NMUN•NY 2021

5 – 8 April 2021

Documentation of the Work of the General Assembly First Committee (GA1) NMUN Simulation*

TOGETHER
TOWARDS
TOMORROW

Conference B

* National Model United Nations (nmun.org) organizes simulations of the UN. The resolutions in this document were the work of dedicated college and university students attending our conference. They are not official UN documents and their contents are not the actual work of the UN entity simulated.

General Assembly First Committee (GA1)

Committee Staff

Director	Angelo J. Bechara
Assistant Director	Ashlee A. Rolheiser
Chair	Achal Kulkarni

Agenda

I. Advancing Responsible State Behavior in Cyberspace in the Context of International Security
II. The Illicit Trade in Small Arms and Light Weapons in all its Aspects
III. Establishment of a Nuclear Weapon Free Zone in the Region of the Middle East

Resolutions adopted by the Committee

Code	Topic	Vote
GA1/1/1	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	Adopted without a vote
GA1/1/2	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	Adopted without a vote
GA1/1/3	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	34 votes in favor, 16 votes against, 0 abstentions
GA1/1/4	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	35 votes in favor, 15 votes against, 0 abstentions
GA1/1/5	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	Adopted without a vote
GA1/1/6	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	Adopted without a vote
GA1/1/7	Advancing Responsible State Behavior in Cyberspace in the Context of International Security	30 votes in favor, 15 votes against, 5 abstentions

Summary Report for the General Assembly First Committee

The General Assembly First Committee held its annual session to consider the following agenda items:

I. Establishment of a Nuclear Weapon Free Zone in the Region of the Middle East
II. Advancing Responsible State Behavior in Cyberspace in the Context of International Security
III. The Illicit Trade in Small Arms and Light Weapons in all Its Aspects

The session was held virtually and attended by representatives of 53 Member States and 0 Observers. On Monday, the committee adopted the agenda of II, III, I, beginning discussion on the topic of "Advancing Responsible State Behavior in Cyberspace in the Context of International Security."

By Tuesday, the Dais received a total of 9 proposals covering a wide range of sub-topics, including educational campaigns about the implications of cybercrime, information security training, strengthening cybersecurity infrastructure, and further encouragement of partnerships between NGOs and international organizations. The atmosphere in committee was one of collaboration and by the end of the session on Wednesday evening, multiple working papers were brought forward with complementary themes.

On Thursday, seven draft resolutions had been approved by the Dais, one of which had a friendly amendment. The committee adopted seven resolutions following voting procedure, four of which received unanimous support by the body. The resolutions represented a wide range of issues, including the regulations and transparency of cryptocurrency and cybersecurity, adopting cyber norms for state behavior, and enhancing cooperation between the UN and other international organizations such as SPECPOL, NATO, and INTERPOL. Efficiency, honesty, and transparency were central to this committee's proposals, and their commitment was primarily to advancing responsible state behavior in cyberspace in the context of international security.

Code: GA1/1/1
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Recalling General Assembly resolutions 73/27 (2018) and 71/28 (2016) on developments in the field of information and telecommunications in the context of international security, resolution 58/199 (2003) on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and the Council of Europe's *Treaty on Cybercrime* (2004) to foster international cooperation against cybercrime,

Affirming the capacity of the Group of Governmental Experts (GGE) to inform Member States of the advancements in responsible state behavior in cyberspace,

Considering that state and non-state actors are increasingly using cyberspace as a platform for malicious acts,

Recognizing the capacity of the United Nations Office of Counter-Terrorism (UNOCT), the International Telecommunication Union (ITU), and non-government organizations (NGOs) to recommend actions and provide expertise in relation to cyber security,

Recognizing the role that Information and Communication Technologies (ICTs) play in achieving the Sustainable Development Goals (SDGs), namely SDGs 4 and 17, to create a more sustainable future to better support cybersecurity,

Observing the rapid increase in access to the internet among developing countries over the past decade and the vulnerability of emerging internet populations to cybercrime,

Commending the work that the United Nations Office on Drugs and Crime (UNODC) Global Programme on Cybercrime has done to increase cybercrime awareness among vulnerable populations,

Concerned that most Member States do not hold sufficient resources to establish functioning cyber security for their citizens independently,

Underlining the necessity for collaborative efforts and sharing of functioning practices to ensure safer usage of the cyberspace,

1. *Calling* for a renewal of the GGE as established by General Assembly resolution 73/266 (2018) upon conclusion of their 2021 report with:

    a. An expanded membership roster, which includes 50 Member States consisting of at least ten Member States from the 5 regions of operation of the United Nations (UN), and

    b. Consultation of the Economic and Social Council for Western Asia (ESCWA);

2. *Encouraging* the GGE to utilize information from the ITU, UNOTC, and the United Nations Office of Information and Communication technology (OITC);

3. *Suggests* that developing Member States create and extend their national cybersecurity capacities through cooperation with:

    a. Neutral UN bodies, like the UNOCT, to respect their sovereignty, and;

    b. NGOs in the field of cybersecurity;

4. *Proposing* to enhance the ITU Global Cybersecurity Index (GCI) by:

    a. Encouraging Member States to regularly answer the relevant GCI questionnaires with more precise information, and;

    b. Extending the Weightage Expert Group and increasing its diversity and representability, with a focus on members of academia to serve as unbiased observers;

5. *Requests* that the UNODC Global Programme on Cybercrime increases engagement with Member States to:

    a. Develop targeted educational campaigns to increase education among emerging internet populations about the potential dangers of cybercrime;

    b. Cooperate with regional organizations to address local needs by utilizing regional expertise to develop targeted curriculum, and;

    c. Strengthen cooperation with law enforcement such as The International Criminal Police Organization (INTERPOL) to further understanding and cooperation on cybercrime, particularly among developing Member States;

6. *Encouraging* youth participation in cyber security through bilateral and multilateral education and jobs training programs and campaigns within regional infrastructures that will:

    a. Empower citizens with knowledge to practice safe and informed behaviors within cyberspace;

    b. Train young professionals on cyber security methods to improve incident response time and ways to mitigate cyber threats;

    c. Promote the creation of internships and scholarships to further promote youth involvement on cyber security through promoting investment from NGOs, national and regional banks and the private sector;

    d. Incorporate SDGs 4 and 17 into education and training programs to foster sustainable development, and;

    e. Work to increase cyber job and career opportunities through the creation of youth cyber security teams in national and regional state departments;

7. *Highly encourages* Member States to develop their use of artificial intelligence (AI) in cooperation with civil society, acknowledging the direct benefits for sustainable development and cybersecurity by:

    a. Promoting security AI data security in collaboration of the United Nations Interregional Crime of Justice and Research (UNICRI);

    b. Encouraging the implementation of AI technology for educations following the guidance of the United Nations Educational, Scientific and Cultural Organization (UNESCO): Guidance for Policy Makers, and;

    c. Supporting scientific research in AI related matters for the accomplishment of SDGs 9, 11, and 17 by seeking a positive impact from technology in the modern society.

Code: GA1/1/2
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Acknowledging the need for universal access to cyber safety materials in the growing world of technology and their impact on education and digital diplomacy,

Deeply disturbed by a report from The World Economic Forum, which found that developments in the world, such as the COVID-19 pandemic, led to a 50.1% increase in cyber-attacks due to more people utilizing virtual platforms,

Expressing with concern that according to the World Bank, less than 1 in 5 people in underdeveloped Member States have access to the internet and are considered at a high risk for cyber-attacks,

Recognizing the role of Information and Communications Technologies (ICTs) towards achieving Sustainable Development Goals (SDGs), namely *SDG 9*, to help build resilient infrastructure, and *SDG 17.9* about international cooperation in the developing Member States to national plans,

Understanding the immense effects that technological advances have on the world and that these developments in cyber technology are leaving citizens, especially youth and other vulnerable populations, exposed to cyber-attacks, as made evident by efforts such as the United Nations (UN) International Youth Day,

Stressing the disruptive development of ICTs and their potential threat to current definitions of state sovereignty, international security, stability, and peace that ICTs pose such as those mentioned in the Report of the *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2021),

Concerned by the lack of consensus on what constitutes responsible state behavior in cyberspace,

Underlining the beneficial effects of effective international cooperation, sharing best practices and other information on cybersecurity, building up trust and security among Member States on national security in light of General Assembly resolution 73/266 (2018) promoting the formulation of international norms for responsible state behavior in cyberspace,

Expressing its appreciation of regional efforts such as the Trans-Eurasian Information Super Highway project that aims at improving internet connectivity in emerging economies,

Fully alarmed with the rise of cyber criminals who are utilizing COVID-19 to exploit sensitive information and undermine digital privacy, and the lethal consequences that misinformation has on various states during COVID-19,

Recognizing with satisfaction General Assembly resolution 64/211 (2010), which highlights the importance of incident management and recovery in capacity-building for cybersecurity,

Recalling The Council of Europe's *Treaty No. 185 Convention on Cybercrime*, requiring signatories to criminally prosecute those actors who commit cybercrimes,

Alarmed by the digital divide in Africa where more than 75.6% lack access to internet services and how the agriculture industry has been thoroughly disrupted in the African continent and globally due to the spread of COVID-19,

1. *Invites* Member States to work collaboratively to empower Least Developed Countries (LDCs) through the adaptation of Artificial Intelligence (AI) technology by creating a monitoring network under the name of CyberSafe, that:

    a. Focuses on medical data communication, financial technology use, and social media sharing, and;

   b. Generates security risk management technologies that ensure the rights of affordable consumer privacy;

2. *Strongly encourages* the expansion of the General Assembly resolution 74/28 (2019), designed to help facilitate the development of safe cyberspace networks and internet access in LDCs;

3. *Emphasizes* the importance of encouraging youth involvement in both the participation of cyber awareness trainings and drills in order to foster sustainable economic growth and close the digital divide;

4. *Further encourages* the continuation of regional and international partnerships and projects between Member States, non-government organizations (NGOs), and other international groups such as *Treaty No. 185 Convention on Cybercrime* and the Trans-Eurasian Information Super Highway project;

5. *Draws attention* to the creation of a biennial summit, where Member States could share their latest advancements in the field of cyberspace through initiating exchange programs that coordinate between the respective government's information technology departments to build long-standing practices to create a more resilient global cyberspace and infrastructure, promote mutual trust and common development, and address the means to combat the recent "infodemic" phenomena in collaboration with the UN Campaign Verified;

6. *Suggests* the creation of a voluntary code-of-conduct at the biennial summit which establishes cohesive norms of responsible State behavior in cyberspace which would:

   a. Define cybersecurity and cyberspace;

   b. Prohibit Member States' use of ICTs to undermine the security, stability, or sovereignty of other Member States;

   c. Respect the human rights as declared in the Universal Declaration of Human Rights (UDHR) (1948), territorial sovereignty, and the differences in political and social system between Member States while operating in the digital sphere;

   d. Ensure that Member States with emerging economies are able to develop their ICTs without interference, and;

   e. Encourage the sharing of best practices and other information between Member States;

7. *Recommends* the use of the International Telecommunications Union (ITU) as the official specialized agency in responding to cyber-attacks by regularly conducting cyber drills to improve and maintain Member States' capacities against cyber insecurity;

8. *Calls for* the development of information security awareness training in cyberspace that focuses on, but not limited to, malicious software used to steal information such as financial information, user credentials, and biometric data; password security that enhances authentication systems; and physical security and environmental controls to mitigate potential security risks such as tailgating, malfunction of physical security controls, and impersonation;

9. *Strongly advises* considering the recent Consensus Report on ICTs in the Context of International Security elaborated by the UN Open Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), especially looking at the additions regarding medical and critical infrastructures;

10. *Taking into consideration* the provision of a voluntary fund, facilitated by General Assembly Second Committee, for maintenance and improvement of information security, protection against hybrid threats at the national level, protection of critical infrastructures in companies and institutions, through information on ways to prevent, detect, protect, and mitigate the consequences of cyber-attacks;

11. *Encourages* Member States to develop cyber-resilient frameworks that analyze and survey the market for agriculture related digital tools and services and can facilitate an enabling environment to encourage uptake and digital literacy to incorporate analytic capabilities for precision agriculture;

12. *Further invites* the OEWG mandated with the exploration of applying existing international law to cyberspace to further guide the creation of a voluntary code of conduct for state behavior in cyberspace in alliance with Member States' request in their Final Substantive Report of 2021;

13. *Calls upon* the United Nations Security Council to establish an annual forum for all Member States to participate in discussions regarding the establishment of international norms and practices in cyberspace, as well as discussing the benefits of sharing information on cybersecurity and tactics to combat cyberattacks by state and non-state actors.

Code: GA1/1/3
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Emphasizing the need for inclusivity in any global and regional framework in regards to cybersecurity through a widespread and consistent medium, in line with the International Telecommunication Network's (ITU) *Global Cybersecurity Agenda* (GCA),

Reaffirming Security Council resolution 2341 (2017), which encourages the Member States to strengthen national, regional, international partnerships with stakeholders, public and private as appreciate to share information, knowledge, and experience in order to prevent, protect, investigate, respond and recover damage from terrorist attacks on critical infrastructure attacks in cyberspace,

Concedes the General Assembly resolution 65/230 (2010), which mandates Member States examine options to strengthen existing and to propose new national and international legal or other responses to cybercrime,

Cognizant of the need to expand the participation of developing countries in international institutions of governance as a means of ensuring the universal attainment of the Sustainable Development Goals (SDGs), and in line with the objectives outlined in SDG 16, specifically indicator 8,

Recalling the 6th review of the United Nations (UN) Global Counter-Terrorism Strategy (2018) and being concerned with the lack of a proper definition of cyber security that must be adopted by the body,

Recalling the efforts of the International Telecommunication Union (ITU) in increasing the confidence and trust of Member States in the use of Information and Communications Technologies (ICTs), as well as national capacities,

Underlining the objectives of the SDGs 17.6 and 17.7, of the *2030 Agenda*, about the international cooperation and the exchange of the technological knowledge,

Alarmed that according to a 2018 study done by McAfee, a global organization dedicated to overcoming cybercrime, found that the act of cybercrime costs global companies USD$600 billion yearly,

Understanding that not all Member States have the technological capacity to develop their own networks and cybersecurity,

Noting the importance of the pre-existing agreements such as the General Assembly resolution 74/28 (2019) and the importance of working to alter and update them in order to reflect modern technology, allowing for future development and expansion of stronger cybersecurity technology,

Calling attention to the work of the European Network and Information Security Agency through the establishment of the European (EU) Network and Information Security (NIS) Directive which works to fortify the national cybersecurity capabilities of Member States,

Bearing in mind the potential cyber threats exacerbated by the COVID-19 pandemic and the new age boom in technology, in relation to commitments outlined in article 1.1 of the *Charter of the United Nations*,

Acknowledging the benefits that data gathered on major cybersecurity interactions can provide for Member States developing future guidelines for proper behavior in cyberspace,

Stressing the importance of inclusivity in cyber security, moreover, recognizing the importance of developing and underdeveloped Member States in the creation of regional and global cybersecurity frameworks, in pursuit of a safe world order in international cyberspace,

Saddened by the systemic misuse of cyberspace regarding the harassment and exploitation of women, as acknowledged by The Interagency Network on Women and Gender Equality (IANWGE),

Recalling the UN Secretary-General's *UNiTE by 2030 to End Violence Against Women Campaign* (2015) in answer to the proliferation of violence against women, due to COVID-19, *Aware* of the economic need for women in the cybersecurity workforce as promoted by UN Security Council resolution 1325 (2000), reaffirming the importance of women in global peace and security,

Deeply concerned with the lack of cybersecurity safe-use practices that can harm families and children in developing countries,

Recognizing that cyberattacks carry vast potential for creating inter-state conflicts that put the development of least developed countries (LDCs) at great risk,

Understanding the need for the input of developing nations on cybersecurity to ensure unsustainable cycles of dependency do not occur,

Cognizant that governments engage in cybersecurity from many angles and motivating factors,

1. *Invites* the possibility of exploring surveillance systems developed by the private sector to create a global strategy to establish a cybersecurity initiative education system;

2. *Requests* total inclusivity of developing and undeveloped Member States in the creation of any global or regional cybersecurity framework, shared global databases, establishment of independent cyber organizations, and educational forums;

3. *Recommends* that cyber security be defined by the body as the frame of technologies, mechanisms, and practices designed for the purpose of protecting people and institutions' networks, their devices, programs, and data from any form of damage, attack, or unauthorized access;

4. *Recommends* establishing dialogues and cooperation between *The Global Forum on Cyber Expertise* on norms and standards in cyberspace, encouraging the creation and further development of cybersecurity partnerships for public authorities, the business community and civil society organizations to create a set of basic security measures;

5. *Decides* to expand participation in the Group of Governmental Experts (GGE) through extending open invitation for participation in the GGE to all willing and able Member States, which will ensure that the developing perspective will be adequately represented in global discussion on the topic of cybersecurity;

6. *Recommends* the expansion of the United Nations Office on Drugs and Crime (UNODC) Cyber Security Depository through the inclusion of a cyber threats and global frameworks database to assist Member States in the development of global cyber norms and standards;

7. *Draws attention to the* creation of an annual, online education forum called *LearnCyber*, which will allow all willing Member States to share best practices regarding cybersecurity and work with relevant UN bodies such as the UN Institute for Disarmament Research (UNIDIR) by:

    a. Collaborating with other participating Member States on proactive methods to prevent cyber-attacks, and;

    b. Asking for funding from the General Assembly Fifth Committee to be allotted for cybersecurity education;

8. *Requests that* Member States offer expertise and technology to developing states to aid these states in creating their own cyber platforms along with a modern, advanced cybersecurity system by:

    a. Relying on the United Nations Office of Disarmament Affairs (UNODA) and the International Criminal Police Organization (INTERPOL) to organize this information and technology and to distribute it to states in need, and;

    b. Facilitating cooperation between Member States in a variety of agreements to enhance the technical capacity of developing countries;

9. *Requests* the referendum of pre-existing cyberspace agreements to expand cybersecurity enhancements to accommodate for modern technology and future development of technology by:

a. The utilization of non-governmental organizations (NGOs), such as the Global Commission on Internet Governance, as an overseer of established security measures, eliminating an individual state’s bias for aide, if conflict between states were to occur via cyberspace, and;

b. Allowing for the expansion and development of new security measurements across nations with the research and sharing of information for effectiveness;

10. *Expresses its hope* that fellow Member States will consider using the guidelines of the European Network Information Service (NIS) Directive to establish a National Computer Security Incident Response Team (CSIRT) that:

a. Is responsible for responding to cybersecurity incidents in different infrastructures,

b. Enhances internal security, prevention, and preparedness,

c. Enhances effective responses to incidents that could affect the operation of critical infrastructures in both and private sectors, and

d. Creates cooperation among Member States and the European Commission to share early warnings on risks and ongoing threats, in the hopes of moving toward the creation of a Joint Cyber Unit;

11. *Recommends* the reconvening of the Open Ended Working Group (OWEG) to expand the current international cybersecurity framework to include the growing concerns and needs of developing Member States by assessing methods to:

a. Advance the development of information technology (IT) and cyber security measures for Member States that don’t have the funds and the resources to pursue the creation of such technologies,

b. Promote cooperation between Member States and the private sector to ensure target-oriented tools to achieve solutions that cover different issues present in each individual sovereign,

c. Create funds for developing Member States for the advancement of cybersecurity development, and

d. Encourage the formation of NGOs that focus on the specialized needs of developing Member States, as well as increasing information sharing among the developing world;

12. *Advocates* that Member States address Violence Against Women and Girls (VAWG) and the femicide rates around the world being exacerbated by cybercrime and the spread of heinous crimes via internet usage and cyber hacks by:

a. Increasing awareness of vulnerable populations on internet accounts, databases and groups through educational forums utilizing INTERPOL, which addresses 190 Member States with opportunities to collaborate on international cybercrime, and

b. Spreading information regarding cybercrime against women as exemplified by The Council of Europe’s *Action Against Cybercrime* by utilizing technological information provided by the UNODC through the Sharing Electronic Resources and Laws on Crime (SHERLOC) database and Cybercrime Repository;

13. Suggests that the International Telecommunication Union (ITU) in conjunction with the United Nations Educational, Scientific and Cultural Organization (UNESCO) continue to spread awareness of cybercrime and VAWG through the Broadband Commission of Digital Development, specifically regarding cyberstalking and sexual exploitation through illicit images;

14. Encourages the spread of economic opportunities for women in the cyberspace and cybersecurity workforces through commitments like the Women’s Empowerment Principles (WEP) in conjunction with UN-Women and the UN Global Compact:

a. Acknowledge women's unique perspectives and assets to combat cyberterrorism and additional cybersecurity issues relating to General Assembly resolution 60/288 (2006),

b. Promoting employment of women in cybersecurity efforts and cyber-related businesses, by utilizing Gender Advisors across all peacekeeping functions involving cybersecurity, including, but not limited to the UN Office of Counterterrorism (UNOCT), INTERPOL, UNODC, and ITU,

c. Promoting the Cybersecurity and New Technologies Programme through the UNOCT to UN-Women Security Council 939 (2015), and

d. Enabling the success of women through cybersecurity jobs and educational opportunities through the (WPS) Women, Peace and Security Agenda in line with the Security-General's Action for Peacekeeping Initiative (A4P);

15. *Recommends* the World Health Organization (WHO) to collaborate with Member States to create safe spaces addressing the sexual exploitation of Children in cyberspace through:

a. Promoting the adoption of a specific national plans of action against sexual exploitation of children with clear and precise objectives including the revised structure of the WePROTECT Global Alliance while having the adequate budgetary provisions allocated,

b. Undertaking awareness-raising campaigns to prevent online sexual exploitation, and

c. Developing recovery and reintegration programmes for child victims of any sexual exploitation including online pornography with the help of the INTERPOL, European Union Agency for Law Enforcement Cooperation (EUROPOL);

16. *Reaffirms* the importance of Member States and private organizations combating propaganda and online terrorist presences to hamper terrorist recruitment and reduce the influence of violent extremist groups among young populations;

17. *Further recommends* working with the Cooperative Cyber Defense Centre, in order to reinforce and maintain a secure cyberspace environment to support SDG 17 by understanding the importance of a secure cyberspace environment in both the public and private sector;

18. *Urges* the creation of a UN Forum focused on cyber security in collaboration with the OWEG for developing Member States that will:

a. Allow the participation of NGOs, individual experts, and Multinational Corporations (MNCs);

b. Address many of the specialized concerns developing Member States have in regards to cybersecurity, and;

c. Create a safe space where developed Member States can share their expertise and assist developing Member States in transitioning into a safe cyberspace as well as aiding them in implementing the guidelines set by the Budapest Convention in 2004;

19. *Further recommends* working with the Cooperative Cyber Defense Centre, in order to reinforce and maintain a secure cyberspace environment to support SDG 17, understanding the importance of a secure cyberspace environment in both the public and private sector, which could fill the gap with the implementation of public-private partnerships (PPPs), inclusion of CSOs, and NGOs to further build on the SDG 17;

20. *Urges* the creation of a UN Forum focused on cyber security for developing Member States that will:

a. Be made up of any developing or developed state that is willing to engage and participate in cybersecurity concerns;

b. Allow the participation of NGOs, individual experts, and MNCs;

c. Address many of the specialized concerns developing state have in regards to cybersecurity;

   d. Encourage Member States to participate in government to government cybersecurity collaboration efforts, and;

   e. Create a safe space where developed Member States can share their expertise and assist developing and less developed Member States in transitioning into a safe cyberspace as well as aiding them in implementing the guidelines set by the Budapest Convention;

21. *Encourages* Member States to initiate or continue cooperation through organizations such as the GGE and a multitude of regional organizations formed by UNODA at an annual conference to discuss ongoing and new issues in the area of cybercrime and further task it by:

   a. Authorizing yearly reports to the Secretary-General;

   b. Proposing enhancements of cybersecurity measures;

   c. Furthering the purview and application of international law into cyberspace area, and;

   d. Introducing under UNIDIR the task of monitoring ICT;

22. *Further encourages* an undertaking an observational yearly study of a voluntary participatory nature with the conclusion and results being dispersed to all Member States, no later than three months after adjournment of the preceding conference, having gathered and examined data on state behavior in cyberspace including contexts such as:

   a. Confrontations in cyberspace between state and non-state actors, as well as conflicts between Member States in cyberspace, and;

   b. Novel developments and threat management practices within developed Member State cyber defense institutions, and developing states working to integrate cyber defense into established security organizations.

Code: GA1/1/4
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Acknowledging that Article 12 of the United Nations (UN) Universal Declaration of Human Rights (UDHR) (1948) designates privacy as a human right,

Understanding Article 19 of the UDHR, which outlines the universal right to free speech as a human right,

Expressing concern over the lack of global preparedness in regards to the increasing development of technological attacks and their use in terrorist acts across the globe, which is in direct opposition of the General Assembly resolution 71/291 (2017),

Recognizing that responsible state behavior not only implies the seeking out and neutralization of cyber threats, but also the active protection of a state's population from said threats,

Affirming the commitment among Member States found in General Assembly resolution 57/239 (2003) to create a global culture of cybersecurity which encourages Member States to voluntarily share information regarding cybersecurity and preventative measures,

Noting with concern that according to Cybersecurity Ventures, a non-governmental group of experts, cybercrime damages might reach US$6 trillion in 2021,

Recalling the International Telecommunication Union (ITU) Global Cybersecurity Agenda which provides a framework for international cooperation in the context of cybersecurity,

Acknowledging that a 70% increase in internet users due to COVID-19 and increasing digital dependency increases the risk of misinformation and increase malicious cyber activity,

Concerned by the lack of communicative platforms between Member States to promote a place of collaboration among Member States,

Declaring the need for more widespread dissemination of information pertaining to information and communications technology (ICT) usage and cybersecurity in the context of an increasingly digital society with constantly evolving knowledge bases in both developing and developed Member States,

Noting Article 1.1 of the UN Charter, as a lack of understanding of effectively utilizing ICT technology to combat cybercrime directly impedes international peace and security,

Aware of the global shortage of cybersecurity professionals, especially in developing Member States,

Bearing in mind that the increase in incidents of transnational cybercrime threatens individuals, industries, and governments, as reported by the Open-Ended Working Group (OEWG),

Acknowledging the rapidly developing nature of cyber threats and the inherent risks they pose to the Sustainable Development Goals (SDG) for 2030,

Recalling the commitment to SDG 9 towards promoting sustainable industrialization, building resilient infrastructure, and fostering innovation,

Recalling the objective of SDG target 16.4 to reduce organized crime across the globe,

Recognizing the vulnerability of populations without proper education on information and communication technologies (ICT) to cyberattacks,

Emphasizing the impact digital illiteracy has on cybersecurity vulnerability, as well as the disproportionately high number of mobile device users in relation to mobile devices inherent cybercrime vulnerability as reported by the International Telecommunication Union (ITU) in measuring digital development facts and figures, *Guided by* SDG 17, which aims to ensure international partnerships and collaboration, and relating to the topic of technology,

Recognizing that terrorist threats use cyberspace to solicit and trade weapons,

1. *Encourages* the inclusion of discussion on upholding human rights including privacy in the context of cyberspace, to be included in the 2022 General Assembly Provisional Agenda to further international cooperation in upholding human rights as a facet of responsible state usage of cybersecurity;

2. *Strongly encourages* the development of an established list of procedures that limits, enforces, and depicts the appropriate usage of cyberspace in regards to all Member States' governmental operations, including:

    a. Supporting the creation of a UN team of technological experts that are dedicated and tasked with managing cybersecurity in all Member States, which would include the responsibilities of:

        i. Being a source of expertise for Member States to access in regards to state governmental cyber usage,
        ii. Providing defensive tactics, including cyber-assistance dispersion when Member States are in need of such,
        iii. Monitoring said procedural list referenced above; and

    b. Further supporting the development of an emergency response team including professionally trained individuals who specialize in cybersecurity within the UN to handle privacy breaches in cyberspace by non-state and state actors;

3. *Establishes* the Cyber Threat Information Database Committee (CTIBC) as a partnership committee between the ITU and the Commission on Crime Prevention and Criminal Justice (CCPCJ), in which the identities and methods of previous cyber threats can be easily accessed by all Member States, as well as the necessary countermeasures to such threats through:

    a. Creating a Cyber Threat Information Database (CTIB) to catalogue cyber threats and their remedies through voluntary contributions by Member States;

    b. Publishing annual reports on CTIB contributions,

    c. Releasing recommendations on how Member States can best utilize the information contained within the CTIB, and

    d. Declaring that the success of the CTIB is determined by the volume of contributions and involvement of Member States in the annual reports;

4. *Strongly encourages* the enhancement of global cyberinfrastructure to promote responsible state behavior in cyberspace by:

    a. Suggesting that the UN Office on Drugs and Crime (UNODC) Cybercrime Repository, in collaboration with International Criminal Police Organization (INTERPOL), create a cyberattack database, allowing Member States to report incidents of cyberattacks,

    b. Considering that developing Member States and those with limited resources would be incentivized to report incidents so that they have the resources and information they need to know where they are being attacked from, and

    c. Creating a cybersecurity program called SafetyNET, which implements efforts led by the UN Office of Information and Communications Technology (UNOICT) to assess cybersecurity risks, provide cyber protection resources from Member States and emphasizes the importance of sharing cyber safety best practices and policy recommendations to enhance and protect cyber infrastructures;

5. *Recommends* the establishment of an international platform, in collaboration with the Global Cybersecurity Index (GCI) and UNODC, which will set guidelines to aid Member States in

establishing proper reporting systems on the resilience of cyberspace and existing cyber crimes and provide recommendations for Member States accordingly, through regular cross-evaluation of international cooperative councils to ensure that laws are up to date and are properly being enforced;

6. *Encourages* a panel of experts that will utilize the Budapest Convention's guidelines, GCI, and ITU's guidelines to guide local law enforcement units, INTERPOL, and UNODC on the best uses of emerging technologies to efficiently track and monitor the progress on combating cyber attacks and establish a resilient system to protect critical data through the use of AI technologies;

7. *Requests* the General Assembly establish an annual forum held once a year, where all Member States are able to participate in discussions regarding the continuous implementation of international norms and practices in cyberspace, as well as discussing and participating in the collaboration of sharing information on cybersecurity and tactics to combat cyberattacks by state and non-state actors, which will provide the opportunities to:

    a. Promote and foster confidence and congeniality between Member States regarding the current state of cyberspace,

    b. Allow Member States to denounce cyberattacks stemming from their own borders as well as state potential prosecution actions of said state or non-state actors,

    c. Discuss updates on cyber infrastructure, capabilities, and risk assessments to encourage the improvement of cyberspace to better all Member States, and

    d. Measure overall success by Member States willingness to share information in order to encourage participation;

8. *Supports* the establishment of an international framework for voluntary consultative meetings with relevant Civil Society Organizations (CSOs), National Governmental Organizations (NGOs), cybersecurity experts, other stakeholders, and Member States for the purpose of pooling intellectual capital, data sharing, data collection, and enabling the growth of cybersecurity expertise across Member States;

9. *Further recommends* that the UNODA create a conference for national law enforcement agencies utilizing the expertise from the UNODC Global Programme on Cybercrime and the UN Office of Transnational Organized Crime to inform law enforcement on best practices for combating cyberattacks, especially to protect critical infrastructure from cyberattacks;

10. *Encourages* Member States to expand on existing partnerships with intergovernmental organizations in accordance with SDG 17 to collaborate with regional and subregional organizations in conducting cyber knowledge and technical skills transfer for the maintenance and strengthening of the capacities of Member States against cyber insecurity that would collaborate with the following but is not limited to the:

    a. ITU for policy-makers, legislators, public prosecutors, and investigators,

    b. United Nations Institute for Disarmament Research (UNIDIR) to conduct research for the private sector and civil society organizations, and

    c. Information Systems Security Association (ISSA) for international and national cybersecurity professionals and practitioners;

11. *Calls upon* the ITU and the CCPCJ to develop a Model Cybersecurity Strategy (MCS) which Member States can either implement or use to enhance existing national strategies and which should include but are not limited to measures to:

    a. Protect critical information infrastructure,

    b. Standardize core security requirements; raise citizen's awareness,

    c. Establish an incident response capability,

d. Maintain the right to free speech,

e. Foster research and development in the field of cybersecurity, and;

f. Promote international cooperation;

12. *Requests that* cooperation of international law enforcement is strengthened to facilitate investigations of cybercrime by:

    a. Focusing on the need to combat the cybercrime enforcement gap between Member States and overcome barriers to cooperation,

    b. Encouraging Member States to increase communication with INTERPOL to share data relevant to criminal investigations on a case by case basis,

    c. Supporting further coordination between other UN entities to implement guidelines for the responsible use of digital evidence in transnational cybercrime investigations, and

    d. Recommending the expansion of Official Development Assistance to assist in the implementation of Computer Emergency Response Teams (CERT) in developing Member States to strengthen national law enforcement capabilities;

13. *Supports* the ITU's telecommunication development sector to secure cyber communications to detect when terrorists are using cyberspace to communicate through guidance and expertise in any expansions related to cyber communication;

14. *Calls upon* Member States to apply SDG 16.4 when creating policies combating the spread of organized crime perpetuated in cyberspace, with special attention given to:

    a. Communication between government and civilian investigative entities at the regional and national levels,

    b. Collaboration with regionally located technology companies to ensure devices have higher levels of protection to prevent cyberintrusions by malicious entities, and

    c. Cooperation between functional regional defence centres to successfully train and defend themselves from cyberattacks;

15. *Urges* infrastructure implementation to include ICTs, aiming for affordable and fair access to quality cybersecurity capabilities, particularly least developed countries (LDCs), landlocked developing countries (LLDCs), and Small Island Developing States (SIDS);

16. *Encourages* the General Assembly Second Committee to explore the usage of Public Private Partnerships (PPPs) as avenues to prevent vulnerable populations from being overexposed to both cybercrime and the adverse effects of digital illiteracy through education programs for civilian and government entities;

17. *Recommends* the creation and implementation of regional defence centres, such as the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center of Excellence aided by Member States with significant cybersecurity programs in order to tackle cyber threats;

18. *Proposes* the creation of Government Operations Security Centers and IT Emergency Response centers that allow the private-sector easy access to government cybersecurity services;

19. *Recommends* the implementation of SDG 17 through international cooperation in cyberspace via:

    a. Creating and implementing regional defense centers, such as the NATO Cooperative Cyber Defense Center of Excellence aided by Member States with significant cybersecurity programs in order to tackle cyber threats,

    b. Fostering cooperation in the ICT fields between developed and underdeveloped countries creating Research and Training (R&T) centers, such as the Development Gateway Foundation (DGF) of the World Bank,

c. Creating a center that allows the private sector and draws its attention in cybersecurity and help to implement the creation of e-government,

d. Developing a Group of Governmental Experts as a central group to ensure that the goal is being achieved, and

e. Creating a forum within the UNODA to share each other's work towards battling cybercrimes.

Code: GA1/1/5
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Acknowledging the ever increasing role that technology has in everyday interactions,

Alarmed by the current 4.66 billion internet users and the projected 3 billion new potential targets for cybercrimes by 2030,

Realizing the need for preventative measures that ensure responsible state behavior in cyberspace, occurring through administrative organizations in dealing with cyber conflicts that arise, internationally, regionally, and at the state level,

Encouraged by commissions and research to establish information to understand what is necessary to lay the structure for responsible behavior in cyberspace of Member States,

Calls attention to the final report of the Open-ended Working Group (OEWG) on *Developments in the Field of Information and Telecommunications in the Context of International Security*,

Recognizes the African Union's *Convention on Cybersecurity* (2014) as a guiding and credible framework on cybersecurity to ensure the protection of personal data, promotion of cyber security, and e-governance,

Cognizant of the potential of cyberspace and technology to enhance cybersecurity, as well as the need for Member States to increase cyber infrastructures,

Noting that the Suspicious Email Reporting Service (SERS) initiated by the United Kingdom has made an outstanding contribution in the context of cybersecurity,

Recognizing an escalated demand to better understand acceptable and safe practices in cyberspace, due to the increased usage of the internet during the COVID-19 pandemic, and the rise in the number of cybercrimes,

Affirming the 2015 Group of Governmental Experts Report to guide international law, voluntary norms, and centrality of the United Nations Charter,

Taking note of the necessity of equality at all levels of law, education, and the failures of Information Communication Technologies (ICTs) and cyberspace in the inclusion of women and minority groups,

Acknowledging the significant contribution made by the *Budapest Convention* (2001) towards addressing cybercrime by harmonizing national laws,

Recognizing the need for universally established laws and protocols,

Recognizing the great contribution of the Working Group on Ethical and Legal Artificial Intelligence (AI) in Europe's Artificial Intelligence for European Union (AI4EU) on the use of AI across the region,

1. *Encourages* Member States that have highly developed cybersecurity infrastructure, to consider the establishment of national or regional Computer Security Incident Response Teams (CSIRTs) that would help with global efforts to further understand what will be acceptable in cyberspace and:

    a. Invites all Member States to voluntarily guide the establishment of a CSIRT, such that:

        i. The CSIRTs seek to enhance internal security, prevention, and preparedness towards cyber threats through the monitoring of these threats to security;

        ii. The CSIRTs will seek to enhance the response to such incidents that affect the operation of critical infrastructures, both public and private;

        iii. The CSIRTs will monitor and submit reports on the progress of Member States in improving cyberinfrastructure; and

   b. Reminds Member States with highly developed cybersecurity infrastructure, to consider the General Assembly’s solidarity in the *Budapest Convention* in the establishment of CSIRTs;

2. *Proposes* the adoption of an international cybersecurity platform informed by programs, such as CSIRT, for all Member States’ dedication to dealing with the misuse of cyberspace, cyberattacks, the spread of misinformation, and to uphold a universal code of conduct;

3. *Encourages* the utilization of a Virtual Task Force that would provide technical assistance in assessing and investigating the cybercrimes, as well as the misuse of improper use of encryption in the dark web while protecting citizens who use similar encryption methods elsewhere, through a collaboration with but not limited to the International Cybersecurity Protection Alliance (ICSPA) and Global Cyber Security Capacity Centre;

4. *Further encourages* the creation of a regional judicial expert group to utilize internationally recognized best practices in the sphere of cyberspace, in order to advise and make recommendations for Member States on the best methods to strengthen local legislation in the context of cyberspace;

5. *Suggests* the advancement of national capacities against data breaches through leveraging international and regional think tanks, which include but is not limited to the Center for Strategic Cyberspace and International Studies (CSCIS), International Institute for Strategic Studies (IISS), and regional think tanks, such as but not limited to, Oceania Cyber Security (OCSC),The Institute for Regional Security, Chatham House - Europe, LIRNEasia, and Research ICT Africa;

6. *Further suggests* the formulation of methodological frameworks in the propagation of cybersecurity models through Artificial Intelligence (AI), in collaboration with the International Telecommunication Union (ITU), including but not limited to:

   a. Outlining Security Risk Vectors through cybersecurity vulnerability and exposure assessments,

   b. Mapping Cybersecurity Maturity to identify security requirements and capacities,

   c. Employing analysis mechanisms to determine appropriate cybersecurity models, and

   d. Collaborating with the International Society of Automation (ISA) in the establishment of cybersecurity standards in this framework;

7. *Further reminds and invites* cooperation of all Member States in the strengthening of international cooperation efforts and the exchange of information guided by treaties such as the *Convention on Cybercrime* of the Council of Europe through:

   a. The binding enforcement against cybercrime,

   b. Participation of Least Developed Countries (LDCs), and

   c. Confidence-building strategies amongst Member States;

8. *Requests* a report be published by the Secretary-General's office exploring how the inclusion of women, minority groups, and LDCs can further contribute to:

   a. All substantive discussions on state-actor and non-state actor cyber security behavior,

   b. Education programs designed to reduce digital illiteracy, and

   c. Leadership roles in future ITU, cyberspace, and AI usage;

9. *Encourages* Member States to collaborate and establish a convention, modeled after the Budapest Convention, in order to efficiently tackle cybercrime, including, but not limited to:

   a. Illegal access,

   b. Illegal interception,

c. Data interference,

d. System interference, and

e. Misuse of devices;

10. *Further suggests* the creation of an international convention modeled after the efforts of the African Union (AU) Convention on Cyber Security and Personal Data protection to:

    a. Provide a framework to Member States of the AU, in order to standardize cybersecurity laws regionally and better protect states on the state, and;

    b. Collaborating with Economic Community of West African States (ECOWAS) commission, in order to protect the national infrastructure and ensuring the protection of neighboring states;

11. *Requests* a comprehensive report be published by the UN Secretary-General's Office exploring:

    a. All substantive discussions on Member States' cybersecurity behavior,

    b. The development of innovative development of innovative education programs designed to bridge the digital divide, and

    c. Leadership roles in future ITU, cyberspace, and AI usage on the international scale;

12. *Encourages* the use of the Suspicious Email Reporting Service (SERS) at the international level in combatting:

    a. Spear phishing emails targeting government entities,

    b. Different misuse of social media, and

    c. The increase in threat vectors brought about by the internet;

13. *Recommends* the endorsement of a voluntary adoption for universal standards and cyber norms for state behavior in cyberspace with the goal of building confidence and transparency based on the 2021 findings of the Groups of Governmental Experts (GGE) by:

    a. Information gathering from Non-Governmental Organizations (NGOs) and bipartisan think tanks;

    b. The promotion of voluntary norms for responsible state behavior, and;

    c. Establishment of a universal database for sharing of information regarding cybersecurity;

14. *Further invites* the establishment of a protocol guided by the Budapest Convention, African Union's convention on Cybersecurity, ICTs and the Global governance of peace and security project, and the reports by the GGE to guide activities within the sphere of cyberspace in order to clearly define an internationally accepted mechanism to address the functionality and regulations of cyberspace;

15. *Invites* the formulation of National Broadband Plans (NBPs) in underdeveloped network countries by:

    a. Consulting the plan with representatives of the private sector, the public sector, and civil society organizations,

    b. Establishing national minimum development targets with clear metrics and time limits, and each target should at a minimum cover network coverage and data affordability, and

    c. Funding must be committed and a transparent assessment and review plan should be conducted at least once every two years;

16. *Further requests* financial assistance from governmental and intergovernmental organizations for the aforementioned enhancement of cyberinfrastructures, such as the United Nations Office of Counter-Terrorism (UNOCT) and World Bank (WB);

17. *Suggests* using the expertise and knowledge of Working Groups on ethical and legal AI in Europe's AI4EU and the ITU’s Global Forum of Cyber Expertise (GFCE) to assist the GGE in expanding their working range.

Code: GA1/1/6
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Aware that the Federal Trade Commission on International Consumer Protection (FTC) received more than 2.1 million fraud reports from consumers in 2020, with imposter scams remaining the most common type of fraud reported,

Recognizing that cybercrime is a global problem and providing importance in the expansion of national legislation and international cooperation in the fight against cybercrime,

Acknowledging that a free and secure cyberspace as the necessary condition to prevent human rights violations and requests access to cybersecurity to developed and developing Member States,

Recalling the Council of Europe Treaty No. 185 Convention on Cybercrime, which requires signatories to criminally prosecute those actors who commit cybercrimes,

Emphasizing the need for ardent international collaboration when facing the global threat of unfavorable Member State behavior in cyberspace poses to international peace and security,

Welcoming efforts that advance information sharing and cooperation between Member States and protection agendas set by the United Nations Global Counter-Terrorism Strategy,

Recalling the United Nations Convention on the Rights of the Child that highlights to protect children from all forms of online sexual exploitation and sexual abuse,

Considering the heightened threat of cyber-attack facing less-developed Member States,

Cognizant of the potential of cyberspace and technology to enhance cyber security, as well as the need for Member States to increase cyber capacities,

Alarmed by state and non-state actors are increasingly using cyberspace as a platform for potentially unfavorable behavior that targets essential infrastructure and citizens, undermines democracies, international institutions and organizations, and undercuts fair competition in the global economy,

Reaffirming General Assembly resolution 74/28 (2019), stating that all Member States have a responsibility in maintaining international peace and security in the information and technologies environment, with effective interstate cooperation within the international community to ensure safe cyberspace for all,

Concerned with the global cybersecurity workforce shortage that has been projected to reach upwards of 1.8 million unfilled positions by 2022 while 85% of organizations globally are challenged by information technology (IT) security skills shortage,

Promoting the cooperation between Member States and private sector entities specialized in cybersecurity,

Noting with approval General Assembly resolution 73/27 (2018), which calls attention to the importance of using ICTs for the common good of people,

Calling attention to the Global Cybersecurity Agenda (GCA) which establishes a framework for international cooperation aimed at enhancing confidence and security in the information technology society,

Viewing with appreciation the advent of Apps 4 Digital Peace, a first-of-its-kind competition to stimulate new thinking from innovative young minds across the world,

Noting with concern the proliferation of cyber-weaponry amongst state and non-state actors,

1. *Encourages* the development of an accreditation process to protect consumer from phishing scams and help allow for non-intrusive online trade, fraud, and counterfeit corporations from interfering with daily commerce which will:

a. Compile a list of all cyber scams onto regional data repositories sponsored by the International Telecommunications Union (ITU) that the public could access,

b. Enhance public education on consumer-targeted cyberattacks through programs coordinated by UN Office for Project Services, including:

    i. Social media promotion,
    ii. Working with Member States' government cybersecurity agencies to educate targeted corporations,
    iii. Emphasizing the importance of fostering voluntary collaboration between the private and public sector, and

c. Receive potential funding from National Lottery Community Fund, The Coca-Cola Foundation, Inc., Flower Hospital, The Ian Potter Foundation, and The William and Flora Hewlett Foundation, among other non-state actors interested in contributing to support economic growth of Member States;

2. *Suggests* an immediate expansion of *Treaty No. 185 Convention on Cybercrime* to include criminal policy for those Member States that directly initiate or sponsor non-state actors who pursue cyber-attacks and use harmful malware against other Member States, as well as open the treaty to include other signatories outside the Council of Europe;

3. *Recommends* that the United Nations (UN) Security Council establish an annual forum for Member States to participate in discussions regarding the establishment of international norms and practices in cyberspace, as well as discussing the benefits of sharing information on cybersecurity and tactics to combat cyberattacks by state and non-state actors;

4. *Encourages* Member States to adopt revisions made to the United Nations Global Counter-Terrorism Strategy, extend commitment made to the UN Counter-Terrorism Implementation Task Force Working Group (CTITF), and Security Council resolution 2341 (2017) regarding information sharing and protection of critical infrastructure from terrorist attacks;

5. *Encourages* Member States to enhance, as appropriate, international and regional cooperation, especially, regarding training on good practices, between the UN General Assembly and the International Criminal Police Organization, International Association of Chiefs of Police, European Union Agency for Law Enforcement Cooperation (EUROPOL), International Criminal Police Organization (INTERPOL), European Union Agency for Cybersecurity (ENISA), and the North Atlantic Treaty Organization (NATO), in an effort to prosecute cyber-criminals;

6. *Encourages* Member States to establish an International Cyberspace Monitoring Center (ICMC) comprised of private-sector experts, non-government organizations (NGOs), international law enforcement, and Member States, which would:

    a. Enable participating bodies to organize regional reports on cyberspace, cybersecurity, and the future of institutional and professional cyberspace education internationally, to improve the common grounds, understanding, and guidelines in the use of cyberspace,

    b. Enhance the capacities of participating bodies by collaboratively developing digital systems and instruments to further secure and monitor cyber-activities, particularly by enhancing, monitoring, and tracing digital footprints through the use of firewalls to mitigate illegal activities, enabling them to produce plans of action that are regionally accommodating, satisfying both the needs of developed Member States, as well as providing infrastructural security for developing Member States, particularly through the mitigation of online illegal and terrorist activities, including:

        i. The trade of illicit Small Arms and Light Weapons (SALW) through cyberspace;
        ii. International human trafficking facilitated through cyberspace;
        iii. The spread of terrorist content online;
        iv. The propagation of informatics with malicious intent, especially in the context of health issues considering the COVID-19 pandemic;

v. Online terrorist communications;
vi. Digital fraud and terrorist financing;
vii. Cyberattacks and digital espionage;

7. *Creates* an ICT platform for handling terrorist purposes and implement other appropriate cooperative measures to address such threats;

8. *Encourages the establishment of* an International Cyberspace Monitoring Center sub-committee responsible for addressing the illicit trade of Small Arms, Light Weapons, and fissile material throughout cyberspace in all its aspects (SALWF-CS), to better prepare the global community to combat such challenges by:

    a. Hosting an annual General Assembly First Committee side-event to present real-time occasional reports on "The Trade in Small Arms and Light Weapons on the Dark Web," and

    b. Requests that existing funding dedicated to programs falling in the aforementioned categories remain dedicated to such programs, but that these programs be either reclassified under the International Cyberspace Monitoring Center (ICMC) or officially associated with the ICMC, to ensure maximum return on investment and establish truly a safe, secure, equitable, and widely accessible cyberspace;

9. *Promotes* the development of safe cyberspace practices, protections, and education in developing Member States where inhabitant access to the internet isn't common, with a specific focus on:

    a. Cooperation in the ICT fields between developed and underdeveloped countries by creating Research and Training (R&T) centres, such as the Development Gateway Foundation (DGF) of the World Bank,

    b. Usage of Public Private Partnerships (PPPs) as avenues to prevent vulnerable populations from being overexposed to both cybercrime and the adverse effects of digital illiteracy through education programs for civilian and government entities, and

    c. Expand protections against harassment, exploitation, and recruiting of women and children in cyberspace;

10. *Suggests* the establishment of robust and reinforced cyber infrastructures for the purpose of the upholding the United Nations Convention on the Rights of the Child that focuses on the following to be assisted by the United Nations International Children's Emergency Fund (UNICEF) but not limited to the:

    a. Coordination with the Virtual Global TaskForce (VGTF) in creating online deterrence activities to combat technology-facilitated crimes against children,

    b. Utilization of the Child Sexual Abuse Anti-Distribution Filter of the European Commission as a blocking mechanism for Internet Service Providers, and

    c. Identification of best practices in curbing commercial exchange of child exploitation material in collaboration with the International Centre for Missing and Exploited Children through its Financial Coalition Against Child Pornography;

11. *Invites* the implementation of methods that foster a culture around the promotion of cybersecurity which:

    a. Encourages Member States to support the development and implementation of sustainable development credits as a public, distributed ledger based on blockchain technology that only exist only in accounts established by the ledger to enhance security and transparency,

    b. Urges the creation of a voluntary database where Member States can disclose cybersecurity practices that:

        i. Allow for Member States with less experience with cybersecurity practices to have access to information about cybersecurity;

ii. Provide recommendations for Member States about which cybersecurity practices to implement;

12. *Acknowledges* that a free and secure cyberspace as the necessary condition to prevent any primary and secondary human rights violation and requests access to cybersecurity to developed and developing Member States;

13. *Encourages* the establishment of an international treaty monitoring and limiting the sale of cyberweapons between member states, which will be in the mold of the Arms Trade Treaty and will be administered by the UN Office of Disarmament Affairs (UNODA);

14. Enhance the norms, guidelines, and technology used to facilitate democratic processes to ensure a comprehensive accessibility, reliability, and security when utilizing information and communication technologies in procedures such as elections through electronic voting, that:

    a. Provides reliability during times of local, regional, and international major crises situations,

    b. Ensures that no eligible voter is disadvantaged in the voting process and is offered an easy and straightforward way to vote through cyberspace,

    c. Enables Member States to utilize safe platforms for electronic voting guided through rule-based protocols to ensure the compatibility of election processes.

Code: GA1/1/7
Committee: General Assembly First Committee
Topic: Advancing Responsible State Behavior in Cyberspace in the Context of International Security

The General Assembly First Committee,

Considering the necessity of improving cyberspace security, with the combined efforts of international member states, as cyberspace security both threatens developed and developing Member States,

Recalling the General Assembly resolution 53/70 (1999) for a better understanding in the field,

Reminding Member States that the internet is used for day-to-day functions of the economy especially in the wake of the COVID-19 pandemic,

Acknowledging the importance of new regulation as new technologies such as artificial intelligence (AI) and cryptocurrency usage,

Following the guidance of General Assembly resolution 73/266 (2018), which underlines the necessity for cooperation between Member States,

Taking into account the International Telecommunication Union (ITU) Global Cybersecurity Agenda (GCA) as a framework for international cooperation and the promotion of a safer information society,

Expressing its concern with the rise of phishing emails and malware used in nefarious instances that attempt against security in cyberspace,

Considering cryptocurrency is decentralized and proven to be untraceable and very difficult to deal with by International governments, this transparency allows traffickers to trade small arms and illegal goods into possibly high tensioned areas, causing several damages into infrastructures also spreading poverty and instability,

Condemning the Media Censorship in cyberspace that has been used by the Member States around the globe taking advantage of cyberspace media to spread false information, and misleading news to a mass audience which has the civil consent of the free media and has caused disagreement among civil society,

1. *Highly recommends* the regulation and transparency of cryptocurrency, considering the risk for cybersecurity:

    a. Suggesting Member States establish surveillance by International Agencies regulated by Economic and Social Council of the United Nations and The Global Commission on the Stability of Cyberspace to review the use of cryptocurrency and prevent its involvement in transactions for illicit activities;

    b. Encouraging the introduction of policies to prevent the usage of cryptocurrency in illegal goods and human trafficking, and;

    c. Inviting centralized cryptocurrency, to promote more transparent transactions for the prevention of illicit activities;

2. *Condemns* the use of cryptocurrency from public institutions in untraceable transactions in relation to illicit activities in cyberspace, specifically in developing Member States which:

    a. Prevent public institutions from creating illicit businesses, that may produce a negative impact on society infrastructure, destroying opportunities for many working citizens;;

    a. Encourage Member States to adopt policies to keep cryptocurrency transactions records open to the public in order to promote transparency, and

    b. Ensure an international collaboration in tracking illicit movements for funding national and transnational political campaigns in close cooperation with UN Office on Drugs and Crime training to tackle cryptocurrency-enabled Cyber Organized Crime;

3. *Encourages* the regulation of institutional censorship, in the pursuit of freedom in cyberspace and urges Member States to start progress by:

    a. Promoting awareness campaigns in cooperation with civil society, urging Members States to prevent the censorship of free media, and;

    b. Protecting individuals from misinformation and fake news in close cooperation with the UN Information Center and Regional Institutions;

4. *Expresses* its concern about the recurring issue of institutional corruption in developing Member States and vulnerable communities, and how it has migrated into cyberspace, taking advantage of new technologies promoting extortion, suppression, censorship and even financial illicit activities by:

    a. Supporting role of the Member State in ensuring the legitimacy of its institutions and processes against attacks of state and non-state actors with the cooperation of The Transatlantic Commission on Election Integrity (TCEI) and following the guidance of the third principle of the Paris Trust Call on Protection and Security, and;

    b. Preventing the proliferation of illicit activities held in cyberspace especially by public Institutions with the support of Civil Society Organizations (CSOs) as The International Cyber Security Protection Alliance (ICSPA) with regional and national institutions for the straightening of regulation;

5. *Recommends* Member States prohibit the use of phishing emails and malicious links in cyberspace under with the Cybersecurity Tech Accords by:

    a. Encouraging Member States to adopt policies to not click on suspicious links such as staff training for all members on cybersecurity as stated in the first principle of the tech accords, considering everyone needs protection, and;

    b. Promoting the further development of the Group of Governmental Experts (GGE) report on cybersecurity and protection to prevent the proliferation of ransomware and viruses with the proper review the attention of the international community and civil society;

6. *Promotes* Artificial Intelligence (AI) development among Member States and stakeholders for the accomplishment of the Sustainable Development Goals (SDG) considering the positive impact in society by:

    a. Promoting AI security with the cooperation of the Interregional Crime and Justice Research Institute and the guidance of the UN Secretary-Generals Independent Expert Advisory Group on Data Revolution on Sustainable Development for the support of public institutions against cyber-attacks in all forms;

    b. Establishing a new framework for education worldwide taking advantage of AI technology following the guidance of United Nations Education Science and Culture Organisation (UNESCO): guidance for policymakers and also the cooperation of The World Commission on the Ethics of Scientific Knowledge and Technology, and;

    c. Supporting scientific research on AI matters for a positive impact in society taking advantage of new technologies in close cooperation with civil society;

7. *Promotes* the cooperation with regional organizations as the Regional Technical Commission of Telecommunications of Central America and Civil Society Organizations (CSOs) as Internet Society for capacity building and information exchange on infrastructure, education, and health matters for developing Member States by Information and Communication Technologies (ICTs) following the guidance of the Paris Call for Protection and security in cyberspace by:

    a. Inviting Member States and stakeholders to cooperate with regional Initiatives to establish an effective framework for crisis response in telecommunications-related issues in close cooperation with The International Cyber Security Protection Alliance (ICSPA) and accordance with regional and international reports, and;

b. Recommending the realization of workshops promoting the importance of telecommunications in developing countries, in collaboration with civil institutions such as the Association for the Progress of Communication seeking new techniques for cybersecurity.