American Model United Nations
International Telecommunication Union

ITU/II/2

SUBJECT OF RESOLUTION: Cybersecurity

SUBMITTED TO: The International Telecommunication Union

The International Telecommunication Union,

Understanding the need for guidance and best practices for private organizations,

Reaffirming International Telecommunication Union (ITU) Plenipotentiary Resolution 130 (Rev. Dubai, 2018), which stresses the importance of building security in less developed Member States as a means to achieve global security,

Reaffirming the purpose of Computer Incident Response Teams (CIRTs) already put in place by the ITU,

Emphasizing that voluntary information sharing of cybersecurity techniques would catalyze the creation of a safer technological infrastructure,

Sensitive to the specific cybersecurity needs of less developed Member States,

Recognizing the extent to which cybersecurity affairs of less developed States are dictated by the development of non-governmental organizations (NGOs) and private sectors operating within their borders,

Affirming the sovereignty of all Member States and recognizing the right of Member States to be the primary protector of their national security,

1. *Extends* the responsibility of the CIRTs that have been created by the ITU if the Member States so choose with the purpose to:

(a) Expand to Member States that do not currently utilize the CIRT structure;

(b) Oversee communications regarding cybersecurity internationally and between Member States and NGOs;

(c) Take preventive measures against cyberterrorism and cyber attacks, especially in regards to;

(i) External threats from other Member States;

(ii) Internal threats from non-governmental groups;

2. *Recommends* that individual Member States establish a centralized communications commission within their respective governments through the expanded CIRTs that will:

(a) Work with leaders if the communication and information technology sector in order to establish a framework of best practices;

(b) Focus on public outreach to inform consumers;

(c) Suggest the creation of regulations regarding adherence to the cybersecurity framework;

(d) Be implemented as an extension of the existing CIRT structure;

3. *Encourages* Member States to extend the Global Cybersecurity Index to better address the cybersecurity concerns of private organizations by:

(a) Establishing a set of unified best practices meant to be used as a standard for private organizations in addressing cybersecurity concerns such that they;

(i) Are the result of the public-private cooperation to ensure a framework that facilitates the strengthening of cybersecurity infrastructure while remaining cognizant of cost and business needs;

(ii) Are allowed to be used by any private organization with prior attention paid to risk management procedures regardless of size, degree of risk or current level of cybersecurity infrastructure sophistication;

(iii) Offer a methodology to protect the privacy and civil liberties to help organizations incorporate these protections into a comprehensive cybersecurity program;

(iv) Encourage private organizations to share information with governments in order to better identify and address threats;

(b) Government officials holding periodic meetings with key members of the communications sector, such as those corporations contributing significantly to the private cybercommunication sector in their respective Member States which will focus on;

(i) Private organzations that are crucial to communications and information infrastructure and their adherence to the established best practices or an equivalent independently established cybersecurity framework;

(ii) Information sharing regarding cybersecurity threats and possible solutions;

(iii) Continuously evaluating and reassessing the current list of best practices to analyze effectiveness, efficiency, and prospective future changes in order to keep up with the ever-changing cybersecurity landscape;

4. *Recommends* that Member States create a committee to formulate an incentive structure which encourages private organizations to adhere to the nationally established policy framework which should:

(a) Grant subsidies, tax exemptions, or similar benefits to private organizations with a high level of adherence to a centrally established cybersecurity framework;

(b) Provide additional subsidies to organizations that are early adopters of novel cybersecurity technologies;

(c) Impose restrictions on or barriers to organizations that fail to adhere satisfactorily to their established cybersecurity standards;

5. *Encourages* Member States to increase their oversight of the network operations of NGOs within their borders to the fullest extent possible within their respective means:

(a) By establishing permanent information-sharing channels where;

(i) NGOs proactively investigate potential weaknesses in their frameworks that are salient to governments and subsequently provide that information to the Member State;

(ii) Regular reports are written and provided to relevant governmental authorities regarding their network operations;

(b) By recommending a unified set of best practices for both the supranational and State-level operations of NGOs operating within their borders with;

(i) A primary focus on maintaining sovereign control over network operations in their respective States;

(ii) An additional focus on safeguarding information and the security of information distribution channels;

6. *Suggests* Member States who do not wish to implement CIRTs to create their own similar response teams.

Passed, Yes: 24 / No: 6 / Abstain: 14