



American Model United Nations
General Assembly First Committee

GA First/I/1

SUBJECT OF RESOLUTION: Developments in the field of information and telecommunications
in the context of international security

SUBMITTED TO: The General Assembly First Committee

The General Assembly First Committee,

1 *Emphasizing* the comparison between developing and developed countries worldwide in regards to the gap
2 in the security of the telecommunications sector,

3 *Recognizing* the need for an interconnected global society,

4 *Noting with satisfaction* the beneficial opportunities of globalization for the further development of civi-
5 lization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the
6 creative potential of mankind and additional improvements in the circulation of information in the global community,

7 *Acknowledging* the international nature of the issue of cyber-security and the prevalence of non-state actors
8 participating in this area,

9 *Taking into consideration* the importance of reconciling the values of collaboration, transparency and security
10 on the issue,

11 *Expressing its hope* that States will come together and collectively work to end the telecommunications gap
12 and control cyber-terrorism,

13 *Welcoming* continued reports from the Groups of Government Experts (GGE) establishing norms on the re-
14 sponsible behavior of States in the cyber-sphere as well as relevant contextual discussions focused on issues associated
15 with addressing cyber-sphere problems,

16 *Deeply believing* that developed countries can work with developing countries to close this gap and help
17 increase international security,

18 1. *Recommends* that Member States, Non-Governmental Organizations (NGOs) and other organizations
19 involved in foreign aid make the expansion of telecommunications networks a priority;

20 2. *Further recommends* that special attention be granted to the dynamic between each national government
21 and its respective private sector such that a degree of information transparency between private entities in which
22 cyber-networks are an integral component and the government is established, such that:

23 (a) Domestic databases of information, the content, format and scope of which is to be determined
24 by each Member State, can be assembled as a reference by which national CERTs can coordinate informed responses
25 to cybersecurity threats;

26 (b) These measures are brought to the attention of Member States on the domestic level regarding
27 the following conditions;

28 (i) Established power distribution between the government and the private sector assuring that each
29 State's domestic legislation is not interfered with;

30 (ii) Unnecessary coercion of private individuals and business entities is not actively encouraged by
31 the international community;

32 3. *Encourages* Member States, NGOs and other organizations involved in the development of telecommuni-
33 cations throughout the world to make security a principal concern in the expansion of networks with a special focus
34 on:

35 (a) Lending assistance to States with underdeveloped cybersecurity resources and abilities;

36 (b) Focusing on the expansion of cellular telephone and internet access;

37 4. *Encourages* the cooperation between the International Telecommunications Union with the United Nations
38 to facilitate discussion between States on the subject of prevention and response of cyber-theft of intellectual property
39 organized around:

40 (a) The incorporation of the United Nations Office of Drugs and Crime in the process of exploring
41 solutions;

42 (b) A focus on building international consensus with regards to responding to cyber-security and
43 cyber-criminal threats;

44 5. *Invites* Member States to offer increased clarity on the definition of multiple abuses of the cyber-sphere
45 in the reports submitted to the GGE;

46 6. *Recommends* the organization of regional telecommunication security agencies, focused on building and
47 coordinating cyber-security efforts on a regional basis, operating parallel to existing regional cyber-security agencies
48 and multinational efforts as well as the global community as a whole;

49 7. *Discourages* the malevolent use of telecommunications infrastructure to deliberately malign and undermine
50 legitimate uses and users of telecommunications;

51 8. *Applauds* existing State and non-state level efforts to investigate cyber-attacks and cyber-criminal activ-
52 ities pursuant to international goals of reducing incidents relating to information technology;

53 9. *Encourages* all Member States to collaborate with and contribute to existing efforts to combat cyber-crime
54 across all Member States, in particular:

55 (a) To make sure that independent efforts on the part of Member States complement and/or do not
56 interfere with each other;

57 (b) To establish direct lines of communication between Member States in ensuring that efforts are
58 not in violation of national sovereignty;

59 10. *Encourages* Member States to unite and collaborate to prevent third-party cyber-criminals from com-
60 mitting criminal acts both within and across State borders, and that the appropriate criminal courts are advised of
61 the jurisdiction over the prosecution of these individuals or entities should they be apprehended.

Passed, Yes: 84 / No: 8 / Abstain: 7