American Model United Nations
International Telecommunication Union

ITU/II/1

SUBJECT OF RESOLUTION: Cybersecurity

SUBMITTED TO: The International Telecommunication Union

The International Telecommunication Union,

Recalling Resolution 130 (Rev. Dubai, 2018), which strengthens the role of the International Telecommunication Union (ITU) in building confidence and security in the use of information and communication technologies,

Recalling also, Resolution 174 (Rev. Busan, 2014) reaffirming the ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies,

Acknowledging the efforts of France in the Paris Call to the Trust and Security in Cyberspace,

Understanding the importance of technological expansion and advancement, specifically in less developed Member States,

Deeply concerned with the potential negative impacts that increased technological advancements could have for both national and international security in relation to cybersecurity,

Noting that less developed Member States run the largest risk of cyberattacks as their cybersecurity infrastructure is less developed and thus less secure than wealthier Member States,

Noting with approval current steps being taken by Member States in regards to improving cybersecurity and promoting research opportunities into potential threats to cybersecurity,

Recognizing the independent sovereignty of Member States to make developmental decisions,

Acknowledging the importance of international support for development rather than direct intervention by international bodies,

Noting with concern the sanctity of financial capital in developing Member States, as they should not be required to rely on international private corporations for independent infrastructural development,

Believing that access to safe and secure technology is a fundamental human right in today's world,

1. *Urges* communication between Member States in regards to potential and corrected flaws in cybersecurity infrastructure that:

(a) Suggests the disclosure of identified cybersecurity threats, giving individual Member States the freedom to use and implement procedures based on that information as they please through diplomatic channels;

(b) Encourages the international expansion of organizations like the Organization for Security and Co-operation in Europe (OSCE), promoting the creation of a contact point to facilitate pertinent communications and dialogue on information and communication technology-related incidents and coordinate responses between Member States, creating confidence-building measures to ease the tension between participating Member States;

(c) Encourages open access to research portals such as the International Cyber Policy Centre (ICPC) in order to make educated advancements to cybersecurity;

2. *Promotes* the creation of an international support system for individualized technological developments in sovereign Member States that:

(a) Partners with international cyber non-governmental organizations (NGOs) in order to promote the dissemination of cybersecurity standards, and best practices in developing Member States;

(b) Encourages the use of previously vetted private, technological corporations for cyber development in the area of knowledge, while still supporting the rights of Member States to independently foster the development of their own tech corporations;

3. *Supports* the creation of a "United Nations Stamp of Approval" as an education measure for all cybersecurity information that:

(a) Informs organizations and individuals that, in order to receive the "stamp" the committee must be provided with evidence of following the previously held standards of best practices in technological security efforts, as determined by the committee, that will continuously be reevaluated by the committee;

(b) Establishes a whitelist of internet service providers and websites that Member States and individuals can refer to in order to increase public knowledge of what it means to be safe at this point and time and updates it as technological advancements occur;

(c) Provides a disclaimer that all websites can be at risk due to the dynamic nature of technological advancements;

(d) Acknowledges these websites have shown previous efforts to increase their cybersecurity and elaborates on the measures taken so as to increase knowledge on these practices;

(e) Partners with organizations like the National Cyber Security Alliance to promote awareness of internet safety for individuals, specifically as it relates to the private sector, to create a more educated society;

4. *Recommends* that international legislative bodies such as the European Union and the African Union assess the cybersecurity risks of Internet of Things (IOT) devices in Member States' respective countries by implementing measures of identity authentication such as two-factor authentication and biometry;

5. Encourages the implementation of basic cybersecurity systems at the beginning of less developed Member States internet infrastructure development by:

(a) Calling for international legislative bodies such as the European Union and the African Union to create incentives for their Member States to do so;

(b) Partnering with NGOs to aid in security research and awareness;

(c) Encourages continued upgrades to security services as technological advancements occur;

6. *Supports* efforts for the detection and prosecution of cybercriminals of all kinds by:

(a) Encouraging individual Member States to create internal legal regulations to further criminalize and protect against cyber crimes in their Member States;

(b) Encouraging the use of friendly hacking sites like HackerOne, YesWeHack and BugBounty programs to find potential weak points in cyber-framework before they become a problem;

(c) Urging Member States to create an internal framework to identify cyber threats, maintaining the diversity of independent international security protocols and simplifying the reporting processes for identified threats;

(d) Encouraging the International Criminal Court to undertake and investigate cases related to acts of cyber terrorism internationally.

Passed, Yes: 39 / No: 2 / Abstain: 10