troops and vehicles, as well as weaken the defensive capability of the enemy. Cyberwarfare methods may also be used when conventional methods are unfeasible or unavailable.

Today, the most active use of cyberwarfare by state parties is disguised as cyberterrorism by independent parties, unaffiliated sympathisers and lone wolves. Such is the case with election interference, targeted spread of viruses, malware and ransomware, leaking of confidential data and digital infiltration. The latter can also be classified as a form of intelligence gathering, which (in case of clear evidence of state party involvement) is a clear breach of international law and may provoke a direct confrontation. However, due to the somewhat cleaner nature of this type of espionage, it is extremely difficult to trace its source, which also explains why hacking is slowly making older, more traditional forms of espionage obsolete.

[24] https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198803164.001.0001/oxfordhb-9780198803164-e-29 (date of access: 07.02.2021)

2.6 CYBERTERRORISM: CASES AND PRECEDENTS

In order to better understand the technicalities and actors in case of cyberterrorism, analyse the related cases below.

One of the first examples of international cyberterrorism occurred in the Estonian digital space in 2007.[25] Following a series of protests against the removal of a Soviet-era monument dedicated to Soviet troops who fought in World War II, several major Estonian websites, including banks, government agencies, political parties and newspapers were subject to cyberattacks that blocked access to said websites. Some hackers managed to gain access to the websites' servers, defacing frontpages with pro-Russian statements and propaganda.

Thus far, only one Estonian national was convicted in connection to the cyberattacks. However, the scale of the incident indicated that more than one individual was responsible for coordinating and carrying out the attack, and that perhaps a state party was involved. Various high-ranking Russian political figures claimed responsibility for the attack and hinted at its source. However, the allegations were hard to prove, and the exact source of the attack remains undetermined. The international community responded to the attacks by stressing the increasing importance of cybersecurity as an integral part of any modern military doctrine. Since August 2008 the NATO Cooperative Cyber Defence Centre of Excellence has operated out of Tallinn, Estonia.[26]

A broader, larger-scale attack took place during the Russo-Georgian war of 2008. In this case there were actors acting on both sides, since Russia and Azerbaijan were also targeted, in addition to Georgia. The attacks generally followed the scheme of the 2007 Estonian incident, with media outlets and the government. The attack was so severe that Georgian government websites had to migrate to foreign servers, with help from the United States and Estonia. The attacks once again received condemnation from the international community, but the exact source of the attack remained a mystery53. The official position of the Russian government is that the attacks were carried out by lone sympathizers, and the case should be treated under the definition of international cyberterrorism.

Today, sporadic cyberattacks and defacements continue to target political websites, with nearly any party having the potential to carry out such kinds of attacks.

2.7 CYBERCRIME THROUGH THE SCOPE OF THE UNSC

With the means of carrying out cyber attacks becoming increasingly available, and the upgrade of anonymization technologies, fighting cybercrime on a global scale seems nearly impossible. However, there are some measures already in place by the international community to combat cyberwarfare and cyberterrorism.

Before hastily establishing a possible perspective on the Security Council, it is important to examine other United Nations bodies that fight cybercrime more directly. In particular, the International

[25] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (date of access: 07.02.2021)

[26] https://ccdcoe.org/ (date of access: 07.02.2021)

Telecommunications Union (ITU), which has a Cybersecurity Programme. Although extremely prospective and broad, the outlook of the ITU lacks universality and enforcement possibilities. Among other aspects, the ITU deals with aiding states in developing national cybersecurity strategies, manages the Global Cybersecurity Index (GCI), provides assistance in developing related legislation, and publishes insights on current cybersecurity threats. Many of the practices currently used by the ITU may be adopted in a new framework by the Security Council. Another United Nations body currently fighting cybercrime is the United Nations Interregional Crime and Justice Research Institute's (UNICRI) Centre for Artificial Intelligence and Robotics. However, the official position of the abovementioned Centre has so far been rather general and inconclusive.

Among many other international organizations, the European Union Agency for Law Enforcement Cooperation (formerly EUROPOL), and the International Criminal Police Organization (INTERPOL) are investigating the issue. EUROPOL's involvement has largely been practical, With financial aid being allotted to build and strengthen existing oversight systems, assist in the investigations and develop national frameworks according to current EUROPOL laws s. INTERPOL and EUROPOL operate in similar ways, both work on a global scale and provide their members with all the necessary means of cooperation in the field. Practical approaches developed by both organizations could serve as an example for possible action authorized by the Security Council.

The United Nations Security Council has been carefully working towards developing a common cybersecurity framework. The Security Council has agreed to an equal application of international cyberspace law, which sets the legal framework for future action., No resolutions concerning cybersecurity issues have been adopted by the United Nations Security Council thus far. Draft resolutions for different aspects of cybersecurity have been forwarded to the United Nations General Assembly by three of its six main committees (the Disarmament and International Security Committee; the Economic and Financial Committee; and the Social, Humanitarian and Cultural Committee).[27] Perhaps the most noteworthy developments have taken place in the Disarmament and International Security Committee, regarded as a unique forum for key members such as the United States, China and Russia to discuss the "high end" of information security threats. Since 1998, the Russian government has annually introduced a draft resolution in the First Committee on "Developments in the field of information and telecommunication in the context of security".[28] With gradual changes, the non-binding resolution has been adopted by the United Nations General Assembly (UNGA) each year. However, the document remains a non-binding proof of concept, with tensions rising among the members of the international community.

Therefore, to establish a universal structure to fight cybercrime, the highest authority is needed to develop, promote and enforce a framework that fights cybercrime on a global level. The Security Council i decides what measures each Member State need to follow, and the Council Members should use their mandate to focus on cooperation, agree on common definitions and devise a universal outlook on possible future security threats in the scope of cybercrime.

Considering the history of cybercrime, its many forms and manifestations, as well as the development of adjacent technologies, such as artificial intelligence, the problem poses an existential risk comparable to threats associated with weapons of mass destruction. By developing

[27] https://freedomonlinecoalition.com/working-groups/working-group-1/cybersecurity-and-united-nations/ (date of access: 07.02.2021)

[28] https://ccdcoe.org/organisations/un/ (date of access: 07.02.2021)

a unified, swift and ground-breaking resolution the Security Council will set the agenda for regional and national development of sustainable solutions in the field.

2.8 BLOC POSITIONS

Countries have different economic opportunities for ICT development, which must be considered when analysing the barriers to reaching a single agreement. ICTs are of great economic importance, which is a factor in the growing rivalry between countries in this area. The United States is the largest global technology market, currently accounting for 32% of the total.[29]

Moreover, in modern society, the technological gap between countries continues to persist. "The Declaration on Development and International Cooperation in the 21st Century: The Role of Information Technology in the Context of a Knowledge-Based Global Economy", adopted by the Economic and Social Council on July 7, 2000, used the term "digital divide." In developing countries, ICT development is hampered by factors such as a lack of infrastructure, educational opportunities, investment, and Internet connectivity.

Some major cases listed below:

The **United States, the United Kingdom, and France:** The United States has significant cyberwarfare capabilities; recent allegations have also highlighted its controversial practise of intercepting civilian communications (collected from members of the North Atlantic Treaty Organization and other allies). It has come under significant international pressure from some of its allies after allegations that it tapped the communications of several word leaders. It has heavily defended the National Security Agency as an important aspect of its national defence plan, raising questions about whether it is ultimately about security from foreign threats or internal security. Allies including the United Kingdom and France have some of the most advanced cyberwarfare capabilities and have followed the lead of the United States in collecting information.

China: relations between the United States and China are harmed by their disagreements over information technology. The United States' government departments have identified China's People's Liberation Army (PLA) as the source of cyberattacks against the United States' government and key private companies. The Shanghai Cooperation Organisation (members include primarily China and Russia) defines cyberwar to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states". In September 2011, these countries proposed to the United Nations Secretary General a document entitled "International code of conduct for information security". The approach was not endorsed by most western countries as it revealed many hints on political censorship of the internet.

Russia: Russia co-sponsored a resolution to give states a greater role in governing the involvement of the internet at a meeting of the International Telecommunication Union in April 2013, joined by China, North Korea and Iran. This was rejected by the United States and other NATO allies, which caused some conflict. Russia's decision to grant asylum to Edward Snowden has also worsened relations with the United States over cyber security issues. In Russia, the term information security

[29] https://www.comptia.org/content/research/it-industry-trends-analysis (date of access: 07.02.2021)

is used more often in official documents than in cybersecurity.it implies the inclusion of the human dimension in the regulation of the ICT sphere.

Brazil and Developing Countries: As an emerging 'BRIC' economy, Brazil has become a key figure for the concerns of developing countries with regard to cyberthreats. The revelation that the United States may have tapped the phone of Brazil's president, Dilma Rousseff created tension between the United States and Brazil. and in Other world capitals, and calls were made for states to limit their online data collection activities or risk breaching international conventions on proper targets of espionage.

2.9 QUESTIONS A RESOLUTION MUST ANSWER

1. What will be the mechanism that ensures cooperation and compliance among the Members?
2. Given modern breaches in cybersecurity, how should "cyberwarfare" and "cyber-attacks" be legally defined? Define, or update, the legal definitions of cyber warfare, cybersecurity and cyber attacks.
3. With the number and sophistication of cyber-attacks increasing, what measures should be taken to prevent, or decrease, future state to state cyber-attacks?
4. Should an international framework be established to increase international cybersecurity?
5. Cyberthreats originating from non-state actors, specifically rogue and terrorist organizations, are often excluded in conversations regarding international cybersecurity. With increasing accessibility to tools of technological destruction among individuals and non-state actors, what should be done to ensure security from non-state actors and terrorist organizations?
6. Issues of personal privacy have become a contentious topic of debate with many civilians distrusting government surveillance. How can security be increased without violating the privacy of citizens? What measures can be taken to ensure the right to personal privacy?
7. Computer systems and informational technologies are fields of constant change and evolution. What tactics should be employed in order to keep up with advancements in cyber warfare technology?

3. BIBLIOGRAPHY / SUGGESTED READING

1. General Assembly, Developments in the field of information and telecommunications in the context of international security, UN document A/RES/53/70, 4 January 1999, retrieved from https://undocs.org/A/RES/53/70
2. General Assembly, Creation of a Global Culture of Cybersecurity, UN document A/RES/57/239, 31 January 2003, from http://undocs.org/A/RES/57/239
3. General Assembly, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, UN document A/RES/58/199, 30 January 2004 from http://undocs.org/A/RES/58/199
4. General Assembly, Report of the First Committee, "Role of science and technology in the context of security, disarmament and other related fields", UN document A/53/576, 18 November 1998, retrieved from http://undocs.org/A/53/576
5. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201, 30 July 2010 from https://undocs.org/A/65/201
6. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/68/98, 24 July 2013 from https://undocs.org/A/68/98
7. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/70/174, 22 July 2015 fromhttp://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
8. General Assembly, Letter Dated 12 September 2011 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN document A/66/359, 14 September 2011 from http://undocs.org/A/66/359
9. General Assembly, Letter Dated 13 January 2015 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN document A/69/723, 13 January 2015 from http://undocs.org/A/69/723
10. UN CHAPTER VII: action with respect to threats to the peace, breaches of the peace, and acts of ag-gression, retrieved from: http://www.un.org/en/sections/un- charter/chapter-vii/index.html

11. UNODC (United Nations Office on Drugs and Crime) The use of Internet for Terrorist Purposes: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

12. Norton Cyber Security Insights Report Global Results: https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf

4. COUNTRIES PRESENT IN THE COMMITTEE

1. Australia
2. Canada
3. Democratic Republic of Congo
4. Democratic Socialist Republic of Sri Lanka
5. Federal Republic of Germany
6. Federative Republic of Brazil
7. French Republic
8. Hellenic Republic (Greece)
9. Islamic Republic of Pakistan
10. Japan
11. Kingdom of Saudi Arabia
12. People's Republic of China
13. Republic of Colombia
14. Republic of Estonia
15. Republic of India
16. Republic of Kenya
17. Republic of South Africa
18. Republic of Turkey
19. Russian Federation
20. State of Qatar
21. The Republic of Korea
22. United Arab Emirates
23. United Kingdom of Northern Ireland and Great Britain
24. United Mexican States (Mexico)
25. United States of America