United Nations A/RES/64/211

# General Assembly

Distr.: General
17 March 2010

**Sixty-fourth session**
Agenda item 55 (*c*)

## Resolution adopted by the General Assembly on 21 December 2009

[*on the report of the Second Committee (A/64/422/Add.3)*]

### 64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

*The General Assembly*,

*Recalling* its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity and 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures,

*Recalling also* its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008 on developments with respect to information technologies in the context of international security,

*Recalling further* the outcomes of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),[1]

*Recognizing* that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented,

*Recognizing also* the increasing contribution made by networked information technologies to many of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals and organizations, Governments, business and civil society,

[1] See A/C.2/59/3 and A/60/687.

*Recognizing further* that, in a manner appropriate to their roles, Governments, business, organizations and individual owners and users of information technologies must assume responsibility for and take steps to enhance the security of these information technologies,

*Recognizing* the importance of the mandate of the Internet Governance Forum as a multi-stakeholder dialogue to discuss various matters, including public policy issues related to key elements of Internet governance in order to foster sustainability, robustness, security, stability and development of the Internet, and reiterating that all Governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet,

*Reaffirming* the continuing need to enhance cooperation, to enable Governments, on an equal footing, to carry out their roles and responsibilities in international public policy issues pertaining to the Internet, but not the day-to-day technical and operational matters that do not impact on international public policy issues,

*Recognizing* that each country will determine its own critical information infrastructures,

*Reaffirming* the need to harness the potential of information and communications technologies to promote the achievement of the internationally agreed development goals, including the Millennium Development Goals, recognizing that gaps in access to and use of information technologies by States can diminish their economic prosperity, and reaffirming also the effectiveness of cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity,

*Stressing* the need for enhanced efforts to close the digital divide in order to achieve universal access to information and communications technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing countries, especially the least developed countries, in the areas of cybersecurity best practices and training,

*Expressing concern* that threats to the reliable functioning of critical information infrastructures and to the integrity of the information carried over those networks are growing in both sophistication and gravity, affecting domestic, national and international welfare,

*Affirming* that the security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles,

*Recognizing* that national efforts should be supported by international information-sharing and collaboration, so as to effectively confront the increasingly transnational nature of such threats,

*Noting* the work of relevant regional and international organizations on enhancing cybersecurity, and reiterating their role in encouraging national efforts and fostering international cooperation,

*Noting also* the 2009 report of the International Telecommunication Union on securing information and communication networks and best practices for developing a culture of cybersecurity, which focused on a comprehensive national approach to cybersecurity consistent with free speech, the free flow of information and due process of law,

*Recognizing* that national efforts to protect critical information infrastructures benefit from a periodic assessment of their progress,

1. *Invites* Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity, so as to highlight areas for further action, with the goal of increasing the global culture of cybersecurity;

2. *Encourages* Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity by providing such information to the Secretary-General for compilation and dissemination to Member States.

*66th plenary meeting*
*21 December 2009*

## Annex

## Voluntary self-assessment tool for national efforts to protect critical information infrastructures[2]

*Taking stock of cybersecurity needs and strategies*

1. Assess the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.

3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present and the current management plan; note how changes in the economic environment, national security priorities and civil society needs affect these calculations.

4. Determine the goals of the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives and how such a strategy fits within regional and international initiatives.

[2] This is a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity.

*Stakeholder roles and responsibilities*

5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

- National Government ministries or agencies, noting primary points of contact and responsibilities of each;
- Other government (local and regional) participants;
- Non-governmental actors, including industry, civil society and academia;
- Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

*Policy processes and participation*

6. Identify formal and informal venues that currently exist for Government-industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

7. Identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

*Public-private cooperation*

8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information-sharing and incident management.

9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

*Incident management and recovery*

10. Identify the Government agency that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

11. Separately, identify national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident-management information.

12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

*Legal frameworks*

13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

*Developing a global culture of cybersecurity*

18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.