UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

SECURITY AND TECHNOLOGY PROGRAMME

GGE recommendations on confidence building and cooperative measures

2004-2005 GGE | A/60/202

Procedural report only

2009-2010 GGE | A/65/201

To reduce the risk of misperception stemming from ICT disruptions, the Group recommended that States:

18.

i. Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure;
ii. Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
iii. Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
iv. Identification of measures to support capacity-building in less developed countries;
v. Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.

2012-2013 GGE | A/68/98

To increase transparency, predictability and cooperation, the Group recommended that States consider:

26.

a) The exchange of views and information on a voluntary basis on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation. The extent of such information will be determined by the providing States. This information could be shared bilaterally, in regional groups or in other international forums;
b) The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from State use of ICTs and how these incidents might develop and be managed;
c) Enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of

communication for crisis management, and supporting the development of early warning mechanisms;

d) Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels;

e) Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among States against disruptions perpetrated by non-State actors;

f) Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security.

27. States should encourage and build upon progress made bilaterally and multilaterally, … . In building upon those efforts, States should promote complementarity of measures and facilitate the dissemination of best practices, taking into account the differences among nations and regions.

28. While States must lead in the development of confidence-building measures, their work would benefit from the appropriate involvement of the private sector and civil society.

Additional recommendations

29 [T] here is a need to enhance common understandings and intensify practical cooperation. In this regard, the Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums, and other international organizations.

2014-2015 GGE	A/70/174

To enhance trust and cooperation, and reduce the risk of conflict, the GGE recommended:

16.

(a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;

(b) The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;

(c) Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;

(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:

  a. A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;
  b. The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
  c. The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;
  d. The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.

Additional recommendations

17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to:

a. Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;
b. Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;
c. Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;
d. Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;
e. Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

18. [T]he Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums and other international organizations.

2016-2017 GGE	A/72/327
Procedural report only	