LAGOS MODEL UNITED NATIONS (LMUN) 2020

21-25 September 2020

Documentation of the Work of the United Nations Security Council

Committee Supervised by:

Olufolajimi Otitoola (Deputy Secretary-General)
Ima-Abasi Emmanuel Ubong-Abasi (Under-Secretary-General Research)
Adedokun Titilope Ayo (Under-Secretary-General for Peace, Security and Human Rights)

United Nations Security Council (SC)

Committee Staff

Chair	Chikamso Ononuju
Vice-Chair	Abisola Tiwalade Fayinka
Researcher	Ayomide Sofekun
Researcher	Oluwalani Keshinro

Agenda

I. Cyberespionage and Cyberterrorism in the 21st century
II. Women in International Peace and Security

Resolutions Adopted by the Committee

Code	Topic	Vote
SC 1/1	Cyberespionage and Cyberterrorism in the 21st Century	Adopted by Acclamation
SC 1/2	Cyberespionage and Cyberterrorism in the 21st Century	Adopted by Acclamation

Summary Report

The United Nations Security Council held its annual session to consider the following agenda items:

I. Cyberespionage and Cyberterrorism in the 21st Century
II. Women in International Peace and Security

The session was attended by representatives of 15 Member States of the Security Council. On Monday, the committee adopted the agenda of I and II, beginning discussion on the topic of "Cyberespionage and Cyberterrorism in the 21st Century."

By the end of the first day, delegates already formed blocs and sent in the first draft of their working papers which covered a wide range of subtopics such as capacity building, cybersecurity education, public-private partnerships and the use of mainstream media to create awareness on cyberterrorism. By Tuesday, the delegates were adding more creative ideas and working together to create more innovative ways to solve the problem of cyberespionage.

On Wednesday, the working papers were sent back to the delegates after a thorough review had been done by the dais and corrections were made in the document. The delegates accepted the changes and inputted more solutions. By Thursday, the document was sent to the Under-Secretary Generals and Deputy Secretary-General for vetting. The committee adopted two draft resolutions which both received unanimous support by the entire committee. The resolutions covered the need to strengthen cooperation and capacity building amongst Member States and encouraging cybersecurity education, public participation and partnerships. The overall work of the committee throughout the conference was collaborative and the delegates exhibited great diplomacy skills to build consensus and renew the conversation about cyberespionage and cybersecurity.

Code: SC 1/1
Committee: Security Council
Topic: Cyberespionage and Cyberterrorism in the 21st Century

The United Nations Security Council,

Acknowledging the Security Council resolution 1373 (2001) which mandates countries to harmonize their national laws with the existing international framework on terrorism which will therefore serve as a way to combat terrorist groups and their activities,

Recalling the provisions of Security Council resolution 1189 (1998), 1269 (1999) and 1368 (2001) which urged Member States to come up with plans to combat terrorism in the future while frowning upon acts of terrorism in the past,

In line with the Sustainable Development Goal 16 which focuses on Peace, Justice and Strong Institutions,

Recognizing the efforts of the North Atlantic Treaty Organization (NATO) in developing cyber defence strategies in combating cyberterrorism and cyberespionage,

Commending the European Union (EU) for regulating activities on cyberspace in a bid to prevent and manage cyberattacks,

Strongly supporting the efforts of the G20 in combating cyberespionage and cyberterrorism by issuing a communique in 2017, affirming that existing international law applies to Member States' behaviour in cyberspace and Member States should abide by responsible State behaviour,

Recognizing the various efforts Member States have employed in combating cyberterrorism and cyberespionage such as enacting national policies, signing mutual agreements amongst others,

Highlighting the importance of the sensitization and training of Member States and also the challenges of funding for some Member States as regards the issue of cyberespionage, cyberterrorism and cybersecurity in a bid to reduce these attacks,

Deeply concerned about the negative impacts cyberespionage and cyberterrorism has on the national governments of Member States and citizens such as instilling fear in citizens and attacking critical government infrastructure amongst others,

Affirming the provisions of the *Convention on Cybercrime* (2001) and the *Additional Protocol to the Convention on Cybercrime* (2003) which criminalizes xenophobic acts committed with computer systems on cyberspace,

Realizing the need for the creation of awareness on the topics of cyberattacks, cyberespionage, cyberterrorism and cybersecurity measures,

Further realizing the need for partnerships between the international community, Member States and regional organizations,

Underscoring that Member States are obligated under *Article 25 of the United Nations Charter* (1945) to accept and carry out the decisions of the Security Council,

1. *Calls upon* Member States to set measures in place that create awareness for all levels with emphasis on local institutions and communities about the effects of cyberterrorism, how to prevent attacks and ensuring that safety measures are put in place in the events of attacks by:

    a. Creating awareness in tertiary institutions, especially to deter upcoming cyberattackers from engaging in such conducts by:

        i. Including cybersecurity as a vocational subject in higher institutions which students are required to pass;

        ii. Ensuring qualified cybersecurity experts are provided to take these classes;

        iii. Organizing practical classes for students interested in cybersecurity as this would enable them to get a better grasp of cybersecurity strategies;

    b. Organizing sensitization programs on the effects of cyberespionage and the importance of cybersecurity on all levels of education; vocational institutional inclusive by:

        i. The funding of these programs by Member States and ensuring qualified cybersecurity experts are made available to take these sensitization classes;

        i. Annual lectures on the national progress of cybersecurity in order to keep the citizens informed on the latest happenings on cyberwarfare issues;

        ii. Workshops for older citizens to teach them basic cybersecurity steps in order for them to protect their relevant information;

2. *Strongly suggests* that Member States should encourage the full participation of major stakeholders including affected private organizations in each State in the tackling of cyberterrorism and cyberespionage by:

    a. Organizing technological advancement programs for communities and sectors affected or involved, through setting up skill-intensive workshops with the Counter-Terrorism Committee, United Nations Office of Drugs and Crime (UNODC) or any other sub-unit of the United Nations (formed for this sole reason) where essential skills and knowledge required for developing cyberweapons are taught to members of the general public and personnel of the involved sectors;

    b. Organizing competitions for participants of these programs to develop cyberweapons indigenous to their sphere and community to act as an incentive for future advancement and boost participation;

3. *Decides* that Member States partner with private organizations and Civil Society Organizations with the same interest of combating cyberespionage and cyberterrorism in providing adequate cybersecurity measures in each country through:

a. Soliciting for the cooperation of private organizations and civil society organizations with a similar interest of strengthening cybersecurity by reaching out for partnerships to these organizations via public media houses;

b. Providing incentives such as giving out awards on national holidays to these private organizations and civil society organizations in order to encourage their activities in combating cyberterrorism and cyberespionage;

4. *Decides* that Member States should make concerted efforts through international cooperation and partnerships by:

a. Joining regional communities like the North Atlantic Treaty Organization (NATO), Association of Southeast Asian Nations (ASEAN) and the European Union (EU) in furtherance of regional cooperation and to foster partnerships for collaborative efforts in cyberterrorism and cyberespionage through:

i. The organization of bi-annual seminars on the topic of cyberterrorism and cyberespionage by these regional bodies;

ii. Ensuring Members of these regional organizations share experience and information on their national counter-cybercrime efforts, challenges faced and suggest best practices for combating cyberterrorism and cyberespionage;

b. Developing a policy or legal framework that aids participating Members of these regional organizations in developing their national cyberterrorism strategies with:

i. Effecting sanctions if these policies are not implemented by Member States;

ii. Setting in place mechanisms and machinery to ensure these sanctions are properly issued;

5. *Decides* that Member States partner with major media houses or organizations (government-owned and private-owned) within, to help enlighten citizens of each Member State in mitigating the effects of cyberespionage and cyberterrorism and also prevent future attacks through:

a. Consistent announcements by such media houses of the effects of cyberespionage and cyberterrorism and how citizens can protect their devices and personal information;

b. By announcing the penalties and sanctions attached to conducts resembling cyberespionage and cyberterrorism as this would serve as a deterrence to citizens about to engage in terrorist propaganda on cyberspace;

c. Through sponsoring notable media personalities as the faces of campaigns against cyberterrorism and cyberespionage in such State, as popular media personalities have been seen to positively affect the behaviour of citizens.

Code: SC 1/2
Committee: Security Council
Topic: Cyberespionage and Cyberterrorism in the 21st Century

The United Nations Security Council,

Reaffirming its respect for the sovereignty, territorial integrity and political independence of all States per the *United Nations Charter* (1945), on the fight against terrorism, as deeply concerned by the increase in acts of terrorism,

Recalling the Security Council resolution 2370 (2017) which urges Member States to act cooperatively to prevent terrorists from acquiring weapons, including through information and communications technologies, while respecting human rights and fundamental freedoms and in compliance with obligations under international law,

Recognizing the *Arab League's Convention on Combating Information Technology Offences (2010)* whose primary aim is to strengthen cooperation between States to enable them to defend and protect their property, people and interests from cybercrime and cyberterrorism,

Approving the adoption of the *African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa* (Draft African Union Convention) 2012 which promotes the provision and maintenance of human, financial and technical resources needed to facilitate cybercrime investigation,

Aware of the *African Union Convention on Cybersecurity and Personal Data Protection* (2014) which includes a call to the African Union States to create and/or amend national laws to adequately combat cybercrime, harmonize national laws, create mutual legal assistance treaties,

Deeply concerned about the incitement of terrorist acts motivated by extremism and intolerance which consequently poses a serious and growing danger to the enjoyment of human rights, threatens the social and economic development of all States and undermines global stability and prosperity,

Emphasizing the need to take all necessary and appropriate measures in accordance with international law at the national and international level to protect the right to life which was and still, is of utmost importance,

Commends Member States for their cooperation with the Counter-Terrorism Committee,

Appraising the progress made so far by the Counter-Terrorism Committee established by the Security Council under paragraph 6 of resolution 1373 (2001) acting under Chapter VII of the *United Nations Charter* (1945) in discharging its important responsibility to monitor the implementation of that resolution,

Recalling the Security Council resolution 2370 (2017) which recommends collaborative efforts of Member States with respective private sectors in the fight against cyber threats,

Noting with appreciation the progress made in efforts undertaken by the European Union (EU) in developing cyber-defence strategies in strengthening cyber resilience, by adopting EU Regulation 2016/679 on the protection of data (GDPR) and Directive (EU) 2016/1146 on the security of network and information systems that takes into account competition demands and digital technology,

Recognizing the regulations and other actions adopted by the EU towards protecting citizens, companies and Member States' right to privacy, personal data protection, protection of critical infrastructure and fight against online terrorist content,

Recognizing explicit attempts to secure the cyberspace from transnational subversion of national security,

Noting further the urgency of specialized training on malware analysis and digital forensics and the conduction of periodic research seminars,

Emphasizing the importance of strengthening international peace and security by reducing and eliminating the causes of mistrust, fear, misunderstanding, and miscalculations that States have about the military activities of other states,

Deeply concerned about the rising number of cyberattacks against States in recent years, with the potential of harming economic growth, political growth and military growth,

Fully alarmed by the high percentage of Member States without a cybersecurity strategy, being 13% without any cybercrime legislation, 2% without data and 5% with draft legislation,

Affirming that the adoption by all Member States of appropriate legislation against the misuse of Information and Communication Technologies for criminal purposes, including activities intended to affect the integrity of national critical infrastructure of States is central to achieving global cybersecurity,

Deeply conscious of the importance of the harmonization of legal frameworks by all Member States to combat cybercrime and facilitate international cooperation,

Appraising the efforts of the International Telecommunication Union in creating the 'Best Practice in Policy/ Legal Enabling Framework and Capacity Building in Combating Cybercrime' which elaborates strategies for the development of cybercrime legislation that is globally applicable and inter-operable with existing national and regional legislative measures by providing a model for Member States,

Reaffirming Goal 16 of the Sustainable Development Goals (SDGs) which promotes peaceful and inclusive societies for sustainable development and justice for all,

1. *Proposes* the development and implementation of Cyber Confidence Building Measures (CBMs) in bilateral, multilateral and regional security revenues by:

    a. Commencing with symbolic measures, with which the CBMs may be progressively implemented in evolutionary stages of increasing significance;

    b. Ensuring that the intent and modalities of a CBM are obvious, open and unambiguous to leave no room for misinterpretation of its purposes;

    c. Verifying (possibly third parties) to reduce fear and mistrust particularly in cases where reciprocity is expected;

    d. Provision of appropriate communication channels to provide for direct dialogue as a means to clarify potential misunderstandings, misperceptions or mistakes;

2. *Strongly recommends* the creation of a commission, specifically for cyber defence and capacity-building in the international cyberspace, financed by Member States according to their financial capacity which would:

    a. Ensure Member States establish a single central body for cybersecurity at the national level that will be responsible for monitoring cyber incidents; review compliance with relevant cyber laws, detect threats and anticipate attacks from cyberterrorists and criminals by the:

        i. Creation of neutral bodies that solely counter cyberattack and protect national cybersecurity;

        ii. Creation of a Computer Emergency Response Team for crises;

        iii. Creation of a defined framework to protect critical infrastructure in the cyberspace;

        iv. Provisions in new legislation for sanctions to defaulting persons, organizations or groups funding or involved in cyberattack as a means of deterrence;

    b. Ensure Member States are transparent especially as regards their cybersecurity strategy, their doctrine for managing cyber crises and responding to a cyberattack by:

        i. Providing an annual report to the international community on how far they have gone as regards cybersecurity;

        ii. Exposing any Member State who has been proven to have launched an attack while disregarding international law;

        iii. Ensuring national strategies be included in the annual report to be provided to the international community;

        iv. Ensuring sanctions are accorded to Member States who default in providing these reports;

    c. Oversee the current bilateral and multilateral initiatives gendered towards the building of cybersecurity capabilities of Member States lacking the financial and infrastructural resources required to effectively set up cyber defence strategies;

3. *Urges* Member States to provide and explore enacted policies targeted at mitigating cyber espionage by:

    a. Enacting cybercrime legislation if not already in place, using as a model, the International Telecommunication Union's toolkit for cybercrime legislation, making special provision for the prohibition of actions amounting to cyberespionage and cyberterrorism;

    b. Enacting various legislations that mandate all organizations operating in respective territories to safeguard the volumes of data collected and processed from all partners and stakeholders;

c. Enacting sanctions to serve as deterrence to Member States, organizations and groups from engaging in cyberespionage and cyberterrorism and funding cyberespionage and cyberterrorism activities;

4. *Strongly suggest*s that the United Nations and Member States be meticulous and be specific in areas of and inclusion of implementation mechanisms which could be amended by:

    a. Making provisions for specificity through including cyberespionage and cyberterrorism expressly in the provisions of conventions and treaties dealing with cybersecurity, cyberespionage and cyberterrorism;

    b. Providing implementation mechanisms respectively in the provisions of cyberterrorism and cyberespionage.