Commission: Disarmament and International Security Committee
Session: 23rd National Model United Nations Conference – 2019
Sponsors: United States of America, Russian Federation, Cuba, Ethiopia, India, Israel, Democratic People's Republic of Korea (North), United Kingdom of Great Britain, Portugal, Turkey

QUESTION OF: **SECURING CYBER BORDERS TO PREVENT PRIVATE AND NATIONAL ATTACKS.**

The General Assembly,

Bearing in mind that ransomware attacks which make use of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid, and cause an estimated $11 billion damages occur every 14 seconds in the world and many cases are left unreported,

Concerned that over the past 5 years, security breaches, resulting in unauthorised access to data, applications, services, networks and/or devices by bypassing their underlying security mechanisms, have increased by 67%,

Keeping in mind that cyber border attacks could have significant effects on national security, the economy and the livelihood and safety of citizens,

Deploring that cyber crimes caused by terrorists to access the country's classified or copyrighted information could disrupt social, economic, financial and environmental stability and lead to international conflicts,

Emphasizing that vulnerabilities in cyber security render the protection of sensitive data (private or at National level), state secrets and digitalized funds more complex and ineffective,

Grieved that with the advancement in technology, our cyber borders are vulnerable to endless cyber-attacks,

Commission: Disarmament and International Security Committee
Sponsors: United States of America, Russian Federation, Cuba, Ethiopia, India, Israel, Democratic People's Republic of Korea (North), United Kingdom of Great Britain, Portugal, Turkey

1. Emphasizes the need to build strong diplomatic global relationships to share knowledge and work to reduce the risks of spying through spyware, online surveillance, international espionage and siphoning of data;

2. Urges governments to collaborate with the private sector to collectively use a risk-management approach to mitigate vulnerabilities, raise the base level of cyber security and build resilience towards cyber threats;

3. Recommends the upgrading of the workforce in national and private sectors, by improving the size and skills of the labour force;

4. Further recommends the implementation of stricter rules, laws and penalties to discourage acts of international piracy and cyber-attacks;

5. Suggests the use of ethical hackers to discern threats, vulnerabilities in systems which may be exploited by malicious attackers, causing loss of data, financial loss or other major damage, as a means to track down real hackers and secure cyber borders;

6. Urges countries to work with international organisations to facilitate dialogue and partnerships among international public and private sectors, focused on protecting information structures and promoting a global culture of security;

7. Encourages the development of a global strategy promoting honesty and transparency, confidentiality of information and communication;

8. Supports a process for national vulnerability assessment to better understand the potential threats, and to be better prepared for upcoming security risks;

9. Requests member states to adopt laws on cybercrime and enable global collaborative policing to deal with cyber attackers;

Commission: Disarmament and International Security Committee
Sponsors: United States of America, Russian Federation, Cuba, Ethiopia, India, Israel, Democratic People’s Republic of Korea (North), United Kingdom of Great Britain, Portugal, Turkey

10. Further invites countries having efficient anti-cybercrime units to be involved in a global effort, share knowledge and help countries with weak anti-cybercrime units;

11. Urges governments to provide cyber defence-related education in educational institutions to promote safe web-browsing culture;

12. Suggests the use of Artificial Intelligence, machine learning and a high degree of automated processes to help protect our cyberspace, while seeking partnership from specialised agencies.