United Nations A/RES/58/199

General Assembly

Distr.: General
30 January 2004

Fifty-eighth session
Agenda item 91 (*b*)

Resolution adopted by the General Assembly

[*on the report of the Second Committee (A/58/481/Add.2)*]

58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures

The General Assembly,

Recalling its resolutions 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity, 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies, and 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Recognizing the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services, the conduct of business and the exchange of information for Governments, businesses, other organizations and individual users,

Noting the increasing links among most countries' critical infrastructures — such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health — and the critical information infrastructures that increasingly interconnect and affect their operations,

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

Recognizing also that this growing technological interdependence relies on a complex network of critical information infrastructure components,

Noting that, as a result of increasing interconnectivity, critical information infrastructures are now exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns,

Noting also that effective critical infrastructure protection includes, inter alia, identifying threats to and reducing the vulnerability of critical information infrastructures, minimizing damage and recovery time in the event of damage or attack, and identifying the cause of damage or the source of attack, *Recognizing* that effective protection requires communication and cooperation nationally and internationally among all stakeholders and that national efforts should be supported by effective, substantive international and regional cooperation among stakeholders,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cybersecurity and the protection of critical information infrastructures through the support of national efforts aimed at the enhancement of human capacity, increased learning and employment opportunities, improved public services and better quality of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting the work of relevant international and regional organizations on enhancing the security of critical information infrastructures,

Recognizing that efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation,

1. *Takes note* of the elements set out in the annex to the present resolution for protecting critical information infrastructures;

2. *Invites* all relevant international organizations, including relevant United Nations bodies, to consider, as appropriate, inter alia, these elements for protecting critical information infrastructures in any future work on cybersecurity or critical infrastructure protection;

3. *Invites* Member States to consider, inter alia, these elements in developing their strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for critical information infrastructure protection into account in their preparations for the second phase of the World Summit on the Information Society, to be held in Tunis from 16 to 18 November 2005;

5. *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;

6. *Stresses* the necessity for enhanced efforts to close the digital divide, to achieve universal access to information and communication technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building, in particular to developing countries, especially the least developed countries, so that all States may benefit fully from information and communication technologies for their socio-economic development.

78th plenary meeting
23 December 2003

Annex

Elements for protecting critical information infrastructures

1. Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.

2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.

3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.

4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.

5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

6. Ensure that data availability policies take into account the need to protect critical information infrastructures.

7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.

8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities.

9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.

10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

11. Promote national and international research and development and encourage the application of security technologies that meet international standards.