Resolution GA/1/1.1

General Assembly First Committee

Co-sponsors: Republic of Angola, Republic of Botswana, Canada, Arab Republic of Egypt, Federal Democratic Republic of Ethiopia, Republic of France, Republic of Iraq, Republic of Kenya, United Mexican States, Islamic Republic of Pakistan, Republic of Rwanda, Slovak Republic, Republic of South Sudan, Socialist Republic of Viet Nam

Topic: Cybersecurity

The Committee,

Fully alarmed at the advancement in complete international cyber threats to accessible information on individuals, organizations, and infrastructure,

Deeply disturbed that 95% of breached records came from only three industries in 2016,

Bearing in mind the actions taken against cybercrime, the UN emphasizes that international framework is needed for establishing standards on cyberspace conduct and educating on the issues that cybercrime presents,

1. Calls upon the creation of a committee dedicated towards protecting cyberspace, spearheading cybersecurity incentives, the creation of task forces in collaboration with companies to implement the following suggestions, and deliberating towards an international framework;

2. Encourages the creation of a fund to educate and protect against cybercrime to be founded by member states of the proposed committee;

3. Proposes the creation and funding of programs to educate and promote awareness on pirated media and other forms of cybercrime, through increased training and presence from professionals, as well as from schools and workshops;

4. Recognizes that cybercrime is a prominent issue, the UN encourages that countries report on activities in cyberspace on a yearly basis, and recommends that member states are supplied with means of tracking cyber offenders and malware such as "red herrings" to allow authorities to track down hackers all over the world and trying to find information of hackers, in order to keep malware from being extremely powerful;

5. Declares accordingly that based upon the nature of this activity in countries facing the world disparity in cyberspace management, committee-funded programs will respond with contributions such as policy development, vulnerability assessments, forensic investigations, firewalls, synchronized encryption, backup cloud, cybercrime software, and anti-phishing campaigns;

6. Declares accordingly that through the cooperation between the committee-extension task force and worldwide corporations, as well as through education programs informing the public specifications on policy development will include;
    a. Further requests funding for firewalls especially in areas that don't have any already and focusing special attention on low income areas who are at higher risk of cyberattacks;
    b. Further recommending adding a messaging system and software to alert people of cybersecurity breaches as soon as they happen and organizations can inform you when you have been hacked;
    c. Encourages companies to have a back up of their records in a safe/second place on file, folder, etc;
    d. Update important passwords consistently (recommending every 1-3 months) and other passwords every 2 years and make sure you have two factor authentication;
7. Designates that a cybersecurity framework will be enforced as compulsory through monetary fines and other penalties, through potential means of a committee-sponsored treaty, as to more effectively ensure international security.