FORUM: Special Conference
QUESTION OF: Countering the Rising Cyber Security Threat
MAIN SUBMITTER: South Africa
CO-SUBMITTERS: The Hashemite Kingdom of Jordan

Taking Into Consideration the rapid and widespread growth and expansion of the internet, and the inevitable rampant expansion of cybercrime and breaches of cyber-security,

Alarmed by CSO Online's prediction that ransomware attacks will quadruple by 2020 and the Official Cybercrime Report 2017's prediction that global cybercrime damages will cost over 6 trillion USD annually by 2021,

Gravely Concerned by the possible dangers posed by state sponsored cybercrime to the security and stability of countries and its citizens,

Appreciating General Assembly resolution 65/230 and the Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8, mandating the Global Programme on cybercrime to assist member states in their struggle against cyber-related crimes through capacity building and technical assistance,

Acknowledges the need for improved efforts and communication to help provide adequate universal access to information and communication technologies to aid in protecting key information infrastructure and the privacy of users through transferring and sharing of technologies to developing countries with developing cyber-infrastructures.

1. Requests that state-sponsored cybercrime be treated as a serious act of aggression, and that the repercussions be serious as well, and therefore member states are urged to:
    a. Disapprove of any and all instances of state-sponsored cybercrime, as it is a barbarous and malicious act being carried out only to be detrimental to another state,
    b. Impose economic consequences on a state that has been found guilty of cybercrime, which could include,
        i. Economic penalties,
        ii. Tariffs imposed on goods imported from the guilty state;

2. Strongly Recommends the creation of legislation concerning cyber-security and cybercrimes in all member states, if not already done so, with sections on but not limited to,
    a. Defining the types of cybercrimes with their gravity and impact,

b. Forms and procedures for investigating cybercrimes,
c. Appropriate punishments for conspiring or orchestrating instances of cybercrime and breaches of cyber-security,
d. Responsibilities of businesses and organizations to protect, use and store user and sensitive data in a secure manner
e. Procedure for dialog and cooperation in events where an instance of cybercrime affects the world at an international level;

3. Invites member states and appropriate organizations to share their practices and security measures that they have developed to ensure the protection and security of critical infrastructure by providing the information to the UNODC for review and distribution among member states;

4. Recommends all member nations to create regulations on the collection, storage, usage, and sales of user data by the private sector, regulations may include but are not limited to,
    a. Policies that demand transparency on how and to who data is collected, and sold,
    b. Policies that ensure that no organization or business's use of data infringes on Article 12 of the Universal Declaration of Human Rights;

5. Strongly Encourages member states to aid developing nations with building up their cyber-security capabilities and enforcement against cyber-terrorism, this can be done by but not limited to,
    a. Monetary funding and support to anti cybercrime departments,
    b. Capacity building and training of law enforcement agencies by advisors and trainers from but not limited to more experienced member states or the UNODC,
    c. Strengthening dialogue and cooperation between the developing nations and more experienced member states, the United Nations and appropriate organizations such as Interpol;

6. Strongly Suggests that all member states improve communication and coordination with their private sector in order to address the common issue of protecting critical information infrastructures from bad actors, this can be done by but not limited to,
    a. The creation of a direct communication and incident reporting channel between government organizations and the private sector,
    b. Developing and coordinating emergency warning systems between consumers, the private sector, and government, to insure,
        i. Transparency
        ii. Awareness of consumers

iii. Swift and cooperative action between private sector and government in the case of a breach,

c. Identifying and examining the interdependencies between government and private sector infrastructures,
d. Creating regular, government-sanctioned inspections on whatever the country determines to be a major company,
    i. Inspections would occur annually,
    ii. The results would be shared with the company and be made public by being posted online in a government report;