FORUM: Disarmament Commission

QUESTION OF: Enforcing Global Cybersecurity in a Rapidly Digitizing Era

MAIN-SUBMITTED BY: Australia

CO-SUBMITTED BY: Kenya

THE DISARMAMENT COMMISSION,

Guided by the purposes and principles enshrined in the charter of Nations,

Acknowledging deaths related to cybercrime such as leaking confidential information,

Keeping in mind that freedom of expression on the Internet must not be violated despite the significance of cybersecurity,

Viewing with appreciation that many great powers have been spending large portions of military budgets on cybersecurity,

Encourages the United Nations to accomplish the following,

1. Strongly recommends using more confidential and secured identification system:
    a. creating an Internet specification where the length and complexity of the password are increase,
    b. subsidizing foundations (including set theory and mathematical logic) mathematicians to find new prime numbers to increase cybersecurity between banks and military organizations,
    c. establishing a joint response system of private, public, and military sectors;

2. Encourages members in MEDCs to support LEDCs with technology, so LEDCs can increase technological development to maintain network security:
    a. coordinating and enacting international cybersecurity system between developed and developing countries to prevent avoidance of false competition, design and implement a national cyber defense doctrine,
    b. advanced tracking systems are needed to regulate Web browsers and programmers;
    c. providing younger generation education regarding the introduction to cybersecurity;

3. Encourages the establishment of an agency under the United Nations, with branches in its members countries with professionally trained employees:
    a. agency that will ensure protection and Information privacy among member states,
    b. it will oversee the country Organizations in countries dedicated to cybersecurity,
    c. operate a national Computer Emergency Response Team (CERT):
        i. options to establish a unit,
        ii. building cybersecurity infrastructure;

4. Promotes nations to subsidize their department of education on cybersecurity:
    a. aiding cybersecurity related majors financially to increase number of developers
    b. increment of job opportunity on cybersecurity:
        i. regulation on IT companies to hire cybersecurity department for their confidential information and technology,
        ii. extend the volume of governmental cybersecurity department;

5. Further reminds the United Nations to warn nations or groups that frequently cyberattack or attempt to hack:
    a. Scrutinizing the traces to specify the location and purpose of attack,
    b. Accusing out those nations or groups officially with evidence:
        i. Malware. Malware is a type of application that can perform a variety of malicious tasks,
        ii. Phishing,
        iii. Man-in-the-middle attack (MITM),
        iv. Distributed Denial-of-Service (DDoS) attack,
        v. SQL injection,
        vi. Zero-day exploit,
        vii. DNS Tunneling,
        viii. Business Email Compromise (BEC).