General Assembly

Distr.: General
31 January 2003

Fifty-seventh session
Agenda item 84 (*c*)

Resolution adopted by the General Assembly

[*on the report of the Second Committee (A/57/529/Add.3)*]

57/239. Creation of a global culture of cybersecurity

The General Assembly,

Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Recognizing that the need for cybersecurity increases as countries increase their participation in the information society,

Recalling its resolutions 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,

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 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Aware that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society,

Aware also that technology alone cannot ensure cybersecurity and that priority must be given to cybersecurity planning and management throughout society,

Recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of international 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 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 that, as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all,

Noting also the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies,

1. *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity;

2. *Invites* all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity;

3. *Invites* Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005;

5. *Stresses* the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity.

78th plenary meeting
20 December 2002

Annex

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks (“participants”) must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary elements:

(*a*) *Awareness*. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(*b*) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(*c*) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(*d*) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(*e*) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(*f*) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(*g*) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(*h*) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(*i*) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.