SAIMUN 2025

Resolution #424

EXPORTED 28TH OCTOBER 2025 21:20
POWERED BY MODEL UNITED NATIONS CONFERENCE MANAGER

FORUM: DISEC
QUESTION OF: The Question of Reducing the Impact of Cyber Threats by International Terrorist Groups
SUBMITTED BY: Italy
CO-SUBMITTED BY: Australia, Bahamas, Bangladesh, Canada, China, Costa Rica, Haiti, Hungary, Iraq, Ireland, Mexico, Myanmar, Poland, Republic of South Africa

DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE,

Recognizing the increasing use of cyber tactics by international terrorist organizations to spread propaganda, recruit members, and conduct cyberattacks on critical infrastructure,
Alarmed by the rise in ransomware attacks, and digital financial crimes, which threaten global security and economic stability,

Noting with concern that many developing countries lack the necessary cybersecurity infrastructure to defend against cyber threats posed by terrorist groups,

Emphasizing that while international cybersecurity cooperation is necessary, each nation should retain sovereignty over its national cybersecurity policies,

Stressing the importance of public-private partnerships, particularly with technology companies, to prevent the use of online platforms for terrorist recruitment, financing, and propaganda,
1. **Emphasizes** the importance of international collaboration in countering cyber threats posed by terrorist organizations by:
a. Enhancing cross-border intelligence sharing and cooperation among states to improve real-time detection and response to cyber-enabled terrorism through encouraging bilateral and multilateral agreements between cybersecurity agencies to facilitate quicker information exchange on cyber threats linked to terrorist networks
b. Developing joint cybersecurity capacity-building programs to assist nations in strengthening their resilience against cyber threats by:
i. providing technical assistance and expertise, particularly to developing countries, to enhance national cybersecurity frameworks through knowledge-sharing initiatives,
ii. promoting public-private partnerships between governments, tech companies, and financial institutions to develop advanced cyber defense strategies against terrorist cyber activities;

2. **Encourages** member states of the United Nations (UN) to strengthen their national

cybersecurity infrastructures to prevent terrorist groups from exploiting cybersecurity vulnerabilities by:
a. detecting and neutralizing cyber threats before they grow by establishing advanced monitoring systems with
i. the implementation of AI-based threat detection systems to identify anomalous activities related to terrorism
ii. integrating cybersecurity measures into national critical infrastructure protection strategies
b. establishing cyber defense units, creating special teams against terrorist cyber attacks, and equipping these teams with the necessary tools and training to recognize threats and respond quickly
c. partnering with tech companies in order to make up for any gaps present in their cyber-security;

3. **Calls** for the creation of the International Cyber Threat Mitigation Organization (CTMO), which will:
a. aid in identifying Zero-Day attacks, which are especially problematic as they take place without the previous knowledge of software developers, by means of:
i. creating streams of funding for open-source developers, whose work makes up a majority of vital software projects, to incentivize them to continue updates and other essential security features
ii. collaborating with software companies to facilitate security best practices and early detection of security breaches
b. provide information to ordinary people, government agencies and private companies in order to educate people and inform them of how to counter cyber threats
c. create new cybersecurity standards which will be more extensive than existing ISO standards such as ISO 27001 or ISO 22301 in order to guide organizations towards better cybersecurity practices;

4. **Suggests** that all member states implement legislation that enforces KYC (Know Your Customer) standards for all monetary institutions, which will result in a severe bottleneck in funding streams for cyber terrorists, such that:
a. threat actors will not be able transfer financial assets without confirming their identity through either national or privatized KYC services,
b. cryptocurrency, IBAN, SWIFT and other means of transferring money without verification will ideally not be available;

5. **Firmly advises** member states to rebuild public trust through the elimination of ambiguous propaganda dissemination on social media which is done through the spread of misinformation, by:
a. Cultivating new information and detection technologies supported by Artificial intelligence to
i. disclose misleading information using a reliable database that is updated and overseen by the UN Open Ended Working Group (OEWG)
ii. educate individuals on the effects of and aspects of cyber terrorism and how it is linked to malicious activities both virtually and holisticallyb. Limiting the access of certain individuals and organisations to media platforms, unveiling their
identities via the standardization of identity verification protocols with the help of Groups of Governmental Experts (GGEs) in the UN;

6. **Invites** Member States to include cybersecurity education in school curricula and public awareness campaigns by:
a. creating public awareness campaigns that inform citizens about common cyber threats and how to practice safe online behavior,
b. integrating cybersecurity education into school curricula help teach the next generations the dangers of cyberattacks;

7. **Calls upon** Member Nations to undergo comprehensive reviews and ratifications of their domestic legal frameworks related to cyber security, with the aim of recognising weaknesses and establishing stronger and more reliable and standardised ways of preventing misuse of technology, further details include but are not limited to:
a. The inclusion of various relevant stakeholders such as national representatives, legal expert representatives from
the UN if consented to by member states, technology manufacturers, other relevant UN organisations such as the UNOCT or the International Telecommunication Union (ITU), and UN legal experts
b. Compliance with and consideration of all human rights, personal freedoms and ethical standards of member nations
c. The establishment of clear and concise legal pathways for the prosecution and sanction of those who misuse technologies for the purpose of cyber-attacks, again in alignment with national ethical standards and opinions
d. Suggestions and recommendations of important legal measures, such as guidelines for data collection, processing, and storage in technologies or the creation of protocols for data deletion after a defined period to negate the potential the compromising of data, unless legal exemptions apply
e. Setting up groups that will monitor all developments of such technology over time and adapt or create policies that will be suited to such development, as well as the promotion of flexible and adaptable policies in general to make this process more efficient.