United Nations YMUN/2024/SC/Agenda B/RES/1

Security Council (SC)

Distri.: General
21 January 2024

AGENDA: Measures to Combat Cyber Threats on the Security of Critical Infrastructure

CO-SPONSORS: Republic of Brazil, People's Republic of China, Republic of France, Republic of Ghana, State of Japan, Republic of Malta, Republic of Mozambique, Russian Federation, United Arab Emirates, United Kingdom, United States of America

Resolution 0001 (2024)

Adopted by YMUN 2024 at its 16th meeting on 21 January 2024

UNITED NATIONS SECURITY COUNCIL (UNSC)**,**

Concerned about both international and regional outbreaks of severe cases of cyberattacks,

Acknowledging the increasing frequency and sophistication of cyber attacks targeting critical infrastructure worldwide and its potential posed on essential services such as energy, transportation, healthcare, and finance,

Concerned by the potential cascading effects of cyber attacks on interconnected critical infrastructure, amplifying the impact and further exacerbating global vulnerabilities,

Strongly emphasising the importance of international consensus and cooperation in addressing the transnational nature of cyber threats to critical infrastructure,

Underlining the role of Member States in adopting comprehensive cybersecurity measures, including risk assessments, information sharing, and capacity-building initiatives,

Reaffirming the commitment to uphold the principles of sovereignty and value of non-intervention in peaceful dispute resolutions in cyberspace, while also recognizing the collective responsibility,

1. *Strongly encourages* member states to acknowledge that the basic requirements of international cooperation are based on essential trust between nations by implementing actions such as:
    a. strongly encouraging member nation in a short term of time to prohibit targeted accusations of specific nations as aggressors of cyberattacks made in the absence of straightforward evidence to recognise nations as negotiation partners, not as potential aggressors,
    b. strongly encouraging nations to empower domestic capabilities to regulate cyber attack initiators with specific actions such as but not limited to:
        i. requiring nations to reinforce domestic legislations to effectively utilise national capabilities of investigation and convict proper punishment to be made for cybercrimes,
        ii. requiring nations to implement measures to advance the efficiency of judicial authorities to enhance investigation capabilities;

2. Decides the formation of strengthened official international cooperation systems under the United Nations Office of Counter Terrorism (UNOCT) in regards to enhancing member states' capabilities to respond to cyberattacks with specific methods such as but not limited to:
    a. establishing a neutral professional investigating group under UNOCT to combat international cyber crimes to:
        i. reassuring that the fundamental principle of the UNOCT is to carry out unbiased and objective investigation at all times,
        ii. ensuring that such investigation groups are composed of individual experts directly employed by the UN, with diverse nationalities and cultural backgrounds to guarantee unbiased investigations,
        iii. inviting the United Nations Office of Project Services(UNOPS) to provide financial support that is required through the team's tasks,
        iv. investigating major incidents of cyberattacks and utilising the knowledge learned from the investigation to enhance coping capabilities when encountering similar attacks,
        v. providing the information about attackers, discovered through the investigation, to the damaged nation's government to support further investigation of each government,
        vi. responding to upcoming cyber attacks and providing possible precautions,
    b. installing effectively functioning cybersecurity systems in vulnerable governments to protect against leakage of critical information by employing methods such as but not limited to:

i. clearly stating that such installations will be operated under the sole decision of each nations to prevent the infringement of national sovereignty
ii. requesting each nation to actively communicate both on the national and international levels to identify vulnerable governmental systems that need a greater degree of attention,
iii. suggesting a wider range of investigations for the identified governmental systems,
iv. providing more protection for the identified governmental systems to preserve targeted information if requested;

3. *Further invites* the Member States of the Budapest Convention to establish an annual review conference to overcome the limitations of the convention and expand its impact by defining the specific composition of the conference with means such as:
    a. discussing methods of further improvements upon the limits of the Budapest Convention to clarify the practical legitimacy of the installation of the new annual conference in areas such as:
        i. lack of global participation from major nations,
        ii. slow adaptation of newly emerging concerns due to the rapid development of cyber technology,
        iii. clarifying the purpose of each review conference to discuss the consistent update process of the Budapest Convention,
        iv. intrusion of private information by establishing a dedicated session within the conference agenda specifically addressing privacy concerns arising from cybercrime,
    b. actively inviting private firms to the annual conference to extend the reach of collaboration to the civil sector and to enhance efficiency of implementations by discussing means such as:
        i. considering private firms as a major stakeholder process of collaboration, such as information sharing and technological cooperation,
        ii. inviting private firms to the pre-existing 24/7 network under the Budapest Convention to enhance information-sharing mechanisms and reinforce investigations in the cyber sector,
    c. obligating nations to designate cybersecurity experts to contribute to the knowledge of the discussion during the conference through methods such as:
        i. calling on nations to review and update their cybersecurity policies, while ensuring the accurate reflection of the latest global threats and developments,
        ii. mandating that each participating nation designates experienced and qualified cybersecurity representatives to contribute actively to the conference discussions;

4. *Decides to* set major legal frameworks regarding cybersecurity to concentrate the collective efforts of international stakeholders with specific means such as but not limited to:
    a. defining major terminologies for the efficient interpretation of collective objectives set by the United Nations through specific definitions such as but not limited to:
        i. defining the term cybercrime as “malicious attempts of illegal activity in the online sector to cause any type of direct or indirect damage to online individuals and socio-economic infrastructure”,
        ii. defining the term cyber attacks as “the aggressive use of force to disrupt, damage, or gain unauthorised access to cybernetworks of any stakeholder in the cyber sector”,
    b. requiring the member states of the General Assembly (GA) to further carry out negotiation to establish clear international legislation and legal standards to regulate both governmental and individual stakeholders in the online sector with means such as:
        i. acknowledging that the ultimate objective of such legislation is to concentrate the collective efforts of international stakeholders under the clear designation of agreed-term,
        ii. regulating governmental activity in the online sector by limiting the operation of governmental-based online aggression organisations,
        iii. regulating individual activity in the online sector through regulating the activity of individual groups that are accused of operating cyberattacks,
    c. requiring the member states of the General Assembly (GA) to conduct further elaboration and revisement of such legislations of regulation to guarantee the participation of all member states in the process of enactment;

5. *Urges* MEDCs that have proper cyber security infrastructure to assist nations that lack stable cyber security systems in a way such as but not limited to:
    a. setting goals to enhance the resilience and security of their critical infrastructure and information systems while recognising the severity of the infringement of cyber security within specific nations such as South Africa and Australia,
    b. requesting technologically advanced nations to provide technical support for stabilising cybersecurity support in methods such as but not limited to:
        i. sending various experienced experts on an official branch of the national cyber police group,

    ii. assisting the establishment of secure communication networks to protect sensitive data,

c. calling for financial aid to support countries with insufficient cyber systems, in which finance will be collected and used in a way such as but not limited to:
    i. requesting direct financial support from donors working with or in the UNODC and thereby allocate funds to acquire and deploy advanced cybersecurity technologies, tools, and infrastructure to protect critical systems and networks,
    ii. implementing projects in collaboration with the United Nations Development Programme (UNDP) for nations undergoing insufficient cyber systems to reinforce technology and cybersecurity
d. employing various methods to ensure appropriate usage of financial aid by utilising methods such as:
    i. evaluating countries that receive financial support and whether they annually utilise the supporting aid for efficient and fit purposes,
    ii. evaluating the usage of the supporting aid within international inspector groups of members,
    iii. stating consequences if their financial aid usage is detected as ‘improper’, the supported country should return the provided aid to the UNSC,
e. guaranteeing incentives to MEDCs who actively engaged in stabilising global cyber security by sharing access to information about former major cybersecurity attacks in the country having benefited from critical aid provided by MEDCs.