SAIMUN 2025

Resolution #422

EXPORTED 14TH AUGUST 2025 03:47
POWERED BY MODEL UNITED NATIONS CONFERENCE MANAGER

TQO: Reducing the Impact of Cyber Threats by International Terrorist Groups
COMMITTEE: The Disarmament and International Security Committee (DISEC)
MAIN SUBMITTER: United States of America
CO-SUBMITTERS: Belgium, Denmark, DRC, Egypt, Finland, Japan, Netherlands, Pakistan, Russia, U.K., Ukraine,

THE GENERAL ASSEMBLY,

Recalling UNSC Resolution 2341 (2017), which stresses the need to protect critical infrastructure from cyber threats by terrorist groups,

Recognizing GA Resolution 73/27 (2018), which highlights the growing risks of cyber threats and calls for international cooperation on cybersecurity,

1. **Calls for** the establishment of the Global Cybersecurity Counterterrorism Committee (GCCC), under the joint supervision of the DISEC Committee and the United Nations Office of Counter-Terrorism (UNOCT), to work in conjunction with the United Nations International Computing Centre (UNICC), UN System Chief Executives Board for Coordination (CEB) and the UN Office for Disarmament Affairs (UNODA), as well with other relevant bodies and NGOs, with funding provided by the International Monetary Fund (IMF) and the World Bank wherever deemed necessary, for this body to oversee the implementation and success of this resolution, for the GCCC to establish international guidelines and frameworks on counter cyber terrorism, remembering the Convention Against Cybercrime, with the aim to carry out the following but not limited to:
a. the establishment of the International Counter-Cyberterrorism Forum (ICF), with the aim to allow member states to share best practices and information regarding information, including but not limited to, potential cyber terrorist groups and independent cyber terrorist attacks, preventative measures
b. the joint initiative to improve cyber security, through the ICF, to help curb the impact on areas of infrastructure such as, Health Care, Financial Institutions, Electricity and other Energy Grids, and key Government Institutions
c. for the member states in the ICF, to discuss a UN definition for Cyber Terrorism with the intention to:
i. identify key groups under this definition, for these groups to be thoroughly investigated by the GCCC and UNOCT, with the creation of a new UN definition for cyber terrorists like the defining of terrorist organisations
ii. create a clear distinction between cyber attacks and cyber terrorism, in order to make discussion in the ICF more effective;

2. **Urges** the creation of bi-annual summit to be held in the UN headquarters in New York, to discuss the issue of cyberterrorism, with the involvement of any and all member states, especially members of the ICF, with participation with the GCCC, UNOCT and the UNICC, with the aim to discuss cyber regulation, prevention and legal frameworks, while encouraging the following:
a. for local governments to take information from both the ICF, private institutions, and the Summit to shape domestic and international policy regarding the prevention of cyber terrorist attacks, for the implementation of

both preventative measures and post attack response, to be created or improved upon
b. the creation of a rapid-response framework among participating nations to facilitate intelligence-sharing and coordinated actions in the event of large-scale cyber terrorist attacks
c. the GCCC to compile an annual report based on findings from the summit, to be given to the Secretary General, with the aim to provide a comprehensive report to all member nations;

3. **Requests** the GCCC to work in conjunction with the UNOCT and the DISEC Committee to produce a voluntary guideline for member states to base cyber security policy, with the aim to allow all member states to establish comprehensive and effective cyber security policies, in line with the threat proposed by cyberterrorism, for the produced guideline to be discussed at the bi-annual summit in clause 2, with discussion to include but not limited to:
a. collaboration between financial, telecommunication and government institutions to implement cyber security regulations, while encouraging:
i. private institutions to implement government sponsored cyber security programs, ensuring no sector is susceptible to attacks
ii. governmental institutions to advise and ensure the safety of private state information as well as the safekeeping of key infrastructure
b. the creation of Cyber Threat Intelligence Centers (CTICs), which analyze real-time cyber threats and provide threat mitigation strategies to government agencies and private sector partners
c. the establishment of an UN-sponsored cybersecurity assistance fund (CAF), designed to help developing nations build secure digital infrastructure and respond to cyber threats;

4. **Recognizes** the need for the GCCC to help improve cyber security capabilities for all member states, through the means of updating computing technology, the training of IT specialists and curbing the expansion and existence of cyberterrorism, which requires:
a. necessary technological equipment to be provided to all member states, that adopt this clause, to be funded by the CAF, to increase the technological capabilities of defense against such attacks
b. special training for new IT hires going into cyber security, and more specifically cyberterrorism security, to be trained in best practices by a joint UNESCO and UNOCT effort
c. a request to be issued to the Security Council to impose targeted economic sanctions against individuals, groups, and states that are found to be harboring cyberterrorists;

5. **Further calls for** public awareness campaigns to educate citizens on cybersecurity best practices and the risks associated with cyber threats by:
a. establishing mandatory cybersecurity curriculum in secondary education to ensure students develop cybersecurity literacy from an early age
b. encouraging the usage of multi-factor authentications and secure password management to reduce vulnerabilities.