Code: GA1/1/1
Committee: General Assembly First Committee
Topic: The Implication of Technology on Global Security

The General Assembly First Committee,

Bearing in mind the duty of the United Nations to ensure peace and security as well as ensuring accountability of Member States in accordance with the *Universal Declaration of Human Rights* adopted on December 10th 1948 and the *Geneva Convention on Warfare* 1949,

Observing the definitions by the Human Rights Watch on autonomous weapons and defense systems in order to clarify different levels of autonomy in weaponry,

Acknowledging the technological research and development towards the proliferation of robotic weapons that are capable of indiscriminate destruction, and machines starting to remove human discretion on the battlefield as mentioned by the *Losing Humanity* report,

Recognizing the role that international ethics and social values must play in the regulation of autonomous weapons systems as iterated in the United Nations Institute for Disarmament Research (UNIDIR) report on *The Weaponization of Increasingly Autonomous Technologies*,

Recalling the progress and clarifications made by the third *Convention on Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems* (2016),

Recalling Resolution 2286 of the Security Council that strongly condemns attack damage on civilians and zones of peace from indiscriminate bombing,

Noting particularly the possibility of Lethal Autonomous Weapon Systems increased collateral damage and indiscriminate bombing capabilities, and emphasizing the importance of accountability and responsibility with the use of advanced weapons systems,

Realizing new developments in weapon technology have made it possible for weapons systems to select and attack targets without human intervention as mentioned in the International Committee of the Red Cross's 2016 report on the *Implications of Increasing Autonomy in the Critical Functions of Weapons, therefore limiting the distinction between civilian and military targets*,

Understanding that the technological gap, especially in terms of defense systems and technology, is a significant threat to global security, as it provides an opportunity for violent non-state actors that could be countered by developed nations equipped with technological weapons such as LAWS, to aggressively expand their operations,

Affirming the need to consider the implementation of a strategic goods list that focuses on the production, distribution, and use of military goods and lethal autonomous weapons systems across international markets,

Guided by the principles of *International Humanitarian Law* as stated in 1925 Geneva Convention, in disregarding practices of warfare, which leads to extraneous suffering and that does not properly distinguish between civilians and combatants, and further stressing the importance of raising awareness to private and non-private sectors with regards to possible threats of autonomous weapons which dramatically changed warfare, bringing new humanitarian and legal challenges,

Recalling the draft resolution A/C.1/57/L.30 passed by the General Assembly First Committee which states that no steps should be taken to further outer space weaponization, in addition, the draft international code of conduct

proposed by the European Union established international norms for peaceful use of space domain, placing weapons in outer space would only further technological inequality as only a few countries would be capable of this,

1. *Reminds* Member States of the duty of the United Nations as an international organization of peace to seek peaceful resolutions to world wide conflict;

2. *Promotes* the use of the language in by the Human Rights Watch in terms of classification for autonomous weapons systems:

    a. Human-*in*-the-Loop Weapons: Robots that can select targets and deliver force only with a human command;

    b. Human-*on*-the-Loop Weapons: Robots that can select targets and deliver force under the oversight of a human operator who can override the robot's actions;

    c. Human-*out-of*-the-Loop Weapons: Robots that are capable of selecting targets and delivering force without any human input or interaction;

    d. Further reminds member states to further peace building practices to encourage the limiting the use of Human-*out-of*-the-Loop Weapons;

    e. Clearly defining this termonolgy would help facilitiate communication amongst the wider international community in order to formulate restrictions or approaches to the extent of use of technology;

3. *Expresses* its hope that member states will maintain human control over all weapon systems as opposed to artificial intelligence control, in a way that is more comprehensive and that will simplify the process of predicting or regulating the evolution of the rapidly moving fields of technology, robotics and artificial intelligence, therefore addressing the topics of:

    a. Keeping in mind international humanitarian law and the goals it aims to accomplish in regards to lethal autonomous weapon systems;

    b. Focusing the need for meaningful human control when developing and utilizing weaponry in order while acknowledging that absence of human involvement on extinguishing human life is an indignity to humanity;

4. *Strongly urges* the international community to ensure, through communication and collaboration with NGOs such as the Syrian Observatoy for Human Rights, who monitor the actions of belligerents in specific conflicts, that lethal autonomous weapons systems are not to be used in contravention to international humanitarian law which entails that:

    a. There must be clear lines of accountability and protocols that focus on the accountability of the potential misuse or malfunction since human control will not be present;

    b. These weapons must be programmed to ensure that non-combatants will not be targeted;

5. *Recommends* that member nations undertake a commitment to maintaining a human element in the deployment of LAWS, which is key in preventing civilian casualties, thus the regional bloc authorities may bear that in mind to the benefit of the international community;

6. *Stresses* that accountability is a pertinent factor in the maintenance of the sovereignty of a nation within its own borders as stated in the UN Charter, and encourages the establishment of authorities within regional blocs to ensure that in the case of any inappropriate LAWS implementation there is an opportunity for review and cooperation by the international community;

7. *Encourages* Member States to utilize autonomous or remote vehicles and weapons systems and technologies in a non-lethal capacity, including, but not limited to:

    a. Reconnaissance vehicles and unmanned aerial vehicles;

    b. Missile defense systems, such as the Iron Dome system in Israel;

    c. Utilizing, as an example, Global Positioning System technologies, be able to create region-specific information sharing to prevent higher risks, such as an awareness of the movement of dangerous groups;

8. *Endorses* the creation of an annual report to be given to Member States from the Group of Governmental Experts (GGEs), to discuss the role of Autonomous Weapons Systems in modern warfare and analyze the dehumanizing effect it has on all parties present in combat zones;

9. *Asks* member states to share nonclassified technology, both in the realms of general military technology (particularly aircraft and vessels) and Internet and cyber technology, in order to facilitate increased capacity for rapid response and the promotion of global security without asking nations to give more than their respective security advisors recommend;

10. *Appeals* member-states to implement a strategic goods lists to monitor the development of weapons and military goods based on the approval of government policies to export certain firearms and ammunition that focuses on but is not limited to:

    a. Equipment, ammunition and explosives for overseas activities in the course of which it may either be consumed, written off, or disposed of;

    b. Stores, equipment, ammunition and explosives of a Visiting Force;

    c. Equipments for repair, servicing or upgrade, and subsequent return to member-states (e.g. ships, vehicles, aircraft, weapons, electronic equipment and their parts);

    d. The adoption of an international framework to monitor the import and export of Lethal Autonomous Weapons based on agreement of the international community;

11. *Further recommends* the Campaign to Stop Killer Robots and the International Committee for Robot Arms Control in addressing the topic LAWS and educating the public about the possible threats in regards to Human Rights Law and International Humanitarian Law;

12. *Further stresses* the consideration of the outer space arms race, specifically that the use or proliferation of weaponry or conflict in outer space should be a matter of international concern.

Code: GA1/1/2
Committee: General Assembly, First Committee
Topic: The Implication of Technology on Global Security

The General Assembly First Committee,

Noting the threat that is posed by violent non-state actors through use of the internet as a tool, namely the use of social media to spread propaganda, recruit new members, finance their activities, train members, and to plan out attacks as stated in the United Nations Office on Drugs Crime Publication *The Use of The Internet For Terrorist Purposes,*

Reaffirming General Assembly resolution 43/77 *Review of the implementation of the recommendations and decisions adopted by the General Assembly at its fifteenth special session* in which the Secretary-General was requested to monitor future scientific and technological developments with potential military applications, which is directly applicable to the technological developments today through the use of the internet,

Recognizing risks posed by lack of adequate legal instruments as noted by the *Counter-Terrorism Implementation Task Force Publication Countering the Use of the Internet for Terrorist Purposes- Legal and Technical Aspects*,

Emphasizing the need of multilateral cooperation in conjunction with domestic effort in combatting cybercrime,

Keeping in mind that national sovereignty must be respected,

Emphasizing that one of the solutions for the strengthening of cybersecurity is rooted in the private enterprises as these private sectors manufacture technological products, employ personnel, and involve different stakeholders with the skills and capacities,

Recognizing the need for collaboration between private and public institutions to effectively implement technological advancements,

Alarmed by the minimal use of centralized bodies under the United Nations that feature a holistic information hub that promotes cyber-capability along with the prevention of cyber-threats,

Recalling International Atomic Energy Agency (IAEA) *Code of Conduct on the Safety and Security of Radioactive Sources, and supplementary Guidance on the Import and Export of Radioactive Sources*,

Noting the *Convention on the Physical Protection of Nuclear Material*, an international agreement on the hindrance and punishment of the offenses pertaining to nuclear material,

Noting further, the IAEA General Conference resolution GC(49)/RES/9 *Measures to Strengthen International Cooperation in Nuclear, Radiation and Transport Safety and Waste Management*,

Basing itself on the call of the United Nations to advocate for the global community especially in incidents affecting international security,

Gravely concerned with the threat of the proliferation of weapons technology to violent non-state actors,

Believing it is the responsibility of the global community to support those Member States with limited access to defense mechanisms,

Noting also the importance of presenting a united global front against these violent non-state actors,

1. *Strongly declares* the need of a unified definition of cybercrime offenses and their risks, denoting specific levels of intensity for offenses ranging from nuclear proliferation to public private data invasion:

a. For all intents and purposes, cybercrime shall be defined as any distribution of Malware, Ghostware, or Blastware or attacking of a network on the part of any state, non-governmental organization, or individual;

b. A cyber security concern will be identified as any alleged involvement, past or present, in a cybercrime as defined above;

2. *Adopts* a unified definition for which actors are encompassed under the term violent non-state actor:

a. For all intents and purposes, the term "violent non-state actors" will refer to any individual or group of individuals acting independent of the will and outside the laws of their home state in order to inflict terror, injury, or fatality against foreign governments or civilian populations;

3. *Calls* for Member States to employ a domestic comprehensive legal foundation for prosecuting the actions of violent non-state actors in regards to cybercrimes as previously defined:

a. Encourages Member States to implement frameworks grounded in regional processes and legislation which would address cohesive means for prosecuting violent non-state actors, such as those utilized in the European Union framework decision 2002/475/JHA and amendment decision 2008/919/JHA which call for the alignment of legislation and the introduction of minimum penalties regarding terrorist offences;

b. Further encourages a harmonization of these suggested domestic regulative frameworks in terms of detection, prevention, and punishment to reach global cyber synergy through efficient and supportive multilateral cooperation;

4. *Endorses* the implementation of regulations on the disposal of nuclear waste in order to curb the use of potentially dangerous waste materials in dirty bombs or the potential cyber-attack on nuclear power facilities:

a. Calls on Member States currently utilizing nuclear energy to utilize a centrally-devised policy from the *International Atomic Energy Agency Nuclear Fuel Cycle Waste Technology* to ensure proper disposal of nuclear waste;

b. Advocates for nuclear energy facilities to implement resilient cyber-security measures to ensure protection against potential cyberattacks;

c. Encourages re-evaluation of advancements in nuclear technology every five years to ensure security and waste management protocols are cohesive with emerging technologies as outlined in the *Treaty of Non-Proliferation of Weapons*;

5. *Invites* Member States to establish efficient reporting and response procedures to cybercrime in accordance with the International Telecommunications Union (ITU):

a. Urges Member States to join the ITU and to further incorporate systems sponsored by the *Dakar Declaration on Cyber Security*, such as Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Systems (CSIRTs)for individual, governmental, and industrial use of cyberspace;

b. Encourages Member States to establish and maintain National Vulnerability Disclosure Reports; these would file shortcomings uncovered by researchers, ethical hackers, and individual agents in all sectors of technology in order to gain data on cybercrime and create stronger firewalls for future use, such as those employed by the Global Forum on Cyber Expertise (GFCE);

6. *Recommends* that Member States utilize regional organizations such as the European Union (EU), Association of Southeast Asian Nations (ASEAN), League of Arab States (LAS), and the African Union (AU) to begin

categorizing emerging technologies such as lasers, intercontinental ballistic missiles (ICBMS), automated weapons systems, advanced satellites, and communications systems:

a. This optional categorization process would encompass the maintenance of a database detailing which Member States possess emerging technologies including the nature and quantity of their armaments;

b. Jurisdiction of the database would lie with the regional organization a given Member State chooses to affiliate with; access to the database will be provided at the discretion of said regional organization;

c. The production, testing, and use of those weapons categorized as chemical or biological weapons will be prohibited in accordance with the *Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on their Destruction of 1997*;

7. *Appeals* to private companies and institutions to consider extending opportunities to students and potential employees from underdeveloped nations in order to train candidates in the field of cyber security in order to advance global technical awareness:

a. Suggests the allotment of additional funds, provided by Japan, to Oversees Development Assistance (ODA) which supports programs in underdeveloped nations;

b. The funds of the ODA will be used to support the expansion of training facilities in regards to cyber security;

c. Invite private institutions to provide opportunities for further employment and training both for graduates of these programs and those unable to access them by other means;

8. *Fully supports* a reduction in national arms production in accordance with international standard:

a. Recommending policies calling for a 10% reduction in the production of new war technologies (including but not limited to artillery, rocket and missile systems, including intercontinental ballistic missiles (ICBMS), and automated weapons systems) each year following a review by United Nations Office of Disarmament Affairs at the end of the first period of five years to assess effectiveness and compliance.

Code: GA1/1/3
Committee: General Assembly First Committee
Topic: The Implication of Technology on Global Security

The General Assembly First Committee,

Acknowledging Chapter 1, Article 1 of the *United Nations Charter* that includes the mission to maintain international peace and security, and Article 10 which authorizes the General Assembly to make recommendations to Member States of the United Nations, in particular the Security Council,

Affirming Sustainable Development Goal 16 that calls for the development of effective, accountable and transparent institutions at all levels,

Recognizing the importance of building trust, increasing confidence and promoting transparency among Member States in ensuring security and stability in the international community,

Recognizes the strengths of the *African Union Convention on Cyber Security and Personal Data* in helping close the technological gap that exists between developed and developing States,

Acknowledges the strengths of creating a greater legal cooperation between Member States and stronger conventional institutions to fight cybercrime, such as the accomplishments of the African Union Convention on Cyber Security,

Recalling General Assembly report 45/4568 to establish sanctions which monitor the advancement and implementations of increasing technological leaps, and its prospective applications within militaries, thereby allaying the potential for all types of cybercrime,

Considering General Assembly resolution 51/39 *The Role of Science and Technology in the Context of International Security and Disarmament,* which emphasizes the role of international guidelines for the technology transfer of military weapons and their impacts on international peace and security,

Fully aware of the *Geneva Declaration for Cyberspace* which aspires to develop common legal norms and standards in a global framework for cybersecurity and cybercrime, seeks to prevent future through cooperation among all nations,

Recalling the 2011 *Vienna Document on Military Transparency*, which aims to enhance transparency in military activities through a voluntary annual exchange of military information, through the creation of annual calendars and the sharing of specific data relating to major weapons systems,

Being fully aware of the efforts of the International Telecommunication Union (ITU) Computer Incident Response Team (CIRT) Programme for improving the Member States' competency in relation to cyber security and enhancing their national computer response or incident teams,

Expressing its appreciation to Asia Pacific Computer Emergency Response Team (APCERT) in cooperatively mitigating cyber threats with leading CIRTs on a regional scale,

Drawing attention to General Assembly resolution 69/28 *Development in the field of information and telecommunications in the context of international security*, which calls upon member states to increase transparency through multilateral cooperation,

Realizing that the sharing of technological knowledge between developing and developed countries requires accountability measures to assure expansive and efficient progress,

Acknowledging the potential benefits of public-private partnerships within and outside of the UN system, as the private sector owns and operates a significant amount of information infrastructures, which Member States depend on in order to access resources such as Information and Communication Technologies (ICTs),

Noting with deep concern the rise of cyber terrorism by both state and non-state actors, including those that interrupt access to technological infrastructure,

Recalling the recommendations of the 19th *Conference on Telecommunications and Security* in 2015 and *European Cyber Security Forum* that urge collaborative international exercises in the field of cyber security to allow a the better understanding of potential threats to sovereignty and prompt further research into anti-malware technology to defend against cyberattacks,

Concerning the lack of regulation of cybersecurity in the *Laws of Armed Conflict*, and the past role that previous Geneva Conventions and the regulation of armed conflict played, cybersecurity must be incorporated into international law of armed conflict, so that there can be a present role set regarding the repercussions one might face if conducting an illegal form of cyber offence towards another body,

Emphasizing the benefits of global partnerships stressed in *Transforming our world: the 2030 Agenda for Sustainable Development* (A/RES/70/1) with the need to pursue collaboration with the private sector, considering that the world's leading technology firms own or have access to the information infrastructures necessary for Member States' security development,

Understanding that the development of technical standards is a different matter for both developing and developed nations,

1. *Recommends* further active participation on the 2011 *Vienna Document on Military Transparency*, such as collaborating upon a voluntary annual exchange of best practices for managing data relating to major weapons systems;

2. *Urges* Member States to collaborate upon and uphold collaborative agreements from regional bodies such as the *African Union Convention on Cyber Security and Personal Data Protection,* and adopt their legal policy frameworks which simplify cooperation among the international community and increase security among participating Member States with regard to personal data security as well as definitions;

3. *R*ecommends the implementation of regionally tailored principles for conduct such as the Code of Conduct set forth from the *African Union Convention on Cyber Security and Personal Data Protection*, a set of rules formulated by the processing official with a view to establish the correct use of computer resources, networks, and the electronic communication of the structure concerned, and approved by the protection authority;

4. *Encourages* the creation of an international framework based on the international collaborative group of leading funders known as *The Transparency and Accountability Initiative* to introduce transparency of technological usage through the development of standards for internet security architecture including but not limited to working with governments, foundations, NGOs, researchers and other practitioners to galvanize support for ambitious new ideas in the field to moderate the sharing of technology;

5. *Recommends* the Security Council create an international database of information sharing techniques and best-practice sharing monitored by the Group of Governmental Experts (GGE) to allow Member States to more fully understand the scope of technology transfers occurring throughout the international community;

6. *Encourages* Member States to embrace the review process and act upon recommendations made by the GGE based on information collected in the international database, as they lie within the limits of national sovereignty;

7. *Calls upon* Member States to participate in developing the framework for GGE monitoring the usage of the database, in hopes of preventing corruption and misuse;

8. *Recommends* that, in the spirit of sovereignty of each Member State and regional body, the Security Council engage all stakeholders in full cooperation to create a central agency devoted to cybersecurity that has monitoring and enforcement powers with the full cooperation of Interpol and cooperating member states;

9. *Further requests* that the Security Council develop a comprehensive definition of both cyber terrorism and cyber warfare;

10. *Invites* all Member States to partake in an international effort to work alongside the private sector to create better ICT and cyber infrastructure safety practices;

11. *Urges* the standards of identity proofing and multi-factor identification methods be transmitted through partnerships with the private sector;

12. *Seeks* to protect the personal information of civilians as well as build capacity for governments to protect itself from corruption;

13. *Encourages* Member States to pursue additional confidence building measures to bridge the gap between developed and developing countries, such as continuing public and private collaboration;

14. *Continuing* public and private collaboration as the private sector owns and operates a significant amount of information infrastructures, which Member States depend on in order to access resources such as Information and Communication Technologies (ICTs);

15. *Invites* all Member States to partake in an international effort to work alongside the private sector to create better safety practices;

16. *Urges* the standards of identity proofing and multi-factor identification methods be transmitted through public-private partnerships;

17. *Encourages* Member States to further cooperate with each other in addressing cyberattacks:

    a. Developing a common standard internationally for cooperation of cybercrime and security;
    b. Further developing of international cybersecurity, law and greater prosecution of rogue hackers;
    c. Providing greater judicial aid to nation states and international organizations with the purpose of prosecution of those individuals through the ICC and other regional international courts;

18. *Recommends* the regulation of cybersecurity through the Geneva Convention *The International Laws of Armed Conflict:*

    a. The developing of the regulations of cyberwarfare through Geneva and the establishment of a treaty;
    b. Establishing that an act of cyberattack can be considered an act of war under the Laws of Armed Conflict;
    c. Empower the United Nation Security Council (UNSC) in regulating and sanctioning Nation States that violate the Laws of Armed Conflict;

19. *Reiterates* the call upon states for the practice of an authoritarian supervision over the utilization of developing technologies:

    a. Developed nations with an advanced cyber framework would help the technological infrastructure of other developing states,
    b. An augmentation of emphasis concerning the exponential growth of new computing technologies such as quantum structures within encryption systems and artificial intelligence and its implications.

Code: GA1/R/1/4
Committee: General Assembly First Committee
Topic: The Implication of Technology on Global Security

The General Assembly First Committee,

Reaffirming role of science and technology in the context of international security and disarmament which recognizes the technological gap between developed and developing Member States,

Reiterating outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society by focusing on Member States' need for existing legal and enforcement frameworks to further improve the transparent application and speed of technological change,

Emphasizing the need of North-South cooperation between developing and developed countries in regards to spreading the accessibility of security systems for cyber defense,

Concerned about the lack of education in information and communications technology (ICTs) training in primary and secondary education schools in developing nations and the vulnerability of potential cyber-attacks within each Member State,

Cognizant of the importance of defending the critical sectors of a Member State's digital infrastructure from cyberattacks,

Emphasizing the criticality of cyber security information dissemination between private and state actors within cyberspace by a central cyber security information entity that stresses on the importance of appropriate and sufficient ICT and telecommunication solutions,

Bearing in mind the important of science, technology and innovation for development which emphasizes multiple aspects of Member States' development,

Recognizing that the United Nations International Telecommunication Union - International Multilateral Partnership Against Cyber Threats (ITU-IMPACT) currently has programs, like Computer Emergency Response Teams (CERTs) and Computer Security Incident Response systems (CIRTs), in place which address the sharing of technology, early response systems, and education on cyber-security,

Noting with deep concern the need to emphasize the cooperative and dedicated effort from the governmental and industrial sectors in a Member State for fulfilling security objectives,

Recognizing the ability of Member States to cooperate in the betterment of individual cyber security systems in the interest of creating a truly global approach to global security while ensuring that national sovereignty in noting infringed upon,

Emphasizing the need to bridge the gap of technological vulnerabilities of Member States in terms of detecting and combatting cybercrime,

Bearing in mind a Member States' low level of security capabilities to detect and respond to cybercrime and information risks among developing nations,

1. *Encourages* Member States to model the ITU-IMPACT cyber-security and telecommunications technology transfer program to:

a. create research and development programs that are inclusive of Member States of different technological capabilities in order to hold developed and developing nations accountable in the sharing of pertinent technological information;

b. encourage all Member States to actively participate in the sharing of ICT and other relevant technologies with the goal of the betterment of global security;

2. *Endorsing* Member States sharing of information about their technological advancements in a global database to encourage transparency and to bridge the gap through:

a. a. investing in regional and international innovative abilities, such as the 2006 European Innovation Scoreboard (EIS), to expand the capability of closing the technology gap by working with international organizations, nongovernmental organizations (NGOs), and UN agencies;

b. b. suggesting an implementation of a data base collection on the international community;

c. c. international research and development and joint cyber security exercises to diversify the inclusion of all Member States;

d. d. international research and development and joint cyber security exercises to diversify the inclusion of all Member States;

3. *Drawing attention* to the usage of technology to promote peace, development, and closing the digital divide through education by:

a. requesting funding from institutions like the World Bank and Norfund to expand comprehensive programs, such as Peace Hacking Camps to educate the population on internet usage and social media to empower youth and women entrepreneurship;

b. emphasizes the importance of curriculums, such as South Sudan's Ministry of Education, Science and Technology, for promotion of technological literacy to enhance the youth's understanding of global security;

c. encourage organizations, such as NATO-Morocco and other developed nations to further enhance and guide training for developing countries on education of new technology;

4. *Invites* the International Development Research Centre (IDRC) to provide ICT initiatives education programs for primary and secondary education schools and Member States' populations by:

a. proposing a prevention strategy, such as Angola's CENAPATI academic and excellence center, to educate students about the importance and risks of cyber-attacks;

b. requesting funds from the International Monetary Fund (IMF) to implement technological education that focuses on ICTs;

c. focusing on joint partnerships, such as the United Nations Children's Fund (UNICEF) supported Quality Primary Education Project which incorporates the ideas of a broad education system that could be implemented within the international community;

5. *Recommends* the establishment of a Cyber Security Center within Member States tasked with:

a. distributing an annual report on cyber security information and knowledge generated and shared between public and private actors to strengthen collective interstate cyber security;

b. developing continuous information security arrangements;

c. requesting consenting Member States to contribute appropriate funds this initiative in accordance with their respective Defense Ministry budgets;

d. recommends the establishment of state-by-state panels comprised of technological experts to head the subunits of the Cyber Security Center.

6. *Encourages* the utilization of cyber-safety security frameworks that will impede non-state actors from soliciting illicit weaponry in cyberspace through the expansion of the framework of the National Information Security and Safety Authority (NISSA), which will;

a. expand NISSA operating models, strategies, and standards for specific guidelines regarding cyber safe networks;

b. mitigate potential errors in practice and increase efficiency by conducting and circulating periodic regional reports;

c. develop partnerships with appropriate agencies, such as the United Nations Office for Disarmament (UNODA) to enhance efforts for cyber security as it relates to disarmament

d. expand on NISSA's "Kareen Initiative", which aims to guide youths on their career paths in information security fields by encouraging mentorship and steering graduation projects to aid in their development of skills required for desirable employment opportunities in the future;

7. *Suggests* Member States to adhere to Norway's *Varsling system for Digital Infrastructure* a national early response system that immediately informs critical sectors, such as nuclear power plants and financial institutions, once the system detects a cybercrime activity in the country though:

a. encouraging the enhancement of cyber security among Member States by enabling these sectors to begin their countermeasures proactively and punctually;

b. data collected from the system should be compiled in a national database where the United Nations and relevant international agencies may access information more effectively and efficiently;

8. *Expresses its hope* for Member States to establish efficient response systems sponsored by the International Telecommunications Union (ITU) for individual, governmental, and industrial use of cyberspace:

a. encourages stakeholders to submit their cyber conflicts to response systems allowing these systems to detect and learn from the various forms of cybercrime, further creating capability to efficiently respond to threats imposed by cybercrime;

b. creating the capability to efficiently respond to threats imposed by cybercrime;

9. *Recommends* the creation of a program by the name of Deterrence of Ominous Threats on Countries Open to Maltreatment (DOTCOM) to assist developing states for the protection of their cyberspace which will include but is not limited to:

a. Virtual peacekeeping operation requested by any Member State who is under cyberattack and cannot defend itself adequately;

b. Volunteer cybersecurity task force comprised of Member States with a head director chosen annually by a majority vote of the General Assembly who oversees recruiting the task force and overseeing the tailored cybersecurity systems to the Member State in danger:

i. Short-term use cybersecurity system until the DOTCOM program deems Member States protected

ii. Placement of DOTCOM headquarters at the United Nations headquarters, staffed by volunteer delegates of Member States;

iii. Requests that consenting Member States contribute appropriate funds toward the Commission on Science and Technology for Development (CSTD) requested by Economic and Social Council (ECOSOC) for DOTCOM technology and facilities;

10. *Calling* for the establishment of national vulnerability disclosure reports based off the initiative of the Global Forum on Cyber Expertise, where an expert researcher or ethical hacker discovers vulnerabilities in all sectors of technology and notifies back to the government;

11. *Promotes* the establishment of national data deposit laws, which would serve as a platform for national and international researchers to deposit their input on the tools and techniques used to identify and collect information on cybercrime activities:

    a. Denoting the inclusion of data provided by a Member States' respective national vulnerability disclosure reports and response systems to further embellish the data platform;

    b. Recognizing that this would be done on a voluntary basis as to not infringe on Member States' sovereignty;

12. *Suggests* Member States enhance their cyber security understanding by participating in simulations regarding this topic;

    a. Member States are encouraged to attend the biannual International Cyber Security Summit (ICSS), mimicking a cross-border cyber drill simulated by the ITU-IMPACT in 2011 in Southeast Asia, in which they would simulate a localized cyber-attack to formulate a response strategy for potential cyber security incidents;

    b. Encourage funding from the ITF because these simulations would promote the awareness, utilization, and effectiveness of digital infrastructure;

    c. Recommends that the ICSS consider inviting specialists on data security and cyber terrorism as well as inviting NGOs that specialize in these areas as well;

13. *Recommends* the use of technological agencies, such as the Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials (ABACC) as a framework for regional agencies to be established to regulate cyber technology transparency:

    a. urging the ITF to financially support the efforts of non-governmental and intergovernmental agencies that focus on ensuring the integrity of the storing technology infrastructure;

    b. further suggesting the openness and transparency of these agencies regarding cyber technology advancement;

14. *Expresses its hope* that Member States will engage in bilateral, trilateral, and multilateral agreements to uphold and protect the integrity of transparency, ensure the safety of important technology infrastructure, and create an avenue for technological safety which can be applied globally:

    a. further investigating and researching autonomous weapons systems through the United Nations Office for Disarmament Affairs (UNODA);

    b. monitoring the development and testing of weapons systems through voluntary and consistent participation in the United Nations Register of Conventional Arms by Member States.

Code: GA1/1/5
Committee: General Assembly First
Topic: The Implication of Technology on Global Security

The General Assembly First Committee,

Taking into account, the First Committee of the General Assembly's mandate to focus on security and disarmament, in context of implications of technology on global security,

Reaffirming the Sustainable Development Goals (SDGs) number 17 in strengthening the means of implementation and revitalize the partnership for global development especially clause 6; means of promoting capacity for information and communications technologies and information sharing, to ensure a safe path to development,

Recognizing General Assembly resolution *GA/RES/6624*, Developments in the Fields of information and telecommunications in the context of international security,

Recalling Security Council resolution 2117 SC on transfer of small arms and light weapons, such as operative clause 7 to encourage information sharing amongst member states to prevent illicit weapons trade,

Affirming the UN resolution, *A/RES/2171* referring to the sharing of information of terrorism of all forms, operative clause 1 in expressing determination to peruse the object prevention of armed conflict,

Taking note of the 2011 global cyber security strategies and global development event, in which member states helped address global cyber security issues through the UN Economic and Social Council (ECOSOC) and recognized that the realm of cyber security is becoming broader with advancement in technology,

Recognizing Security Council resolution 2195 (2014) in urging international actions to break links between terrorists, transnational organized crime, and noting that the disruption of routes of transit can not only put human lives in danger but also disrupt the global economy, such as the current disruptions of safe flow of people and goods respect of international borders by the Islamic State in Iraq and Syria (ISIS),

Supporting the work of the International Telecommunications Union (ITU), in their mission to connect the global community through means of the Internet, multimedia, telecommunications and international trade networks and services,

Noting General Assembly, *A/RES/64/422* on creating a global culture of cyber security and taking stock of national efforts to protect critical information infrastructure,

Supporting General Assembly, *A/RES/2309* in building more extensive collaboration of global technology and infrastructure between all member states able to do so, in order to ensure safe routes of transit,

Reminds the body that the Implication of Technology on Global Security falls under the First Committee of the General Assembly's mandate; and is therefore imperative to have universal commitment and transparency to this mandate in order to address this topic,

1. *Asks* member states for commitment towards clause 6 of SDG 17 and the worlds ability of meeting this goal by 2030; in context of capacity building for information and communications technologies, to improve global defense capability;

2. *Supports* transparent information sharing amongst Member States with regards to using advancements in malware preventing and cyber monitoring technology, with the goal of ensuring the safe routes of passage for people and goods, including legal weapons trades between Member States, such as the United States Comprehensive National Cyber security Initiative as a model for member states;

3. *Urges* every sovereign Member State through transparent communication and the continual advancement and implementation of monitoring and tracking technologies, to domestically keep track of weapons:

    a. Emphasizing, domestic frameworks, thus ensuring each member state has the capacity to keep pace with advancements in and eradication of illicit weapons trade and other advancing technologies that can pose a threat to peoples' livelihoods;

4. *Promotes* the development of anti-malware technology in a framework to monitor and secure; with executable code to defend against computer viruses, worms, trojan horses, spyware and other harmful programs towards technologies that would assist member states monitor safe routes of transit from hackers or cyber terrorists;

5. *Encourages* collaboration between all Member States, with regards to sharing of information and cyber security methods, for the purpose of creating global transparency through information sharing with all other Member States, as well as adoption of a domestic framework, working in cohesion with the proposed international framework which will assist all states to achieve the goal of eliminating the risk of cyber threats;

6. *Suggests* the creation of a framework to modernize monitoring of international routes of transit for people and goods through advanced technological tracking methods, such as sensors and radars, looking out for illicit activities such as untracked weapons trading or advanced technologies that could hinder global security in the context of safe transit and border security such as, illicit weapons trade, malware and cyber attacks:

    a. Making note that the above-mentioned areas of security be addressed through transparent information sharing, with regards to international routes of transit, amongst all member states, using the European Union weapons tracking initiative ITRACE as a global model for transparent communication amongst member states;

    b. Recommends states implement and continue to advance anti-malware technologies to better combat the increasing cyber security threats that affect all Member States in the ability to monitor international routes of transit;

    c. Urging states with the capacity to develop these monitoring technologies to collaborate with developing states, with regards to the development of surveillance technologies and methods to increase overall global security;

7. *Suggests* using the ITU as a global catalyst for Member States to facilitate information with regards to technological security to maintain and develop a modern level of monitoring international transit routes to protect transportation methods of people and good from cyber attacks and illicit weapons;

8. *Calling for* member states to continue to collaborate on these measures of security development, acknowledging the constantly evolving technological environment, which is constantly posing new threats to global security.