ThessISMUN 2018

Thessaloniki International Student Model United Nations

United Nations
First Committee of the General Assembly

Topic area A: 'Towards a new and comprehensive approach in addressing cyber warfare and increasing cyber security"

University of Macedonia
Thessaloniki, Greece

www.uom.gr/mun - www.thessismun.org

Topic Area A: Towards a new and comprehensive approach in addressing cyber warfare and increasing cyber security

TABLE OF CONTENTS

1. Welcoming Letter by the chairs of the First Committee

Dear Delegates,

We are pleased to welcome you all to the 1st Committee of the General Assembly (DISEC). At first, we would like to congratulate each and every one of you for taking part into this year's edition of the Thessaloniki International Students Model United Nations and promise that we will do anything within our powers to facilitate you throughout the conference so as to have a productive and unforgettable experience.

This year's sessions will focus on two rather pressing issues. The first topic, similar to the last year's agenda, calls for a new and comprehensive approach on cyber warfare and cyber security. The abrupt developments that took place in the summer of 2017 and the collapse of the world's main vehicle for negotiations on cyber security, call for a renewed and in depth dialogue concerning the issue, so as to surpass the existing problems and reach consensus between states.

The second topic deals with the issue of proliferation of drone technology as a military means and the various implications that may arise from its use. Being a topical matter, the weaponization of unmanned aerial vehicles, is expected to test your diplomatic "stamina" while, at the same time, requires you to be in line with the national policies set by the country every single one of you represents.

This study guide aims at helping you get a better insight into the Topic Areas of the Committee and offers you a starting point for your research. Nevertheless, it is highly advised to conduct a thorough examination on your country's position concerning the matter discussed and also elaborate on your key national policies within the context of the position paper you will be requested to deliver before the opening of the conference.

We trust in your academic and diplomatic skills and sincerely hope for a remarkable outcome.

We thank you in advance for your in-depth understanding and co-operation and look forward to meeting you in person!

The chair and co-chair of the First Committee of the General Assembly,

Ananias Kapourkatsidis

Sophia Telonaki

2. Introduction to the Committee

The Disarmament and International Security Committee (DISEC)[1] was established in 1993 and constitutes one of the main committees of the General Assembly. The role of DISEC is circumscribed in Article 11, Chapter IV of the United Nations Charter.

"The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and may make recommendations with regard to such principles to the Members or to the Security Council or to both". As per this article, the mandate of DISEC is highlighted as, "to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources".

The body's pivotal responsibilities are interconnected with issues of disarmament, global challenges and threats to peace, all of which greatly affect the international community. DISEC further seeks out solutions to the challenges in the international security regime. Any arising disarmament and international security matter falls within the ambit of the Charter relating to the powers and functions of the First Committee. DISEC implements the following principles when drafting its documents or in session:

- The general principles of cooperation in the maintenance of international peace and security.
- Principles governing disarmament and the regulation of armaments.
- And, last but not least, the promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament while is the only Main Committee of the General Assembly entitled to verbatim records coverage .

[1] The official page of the First Committee of the General Assembly: http://www.un.org/en/ga/first/

3. Introduction to the topic

During the summer of 2017 the main venue for discussion about cyber security on a global level, the Group of Governmental Experts, failed to agree on a report. It is not the first time that the GGE cannot reach consensus. This time though the divisions between the states' representatives were too deep. In their official statements, the representatives showed their unwillingness to continue to negotiate about cyber security in the framework of the United Nations' GGE. This probably means that the international community faces the end of an era for information security.

At the same time cyber threats are increasing both in numbers and in complexity. The year 2017 was predicted to be the year of cyber operations. The data that the experts have gathered prove this prediction. The most recent researches show that approximately four major cyber incidents occurred each moth of 2017. The international community and the United Nations have to focus all of their efforts in jumpstarting the negotiations and look towards a new and comprehensive approach on cyber security.

The First Committee of the General Assembly will play a leading role in this effort. In this year's sessions it is tasked to examine the conditions and the circumstances which led to the collapse of the negotiations in July 2017. Following this attempt, the committee must find ways to tackle the problems that emerge, discuss new vehicles of negotiations and, with the eye fixed on the continuous advance of cyber threats, guide them towards more sufficient approaches in increasing cyber security.

4. Key terms and definitions

Due to the technical nature of the topic, many of the terms used in these guide might be unknown or vague for the delegates who are not familiarized with the field of information technology. Moreover, several of these terms have baffled the international community as they are creating impediments in the progress of the debates. This chapter presents the most widely accepted definitions of the key terms in cyber technology. However, they are not binding, as the committee is tasked to review some of them and, if possible, agree on more specific and concrete definitions.

Cyber: The word cyber is an abbreviation of the 1980s word *cybernetics*[2] and "connotes a relationship with information technology[3]".

[2] Definition of "cyber" from the Oxford Dictionary, available at: https://en.oxforddictionaries.com/definition/cyber
[3] Definition from the Tallinn Manual on the International Law Applicable to Cyber Warfare

Cyberspace: "The environment formed by physical and non-physical components, characterized by the use of computers and the electromagnetic spectrum, to store, modify and exchange data using computer networks"[4].

Cyber attack: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[5].

Cyber infrastructure: "The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements:

- Processing includes the creation, access, modification, and destruction of information.
- Storage includes paper, magnetic, electronic, and all other media types.
- Communications include sharing and distribution of information".

Cyber operation: "The deployment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace"[6].

Hacker: "An unauthorized user who attempts to or gains access to an information system"[7].

5. Historical background

5.1. 1998: the beginning

The issue of cyber security was put to the United Nations agenda by a draft resolution submitted by the Russian Federation to the First Committee of the General Assembly[8]. The resolution was adopted later by the General Assembly without a vote in its fifty-third session in 1998[9]. Since then the Secretary General and the UN member states submit annual reports concerning their views, their progress and in

[4] Definition from the Tallinn Manual on the International Law Applicable to Cyber Warfare
[5] Definition from the Tallinn Manual on the International Law Applicable to Cyber Warfare
[6] Definition from the Tallinn Manual on the International Law Applicable to Cyber Warfare
[7] Definition from the Committee on National Security Systems (CNSS) Glossary
[8] 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
[9] 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

general developments on the field of information technology and telecommunications in the context of international security[10].

The main venue for discussion about cyber security is the Groups of Governmental Experts (GGEs). The process of establishing a GGE starts from a recommendation of the First Committee to the General Assembly, which later adopts a resolution calling for a GGE to commence its deliberations. The First Committee negotiates on the mandate, the size and the number of sessions that a GGE will have, all of which are included in the resolution of the GA. The first GGE took place in 2004/2005 and was follow by four more in 2009/2010, 2012/2013, 2014/2015 and 2016/2017. A consensus is mandatory in order for a report to be submitted to the General Assembly. Two of the GGEs, the first and the fifth have not accomplished to reach a consensus among the representatives of the member states[11].

5.2. 2004-2015: the progress of the first four meetings of the Group of Governmental Experts

As aforementioned the first meeting of the Group of Governmental Experts in 2004/2005 did not manage to agree on a report by consensus between its 15 participants. There were two questions that divided the members of the first GGE. At first, on how the developments of information technologies and telecommunications can be used for military purposes. The experts did not agree on how to characterize the threat coming from a state using these developing tools to attack another state. The second issue that divided the group was whether to focus the discussion on information infrastructure or extend the debate to information content[12]. The president submitted a procedural document to the Secretary General stating only those who attended the GGE and the dates of the sessions[13].

On the contrary, the second meeting of the GGE in 2009/2010 managed to reach consensus and submit a report to the GA which can be viewed as the fundament of the international negotiating agenda on information security. The report stressed the need of the international community to formulate new norms of state responsibility in

[10] UNODA, Developments in the field of information and telecommunications in the context of international security, retrieved from: https://www.un.org/disarmament/topics/informationsecurity/

[11] UNIDIR/CSIS, Report of the International Security Cyber Issues Workshop Series, retrieved from: http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

[12] United Nations Office for Disarmament Affairs, Fact Sheet, Developments in the field of information and Telecommunications in the context of International Security, retrieved from: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

[13] UNIDIR/CSIS, Report of the International Security Cyber Issues Workshop Series, retrieved from: http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

cyber affairs, to enhance the communication and cooperation among states and to ameliorate the capacity of under-developed states in the sector of information security. Finally, it proposed that the following discussions should also focus on working out common terms and definitions concerning the events taking place in cyber space[14].

The next two meetings of the GGE made significant progress, compared to the first two. The third meeting of the GGE in 2012/2013 managed to reach a landmark consensus. The representatives agreed on a report which included the provision that "International law, in particular the Charter of the United Nations, is applicable and essential" to maintain peace in cyberspace. The next meeting made reference to human rights, however due to the disagreements of states in the inclusion of the International Humanitarian Law, the report mentioned only the principles of humanity, necessity, proportionality and distortion.

5.3. The 2016/2017 Group of Governmental Experts: the failure to reach consensus

The fifth meeting of the United Nations' Group of Governmental Experts (GGE) in New York finished its works during the fourth and last session on 19-23 June 2017 without a consensus between the 25 member states. The 2016/2017 GGE was tasked by the General Assembly to study further the existing threats in cyber security, delve deeper into how the International Law applies to cyber space, negotiate norms concerning the responsible behavior of states, confidence-building measures and capacity-building and submit a report to its seventy-second session. The Group, finally, did not manage to submit a report to the GA due to disagreements between the representatives on the applicability of International Humanitarian Law in cyber operations, the right to self-defense and some specific countermeasures[15].

The proposal that Article 51 of the Charter of the UN applied in the cyber sphere arose various concerns. Cuba, voicing its fears, stated that such a scenario would lead to a militarization of cyberspace[16]. In the words of the Cuban representative, this development will "*convert cyberspace into a theater of military operations and […] legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims*

[14] United Nations Office for Disarmament Affairs, Fact Sheet, Developments in the field of information and Telecommunications in the context of International Security, retrieved from: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

[15] Ann Väljataga, Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly, September 1 ,2017, retrieved from: https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html

[16] Ibid

of illicit uses of ICTs"[17]. Similar views have been voiced in the past by the representatives of China and the Russian Federation, notably during the negotiations of the 2014/2015 GGE on the applicability of the IHL in cyber space[18].

Opposing to this stance, the representative of the United States expressed her regret and disappointment towards the reluctance of some experts to "*seriously engage on the mandate on international legal issues*"[19]. In her view this behavior is dragging the international community back, after years of progress and cooperation by the GGEs. According to the expert of the United States talking about how to settle cyber threats in a peaceful way without discussing the legal tools of responding to them is ineffective and indicative that some states prefer to impede the deliberations of the GGE to achieve their political goals through cyberspace[20]. The expert of the United Kingdom, siding with the USA on this issue, later underlined that international law applies in cyberspace and stated that the failure of the fifth GGE does not mean that the work accomplished in its previous meetings is undone[21].

Even though the statement of the British representative is true and one cannot ignore the work done by the previous years, it remains as a fact that since there has been no report submitted to the General Assembly by the fifth GGE, the issue of the applicability of international law in cyber space, among other more specific topics, remains unsolved and the international community is at an impasse. Therefore, the GA has not called for the next meeting of the GGE, resulting to the inexistence of the main international body with a clear mandate to study matters of cyber security and propose concrete solutions and responses to the various threats emerging almost every day.

[17] Cuba's Statement, 71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, June 23,2017,available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information

[18] Stefan Soesanto and Fosca D'Incau, The UN GGE is dead: Time to fall forward, August 15, 2017, retrieved from: http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance#_ftn2

[19] U.S Department of State, Michele G. Markoff, Deputy Coordinator for Cyber Issues, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE),New York City, June 23,2017 retrieved from: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

[20] Ibid

[21] Owen Bowcott, Dispute along cold war lines led to collapse of UN cyber warfare talks, August 23, 2017, retrieved from: https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges

5.4. Cyber incidents of 2017[22]

The incidents presented in this chapter are not selected as the most significant among others for each of the twelve months of 2017. They were picked with the purpose to show the variety of methods, tools, attackers, states, non-state actors, firms and organizations involved in cyber warfare only in one year. This list aims to prove the extent of the problem and the need to revive the international efforts to tackle with these threats.

- January 2017

A Swedish foreign policy institute accused Russia of conducting an information warfare campaign, using fake news, false documents, and disinformation intended to weaken public support for Swedish policies.

- February 2017

Hackers compromised the Singaporean military's web access system and stole the personal information of 850 people. The Ministry of Defense said it was likely the attack was state sponsored.

- March 2017

Wikileaks released a trove of sophisticated CIA hacking tools dated from 2013 to 2016, claiming that the release reflected several hundred million lines of CIA-developed code.

- April 2017

Chinese attempts to penetrate South Korean military, government and defense industry networks continued at an increasing rate since a February announcement that the THAAD missile defense system would be deployed in South Korea.

- May 2017

Thousands of emails and other documents from the campaign of French president-elect Emmanuel Macron, totaling 9 gigabytes, were released shortly before the election, in an effort linked to Russia.

- June 2017

A NotPetya ransomware attack shut down the port terminals of Danish shipping giant Maersk for two days, causing an estimated $300 million in associated costs

- July 2017[23]

The Qatari government accused hackers in the United Arab Emirates of posting fake news and attacking Qatari state-run media websites in a campaign designed to widen a rift between Gulf States.

[22] Center for Strategic and International Studies (CSIS), Significant Cyber Incidents Since 2006, retrieved from: https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity

[23] Most of the cyber incidents that took place in 2017 happened in July

- August 2017

South Korea's Cyber Warfare Research Center reports that North Korea has been targeting South Korean Bitcoin exchanges.

- September 2017

Researchers report malware infections in Cambodia designed to surveil dissidents and disrupt domestic political activity.

- October 2017

North Korean hackers were found to have targeted US electric companies in a spear-phishing campaign meant to probe utilities' defenses.

- November 2017

Uber discloses that it paid hackers $100,000 to delete the stolen data of 57 million of its customers and drivers, including names, phone numbers, email addresses, and license plate numbers.

6. The reasons behind the collapse of the United Nations' Group of Governmental Experts

The failure of the UN's GGE to reach consensus in 2017, though a major step back, was not an unlikely development, mainly due to its challenging topic of discussion. The applicability of International Law in cyberspace has been the bone of contention between states during the last three meetings of the Group. The reference of the 2013 report that "[i]nternational law, and in particular the Charter of the United Nations" is applicable to the ICT environment was considered a milestone consensus in the progress made by the GGE meetings. However, the opinions of the representatives in the GGE, concerning the adequacy of the existing legal framework, differ. On the one hand, there are those who firmly believe that the international law applies in cyberspace as it is and focus their work on its implementation, while others maintain the position that the GGE has to negotiate new legal norms.

The collapse of the 2016/2017 GGE can be explained by the representatives' disagreement on three particular issues. The first is the right to self-defense in case of a cyber attack. The second is the issue of countermeasures, meaning the states' response if they face a cyber threat. The third and final issue is the inclusion of International Humanitarian Law in the 2017 report.

The reference to the right to self-defense derives from the proposal of certain states to include the Article 51 of the Charter of the United Nations[24]. The article mentions that in the scenario of an armed attack a state has the inherent right to defend itself. However, in cyberspace it is very complicated and still difficult to agree on a threshold of what can be considered a cyber attack. During the previous meetings of the GGE there was no direct reference to the right to self-defense. Instead the wording of the 2015 report stating the "*inherent right of States to take measures consistent with international law and recognised in the Charter*" [25] refers to Article 51. The representative of Cuba publicly expressed its objections against the specific reference to the Article 51 by mentioning that there was an attempt to *"establish equivalence between the malicious use of ICTs and the concept of armed attack*"[26].

A similar problem is posed on the issue of countermeasures. In the cyber context a countermeasure is a cyber operation in response to a previous cyber operation. In that case scenario, the most important matter is the ability to attribute the unlawful incident to another state or state sponsored actor. The more technologically advanced countries have the upper hand on this issue, while those who are still struggling in the cyber ecosystem will risk committing an internationally wrongful act[27].

The International Humanitarian Law on the other hand has been a point of division between the representatives in the previous GGE as well. In the 2015 report the representatives avoided a direct reference to IHL and noted the applicability of the principles of "humanity, necessity, proportionality and distinction"[28]. In the previous meeting of the Group, China opposed the direct statement that the IHL applies to

[24] UN CHAPTER VII: action with respect to threats to the peace, breaches of the peace, and acts of aggression, retrieved from:
http://www.un.org/en/sections/un-charter/chapter-vii/index.html
[25] 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 from
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[26] Cuba's Statement, 71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, June 23,2017,available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information
[27] https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges and
Michael Schmitt and Liis Vihul, International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, June 30, 2017, retrieved from:
https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/
[28] 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 from
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

cyber operations[29]. In the fifth meeting it was Cuba that expressed that the inclusion of the IHL will aid in the militarization of cyberspace[30].

7. Two different perspectives: is the existing legal framework adequate for cyberspace or there is a need to negotiate new norms?

The aforementioned disagreements created an impasse in the main international venue of discussion about cyber security. There are those who believe that the Group of Governmental Experts belongs in the past and that 2017 was the end of an era in the discussions about information security[31]. Even if that statement is true and the need to take the next step towards a new comprehensive approach in addressing cyber warfare and increasing cyber security is more urgent than ever, the international community has to search for the impediments that have prevented it from tackling the issue sufficiently.

For this purpose there is a need to search deeper the issues that have divided the representatives in the GGEs. The first step to achieve this is to admit that there are two different perspectives between the states that participated in the GGE. On the one hand, USA and other states consider the existing legal framework adequate and applicable to cyberspace. According to these states the existing international law and the rules governing the use of force apply to cyberspace and the focus of any deliberation should be on the ways to implement them[32].

On the other hand, states like China and Russia have expressed their doubts for the adequacy of International Law in cyber space in various occasions and have attempted to present new legal norms and frameworks to general discussion. A

[29] Elaine Korzak, International Law and the UN GGE Report on Information Security, December 2, 2015, retrieved from: https://www.justsecurity.org/28062/international-law-gge-report-information-security/

[30] Cuba's Statement, 71 UNGA: Cuba at the final session of Group of Governmental Experts on develop-ments in the field of information and telecommunications in the context of international security, June 23,2017,available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information

[31] Stefan Soesanto and Fosca D'Incau, The UN GGE is dead: Time to fall forward, August 15, 2017, re-trieved from: http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance#_ftn2

[32] U.S Department of State, Michele G. Markoff, Deputy Coordinator for Cyber Issues, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE),New York City, June 23,2017 retrieved from: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

paradigmatic example of this is the *International Code of Conduct for International Security* which was presented in the sixty ninth session of the United Nations' General Assembly. The Code was sponsored by China, the Russian Federation, Tajikistan and Uzbekistan[33] and co-sponsored by Kazakhstan and Kyrgyzstan[34]. The document was a revised draft of the initial Code submitted to the General Assembly in 2011, in response to the comments it received.

Paragraph 8 of the Code mentions clearly the need to establish "multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet". The view of these states can be summed up by their disagreement with the "multistakeholder" model of governance in cyberspace and propose a new model of cyber governance controlled mainly by the states. However, in the next paragraph there has been a change in the wording compared with the initial 2011 draft. Instead of the declaration that all states should "lead all elements of society, including its information and communication private sectors, to understand their roles and responsibilities with regard to information security"[35] the revised code mentions that states should "cooperate fully with the other interested parties in encouraging a deeper understanding by all elements in society […] of their responsibility to ensure information security".

Despite the fact that both drafts of the Code were rejected, there are still states that echo the idea of a new international treaty on cyber security[36]. Nevertheless, in order to sufficiently address the issue of information security the international community has to bridge the gap between its viewpoints on the applicability of the existing legal framework in cyberspace. Paragraph 10 of the Code mentions that states need "to develop confidence-building measures aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict". This provision could be the basis where a new discussion on cyber security can start, focusing on bridging the disagreements between the states[37].

[33] These states are member of the Shanghai Cooperation Organization
[34] 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
[35] 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
[36] Cuba's Statement, 71 UNGA: Cuba at the final session of Group of Governmental Experts on develop-ments in the field of information and telecommunications in the context of international security, June 23,2017,available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information
[37] Eichensehr, Kristen, (2015), International Cyber Governance: Engagement without agreement?, retrieved from https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/

8. Unanswered questions regarding cyber security and the urgency to deal with them

As the history has showed, cyber conflict might become a reality as the use of cyber tools either by states or non-state actors is increasing. The need to defend from cyber threats calls for the development of cyber capabilities, the exchange of knowledge and information. How can the international community ensure that these capabilities will not be used for future cyber conflict? This question is troubling the minds of many diplomats, policy makers and legal scholars. To answer this general question the international community has to divide it in more specific topics that need to be answered, before it continues to debate on cyber security[38].

8.1. Under what circumstances can cyber tools be used and to what consequences?

As aforementioned states possess cyber capabilities which can be of some use either offensively or in a defensive manner. States must agree that these tools will not and must not be used offensively against another states in any case. The only circumstances under which states should be allowed to use their cyber capabilities should be to defend themselves from a cyber threat. Nevertheless, the conditions that will define the cyber threat, the ways to react to it and the extent of the reactions are subjects which have to be further discussed.

These topics present different problems, to which the international community has to find solutions. First, due to the duel-use and civilian owned infrastructure of cyberspace, the committee should make proposals and present measures which will facilitate the identification of the originator of a cyber threat. However, the problem cannot be deemed solved. Today, the identification of a cyber threat takes months or even year to be accomplished. Thus, the questions of what the reactions of the international community, in a state-level, could be against a cyber threat that took place the year before and how these reactions could be regulated, in order to operate within the framework of responsible state behavior are to be resolved.

8.2. Who will be responsible in case of damage and how will the adversary react?

This specific topic delves deeper into the issue of the use of the cyber capabilities. The question of who is responsible for a cyber operation is eminent in the international debate and has created many impediments in the course of the negotiations. The difficulty to attribute a cyber operation and to elaborate on the

[38] The questions included in this topic are retrieved from Götz Neuneck, Transparency and confidence building measures: applicability to the cyber sphere? found in UNIDIR The Cyber Index, 2013

countermeasures that need to be taken has been the reason why states did not achieve a consensus in the fifth meeting of the GGE. This reality is one of the main challenges, especially for states that do not possess the technology needed to identify the originator of a specific threat.

Furthermore, even if the origins of a cyber threat are found and it is attributed to a person or a group or an institution, it is extremely improbable to prove that it was state-sponsored. False indications could lead to conflict between states. Thus, to achieve this, experts must insist on capacity and confidence building mechanisms, with the purpose to aid those states still struggling to evolve technologically in the cyber context.

8.3. What do self-defense, offense and defense mean in the cyber context?

These issues have been troubling the international community for years. The last two GGEs have stumbled upon the right to self-defense and, in the end, collapsed due to the disagreements upon its inclusion in their reports. Certainly, the different viewpoints of states concerning the applicability of International Law in cyberspace are relevant. However, the vagueness of these terms in the cyber context can also be found in the states' inability to reach consensus about their application in the cyber sphere. Moreover, in the classical war terminology, the notions "offense" and "defense" cause little disagreement. In the cyber sphere, though, there is still progress to be made, due to the complexity, the wide ownership of cyber infrastructure and their still uncontrollable use.

8.4. What is the definition of a cyber attack and under what conditions can it be labelled as an armed attack?

Article 51 of the Charter of the United Nations mentions: "*Nothing [...] shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations*." The inclusion of these provisions in the final report of the fifth GGE meeting led to its final collapse. As aforementioned, terms such as self defense, cyber attack and cyber war must be agreed upon by the international community. The thresholds must be set to define when a cyber threat is a mere sabotage and when it constitutes a cyber attack which can be considered an armed attack.

The definition of the term "cyber attack" given by the Tallinn Manual and mentioned in the fourth chapter of this guide is: "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". According to this definition, most of the cyber incidents cannot be labeled cyber attacks. Another question arises, namely if the traditional definition of the terms attack and warfare be adequate in the cyber context and

consequently if there should be a new meaning of these terms, in order for them to be better applicable to cyberspace.

8.5. How to prevent future wars from being accompanied by cyber attacks?

Without any doubt, future wars could be accompanied by cyber operations, which will be complementary to conventional means of warfare. Militaries now possess cyber tools and in the case of conflict it remains unknown if they will be used either offensively or in a defensive manner, along with the classical tools. Cyberspace is now deemed the fifth battleground, added to the sea, the earth, the air and space.

To answer this query the international community has first to answer all the previous topics and align towards a common goal. The gap between the different perspectives in the GGE has to be bridged and the experts must focus both on solving their disagreements and agreeing on a common basis. This is how the issue of cyber security can be addressed comprehensively and sufficiently in order to prevent future wars to end up or start as cyberwars.

9. Legal framework

Since the Russian Federation brought the issue of cyber security to the United Nations' agenda in 1998 there have been a number of legal initiatives that have been forming the international and regional legal framework concerning the cyber sphere. The United Nations have played a leading role in the negotiations and have been the main vehicle for discussions, via the Group of Governmental Experts.

The most important legal steps of the United Nations are the following:

- Resolution 53/70 was the first adopted by the General Assembly without a vote in 1998 after the draft resolution introduced in the First Committee by the Russian Federation[39].
- In 2003 the GA adopted resolution A/57/239 called for the states' awareness and readiness to react against cyber security incidents[40].

[39] 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

[40] 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

- In 2004 the GA adopted resolution A/58/199 invites states and other organizations to share their knowledge and information in the context of cyber security[41].
- In 2004/2005 the first Group of Governmental Experts met without achieving a consensus.
- In 2009/2010 the second Group of Governmental Experts met and agreed on a report[42].
- In September 2011 the Permanent Representatives to the United Nations of China, the Russian Federation, Tajikistan and Uzbekistan submitted a letter to the Secretary General which contained the first draft *International Code of Conduct for Information Security*[43].
- In 2012/2013 the third Group of Governmental Experts met and agreed on a report[44].
- In January 2015 the Permanent Representatives to the United Nations of China, the Russian Federation, Tajikistan and Uzbekistan submitted a letter to the Secretary General which contained a revised draft International Code of Conduct for Information Security[45].
- In 2015/2016 the fourth Group of Governmental Experts met and agreed on a report[46].

Other organizations have also taken legal steps addressing the issue of cyber security:

- In May 2007 the International Telecommunication Union Chairman published a report launching the Global Cybersecurity Agenda "as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society"[47].

[41] 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

[42] 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

[43] 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

[44] 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

[45] 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

[46] 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 from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[47] ITU, Global Cybersecurity Agenda, retrieved from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

- The Deauville Declaration was agreed by the Group of Eight, an international forum of the Governments of Canada, France, Germany, Italy, Japan, the Russian Federation and the United States[48]. The Group of Eight aims at creating a information sharing mechanism among technologically advanced states to facilitate the tackling of cybercrime.
- The Council of Europe organized the 2004 Budapest Convention on Cybercrime, which is the only international binding treaty on cybercrime. The Convention on Cybercrime contains guidelines for states to evolve their legislation on cybercrime. Moreover, it serves as a framework promoting international cooperation to tackle the issue[49].

Regional organizations have played a very significant role in addressing the issue of cyber security by bringing together states and aiding in information sharing, capacity and confidence building. Their advantage is that their discussions involve fewer states but with related interests which can cooperate easier on a regional level[50].

10. How to jumpstart international dialogue on cyber security?

The collapse of the Group of Governmental Experts as well as the appearance of new and complex cyber threats underlines the need to jumpstart international dialogue concerning cyber security. Capacity and confidence building are crucial to this purpose, due to the fact that they have been the main reasons of the 2017 failure. Both in the cases of capacity and confidence, most states lack both, resulting in either refusing to accept the existing measures or negotiating new norms.

Certainly, the progress made by states to enhance their cyber security mechanisms is undoubtful. However, the number of incidents only in 2017 proves that there is still a lot of work ahead of the international community in evolving their security mechanisms and preventing new attacks. This development leads to the conclusion

[48] Group of Eight, Deauville G8 Declaration, retrieved from http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf

[49] Cybercrime is not part of the mandate of the First Committee of the General Assembly. Thus, delegates should refrain from proposing measures relevant to it or discussing ways to tackle cybercrime. The inclusion of this paragraph aimed at showing up the developments and steps taken by the CoE in the general context of information technology.

[50] For an extensive analysis of the role of Regional Organizations in addressing cyber security see UNIDIR, The Cyber Index, International Security Trends and Realities, Götz Neuneck, Chapter 2, Regional Organizations, page 101 at http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

that the reactive approach against cyber operations needs to be revised and, if needed, changed. Indeed, the efforts of states to build their capacity to react to the new cyber threats have helped so far and not very efficiently. This is why a more dynamic and proactive approach that focuses more on defense rather than security is necessary.

Defense is a more dynamic concept, one that included both the detection of and reaction to a cyber threat in real time and a preemptive conduct. States need to cooperate on building their cyber defenses by observing each other's incidents and learning from them. Moreover, a multilayered cyber defense is built by observing the tactics of the adversary, gather information and predict the possibility of a first failure. This multilayered and well tested approach should be the focus of new negotiations and capacity building measures.

It will not be possible though to have that kind of capacity building unless states build on their confidence and cooperation. There are many indications that confidence between states is in the lowest level since the beginning of the GGE meetings. The difference in states' perspective and the inability to reach an agreement on core issues such as the applicability of international law prove that confidence should be one of the first priorities in jumpstarting new international dialogue on the issue.

11. Conclusion

The developments in the field of information technology are rapid and easy to get away from our control. The past summer made this more evident than ever. States did not agree, due to either political differences or their inability to adapt in cyberspace. The beginning of a new dialogue is necessary. This beginning should be characterized by the effort of all states to bridge the gap between them, align towards a common goal: international cyber defense and global cyber security. The background and the issues presented in the previous chapters should be considered a guide towards discussing and, hopefully, solving many of the problems created in the summer of 2017. This committee and all its participants must work together to create the foundations upon which this effort should commence.

12. Points to be addressed

- Is there a need to adopt more precise and detailed definitions of key terms regarding the issue?
- Could international law be applicable to cyber space?
- Could the existing legal framework be adequate in the cyber sphere?
- Should the international community focus on developing new legal norms more applicable to cyberspace?
- Under what conditions cyber tools could be used for military purposes?
- Could the international community find ways to effectively attribute cyber damages to the responsible actor without the fear of a destructive error?
- Should the notions of offense and defense be renegotiated in the cyber context?
- Could there be a globally accepted definition of a cyber attack?
- What could be the threshold of an armed attack in the cyber context?
- How can states prevent future wars as well as cyber wars?
- By what measures can states build capacity in addressing the threats in cyber security?
- Should there be a more dynamic approach to cyber security?
- What could be the basis on which states can construct confidence building mechanisms?
- Could the focus on confidence building aid to restart international dialogue on cyber security?

13. Bibliography

13.1.UN documents

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

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

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

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, re-trieved from http://undocs.org/A/53/576

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

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

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 from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

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

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

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

13.2. Other sources

Center for Strategic and International Studies (CSIS), Significant Cyber Incidents Since 2006, re-trieved from: https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity

CoE, Convention on Cybercrime, retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

ITU, Global Cybersecurity Agenda, retrieved from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Group of Eight, Deauville G8 Declaration, retrieved from http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf

UNIDIR/CSIS, Report of the International Security Cyber Issues Workshop Series, retrieved from: http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

UNODA, Fact Sheet, Developments in the field of information and Telecommunications in the context of International Security, retrieved from: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdfUNIDIR, The Cyber Index, International Security Trends and Realities, at http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

UNODA, Developments in the field of information and telecommunications in the context of interna-tional security, retrieved from: https://www.un.org/disarmament/topics/informationsecurity/

13.3. Articles

Ann Väljataga, Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly, September 1 ,2017, retrieved from: https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html

Dan Solomon, The end of reactive security and the move towards a doctrine of cyber defense?, 2014, retrieved from http://www.cybersecurity-review.com/industry-perspective/the-end-of-reactive-security-and-the-move-to-a-doctrine-of-cyber-defence/

Elaine Korzak, International Law and the UN GGE Report on Information Security, December 2, 2015, retrieved from: https://www.justsecurity.org/28062/international-law-gge-report-information-security/

Kristen Eichensehr, International Cyber Governance: Engagement without agreement? 2017 retrieved from https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/

Michael Schmitt and Liis Vihul, International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, June 30, 2017, retrieved from: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms

Owen Bowcott, Dispute along cold war lines led to collapse of UN cyber warfare talks, August 23, 2017, retrieved from: https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges/

Ryan Olson, Cybersecurity will not evolve if we are only cleaning up after a breach, 2015, retrieved from http://www.cybersecurity-review.com/cybersecurity-wont-evolve-if-were-only-cleaning-up-after-a-breach/

Stefan Soesanto and Fosca D'Incau, The UN GGE is dead: Time to fall forward, August 15, 2017, retrieved from: http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance#_ftn2

13.4. Statements from representatives

Cuba's Statement, 71 UNGA: Cuba at the final session of Group of Governmental Experts on devel-opments in the field of information and telecommunications in the context of international security, June 23,2017,available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information

U.S Department of State, Michele G. Markoff, Deputy Coordinator for Cyber Issues, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE),New York City, June 23,2017 retrieved from: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm