



American Model United Nations
International Telecommunication Union

ITU/II/3

SUBJECT OF RESOLUTION: Cybersecurity

SUBMITTED TO: The International Telecommunication Union

The International Telecommunication Union,

1 *Recalling* 2009 Resolution 64/211 in support of creating a global culture of cybersecurity and taking stock
2 of national efforts to protect critical information infrastructures,

3 *Recognizing* the Resolution 55/63 and 73/27, which invite Member States to create legal measures and
4 organizational structures to help combat cybercrime,

5 *Acknowledging* the benefits for Member States found in cooperation between governments in dealing with
6 cyber threats as well as sharing new technologies,

7 *Noting* that currently accepted frameworks for international cooperation regarding cybersecurity are not
8 widely acknowledged,

9 1. *Reaffirms* and publicizes the commitment of Member States to Resolution 73/27 through the education
10 of developers on international guidelines, emphasizing:

11 (a) Respect for human rights and privacy;

12 (b) Protection of critical infrastructure;

13 (c) Ensurance of the integrity of the supply chain;

14 (d) Reporting of information and communications technology (ICT) vulnerabilities, and;

15 (e) Self assessment of actions taken by domestic networks and corporations to ensure that all actions
16 are in line with international regulations;

17 2. *Proposes* that Member States take steps to address the large-scale issue of information asymmetry by
18 establishing a centralized consumer affairs and outreach division which should:

19 (a) Create a variety of classroom initiatives available to Member States to educate youths on cy-
20 bersecurity against attacks by militant groups, individuals, or hostile governments in order to raise a workforce that
21 understands their technological vulnerabilities;

22 (b) Use internet campaign strategies to;

23 (i) Inform citizens about important consumer-related regulatory programs, communication and in-
24 formation technology issues, and other consumer issues that affect their day-to-day life;

25 (ii) Inform citizens about the nature of cyber threats that put individuals at risk, and will periodically
26 update them on new developments and threats;

27 (c) Create a small business guidance initiative which shall;

28 (i) Consolidate information voluntarily given Member States, corporations, and non-governmental
29 organizations (NGOs) who report cybersecurity attacks;

30 (ii) Remain accessible at no cost to all those who wish to access it;

31 (iii) Be updated on a regular basis of three month increments;

32 (iv) Be prohibited from tracking or collecting user data from those accessing it;

33 (d) Launch a broadband and internet service provider labeling program, which consists of;

- 34 (i) A cybersecurity evaluation program which will allow consumers to make informed choices about
35 their broadband and internet service providers;
- 36 (ii) A rating system which will rate or rank broadband and internet service providers according to
37 how well they adhere to either a centrally established or independently established cybersecurity
38 framework;
- 39 (e) Create a small business guidance initiative which shall;
- 40 (i) Consist of a panel of experts in communications and information technologies and cybersecurity;
- 41 (ii) Work with small businesses to help them create customized cybersecurity plans that work on a
42 small-scale while also being cost-effective;
- 43 (iii) Create a streamlined, easy to understand tip sheet from small business to allow them to construct
44 their own cybersecurity plans without the need for direct involvement with the guidance initiative;

45 3. *Recommends* that Member States emphasize cooperation and coordination in cybersecurity efforts by pro-
46 viding to other governments, at their own discretion, relevant data about computer systems or any other information
47 that might be deemed necessary to and for international security by:

- 48 (a) Setting a precedent for information sharing between Member States that;
- 49 (i) Establishes a set of standards for information sharing between Member States that;
- 50 (ii) Formulates a list of sensitive topics related to national security that Member States should avoid
51 when sharing information;
- 52 (b) Setting guidelines and standards for addressing cyber attacks by terrorist organizations which
53 base their operations in multiple Member States;
- 54 (c) Encouraging developed Member States to aid those governments in need of assistance in meeting
55 these goals;

56 4. *Promotes* the following goals to guide Member States' efforts in combating cyber crime:

- 57 (a) Effective assessment that aids governments in their understanding of their domestic situation on
58 cybersecurity;
- 59 (b) Informed legislation that guides cybersecurity decisions;
- 60 (c) Education that develops a skilled and competent workforce to detect, defend and respond to
61 cyber attacks.

Passed, Yes: 20 / No: 14 / Abstain: 15