United Nations A/68/98*

General Assembly

Distr.: General
24 June 2013

Original: English

Sixty-eighth session
Item 94 of the provisional agenda**
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 66/24.

* Reissued for technical reasons on 30 July 2013.
** A/68/150.

13-37166* (E) 310713

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Summary

Information and Communication Technologies (ICTs) have reshaped the international security environment. These technologies bring immense economic and social benefits. ICTs can also be used for purposes that are inconsistent with international peace and security, producing a noticeable increase in risk in recent years as they are used for crime and other disruptive activities. Malicious use of ICTs by actors who often operate with impunity is easily concealed and attribution to a specific perpetrator can be difficult. This creates an environment that facilitates the use of ICTs for increasingly sophisticated exploits.

Member States have frequently affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. International cooperation is essential to reduce risk and enhance security. Further progress in cooperation at the international level will require actions to promote a peaceful, secure, open and cooperative ICT environment. Cooperative measures that could enhance stability and security include norms, rules and principles of responsible behaviour by States, voluntary measures to increase transparency, confidence and trust among States and capacity-building measures. States must lead in these efforts, but effective cooperation would benefit from the appropriate participation of the private sector and civil society.

Recognizing the comprehensiveness of the challenge, taking into account existing and potential threats, and building upon the recommendations contained in the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of July 2010 (A/65/201), the Group of Governmental Experts offers in the present report its recommendations to promote peace and stability in State use of ICTs.

The report recognizes that the application of norms derived from existing international law relevant to the use of ICTs by States is essential to reduce risks to international peace, security and stability. The report recommends further study to promote common understandings on how such norms apply to State behaviour and the use of ICTs by States. Given the unique attributes of ICTs, the report notes that additional norms could be developed over time.

The report reflects the Group's conclusion that international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. The Group also concluded that State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory; States must meet their international obligations regarding internationally wrongful acts attributable to them. The report contains recommendations on voluntary measures to build trust, transparency and confidence, as well as international cooperation to build capacity for ICT security, especially in developing countries. The Group

recommends the holding of regular institutional dialogue on these issues under the auspices of the United Nations as well as regular dialogue in other forums, to advance these measures. Member States should give active consideration to the present report and assess how they might take up these recommendations for further development and implementation.

Contents

Foreword by the Secretary-General

Information and communications technologies (ICTs) are woven into the fabric of daily life. While all nations appreciate the enormous benefits of ICTs, there is also broad recognition that misuse poses risks to international peace and security.

The present report contains recommendations developed by a group of governmental experts from fifteen States to address existing and potential threats from States, their proxies or non-State actors through the use of ICTs. It builds on the 2010 recommendations of a previous group of experts which included the need for further work on norms, ways to increase confidence and capacity-building measures.

I appreciate the report's focus on the centrality of the Charter of the United Nations and international law as well as the importance of States exercising responsibility. The recommendations point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security.

As the group notes, the United Nations plays an important role in promoting dialogue among Member States on the issue of security in the use of ICTs and in further developing international cooperation in this field.

I thank the Chair of the Group and the experts for their diligent work. The report provides a sound basis for future efforts to enhance security and stability in the use of ICTs. I commend its recommendations to the General Assembly as a crucial step in the global effort to minimize the risks associated with ICTs while optimizing their value.

Letter of transmittal

7 June 2013

I have the honour to submit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was appointed in 2012 pursuant to paragraph 4 of General Assembly resolution 66/24. As Chair of the Group, I am pleased to inform you that consensus was reached on the report.

In its resolution, "Developments in the field of information and telecommunications in the context of international security", the General Assembly requested that a group of governmental experts be established in 2012, on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space, as well as the concepts aimed at strengthening the security of global information and telecommunications systems. The Group was also asked to take into account the assessments and recommendations of a previous group (A/65/201). The Secretary-General was requested to submit a report on the results of the study to the General Assembly at its sixty-eighth session.

In accordance with the terms of the resolution, experts were appointed from 15 States: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland and the United States of America. The list of experts is contained in the annex.

The Group of Governmental Experts had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security. The Group met in three sessions: the first from 6 to 10 August 2012 at United Nations Headquarters; the second from 14 to 18 January 2013 at Geneva; the third from 3 to 7 June 2013 at United Nations Headquarters.

The Group wishes to express appreciation for the contribution of the United Nations Institute for Disarmament Research, which served as consultant to the Group, and which was represented by James Lewis, Kerstin Vignard (second and third sessions) and Ben Baseley-Walker (first session). The Group also wishes to express appreciation to Ewen Buchanan of the United Nations Office for Disarmament Affairs, who served as Secretary of the Group, and to other Secretariat officials who assisted the Group.

(*Signed*) Deborah **Stokes**
Chair of the Group

I. Introduction

1. The use of information and communication technologies (ICTs) has reshaped the international security environment. These technologies bring immense economic and social benefits; they can also be used for purposes that are inconsistent with international peace and security. There has been a noticeable increase in risk in recent years as ICTs are used for crime and the conduct of disruptive activities.

2. International cooperation is essential to reduce risk and enhance security. For this reason, the General Assembly requested the Secretary-General, with the assistance of a group of governmental experts, to continue to study possible cooperative measures to address existing and potential threats (resolution 66/24), and submit a report to the sixty-eighth session of the Assembly. The present report builds upon the 2010 report (A/65/201) from the previous Group of Governmental Experts, which examined this topic and made recommendations for future work.

3. The 2010 report recommended further dialogue among States on norms pertaining to State use of ICTs to reduce collective risk and protect critical national and international infrastructure. It called for measures on confidence-building, stability and risk reduction, including exchanges of national views on the use of ICTs in conflict, information exchanges on national legislation, ICT security strategies, policies, technologies and best practices. The 2010 report stressed the importance of building capacity in States that may require assistance in addressing the security of their ICTs and suggested additional work to elaborate common terms and definitions.

4. Numerous bilateral, regional and multilateral initiatives since 2010 highlight the growing importance accorded to greater security of and in the use of ICTs, reducing risks to public safety, improving the security of nations and enhancing global stability. It is in the interest of all States to promote the use of ICTs for peaceful purposes. States also have an interest in preventing conflict arising from the use of ICTs. Common understandings on norms, rules and principles applicable to the use of ICTs by States and voluntary confidence-building measures can play an important role in advancing peace and security. Although the work of the international community to address this challenge to international peace and security is at an early stage, a number of measures concerning norms, rules and principles for responsible State behaviour can be identified for further consideration.

Threats, risks and vulnerabilities

5. ICTs are dual-use technologies and can be used for both legitimate and malicious purposes. Any ICT device can be the source or the target of misuse. The malicious use of ICTs can be easily concealed and attribution to a specific perpetrator can be difficult, allowing for increasingly sophisticated exploits by actors who often operate with impunity. The global connectivity of ICT networks exacerbates this problem. The combination of global connectivity, vulnerable technologies and anonymity facilitates the use of ICTs for disruptive activities.

6. Threats to individuals, businesses, national infrastructure and Governments have grown more acute and incidents more damaging. The sources of these threats comprise both State and non-State actors. In addition, individuals, groups, or organizations, including criminal organizations, may act as proxies for States in the conduct of malicious ICT actions. The potential for the development and the spread of

sophisticated malicious tools and techniques, such as bot-nets, by States or non-State actors may further increase the risk of mistaken attribution and unintended escalation. The absence of common understandings on acceptable State behaviour with regard to the use of ICTs increases the risk to international peace and security.

7. Terrorist groups use ICTs to communicate, collect information, recruit, organize, plan and coordinate attacks, promote their ideas and actions and solicit funding. If such groups acquire attack tools, they could carry out disruptive ICT activities.

8. States are concerned that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security.

9. The expanding use of ICTs in critical infrastructures and industrial control systems creates new possibilities for disruption. The rapid increase in the use of mobile communications devices, web services, social networks and cloud computing services expands the challenges to security.

10. Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world. Malicious actors exploit networks no matter where they are located. These vulnerabilities are amplified by disparities in national law, regulations and practices related to the use of ICTs.

II. Building cooperation for a peaceful, secure, resilient and open ICT environment

11. Member States have repeatedly affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. Further progress in cooperation at the international level will require an array of actions to promote a peaceful, secure, open and cooperative ICT environment. Consideration should be given to cooperative measures that could enhance international peace, stability and security. These include common understandings on the application of relevant international law and derived norms, rules and principles of responsible behaviour of States.

12. While States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society.

13. The United Nations should play a leading role in promoting dialogue among Member States to develop common understandings on the security of and in the use of ICTs, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices.

14. In addition to work in the United Nations system, valuable efforts are being made by international organizations and regional entities such as the African Union; the Association of Southeast Asian Nations (ASEAN) Regional Forum; the Asia Pacific Economic Cooperation Forum; the Council of Europe; the Economic Community of West African States; the European Union; the League of Arab States; the Organization of American States; the Organization for Security and Cooperation in Europe (OSCE); and the Shanghai Cooperation Organization. Future work on security in the use of ICTs should take these efforts into account.

15. Recognizing the comprehensiveness of the challenge, taking into account existing and potential threats, risks and vulnerabilities and building upon the assessments and recommendations contained in the July 2010 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201), the Group recommends the following measures.

III. Recommendations on norms, rules and principles of responsible behaviour by States

16. The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understandings on how such norms shall apply to State behaviour and the use of ICTs by States requires further study. Given the unique attributes of ICTs, additional norms could be developed over time.

17. The Group considered the views and assessments of Member States on developments in the field of information and telecommunications in the context of international security provided in response to the invitation from the General Assembly contained in its resolutions 64/25, 65/41 and 66/24, as well as other measures contained in resolutions 55/63, 56/121, 57/239, 58/199 and 64/211.

18. The Group noted document A/66/359, circulated by the Secretary-General at the request of the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, containing a draft international code of conduct for information security, which was subsequently co-sponsored by Kazakhstan and Kyrgyzstan.

19. International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.

20. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.

21. State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.

22. States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies.

23. States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.

24. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services.

25. Member States should consider how best to cooperate in implementing the above norms and principles of responsible behaviour, including the role that may be

played by private sector and civil society organizations. These norms and principles complement the work of the United Nations and regional groups and are the basis for further work to build confidence and trust.

IV. Recommendations on confidence building measures and the exchange of information

26. Voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. They can make an important contribution to addressing the concerns of States over the use of ICTs by States and could be a significant step towards greater international security. States should consider the development of practical confidence-building measures to help increase transparency, predictability and cooperation, including:

(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. These initial efforts at confidence-building can provide practical experience and usefully guide future work. States should encourage and build upon progress made bilaterally and multilaterally, including in regional groups such as the African Union, the ASEAN Regional Forum, the European Union, the League of Arab States, the Organization of American States, the OSCE, the Shanghai Cooperation

Organization and others. 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.

29. Given the pace of ICT development and the scope of the threat, the Group believes there 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.

V. Recommendations on capacity-building measures

30. Capacity-building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to: improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use.

31. In this regard, States working with international organizations, including United Nations agencies and the private sector, should consider how best to provide technical and other assistance to build capacities in ICT security and their use in countries requiring assistance, particularly developing countries.

32. Building on the work of previous United Nations resolutions and reports, including resolution 64/211 on capacity-building, States should consider the following measures:

(a) Supporting bilateral, regional, multilateral and international capacity-building efforts to secure ICT use and ICT infrastructures; to strengthen national legal frameworks, law enforcement capabilities and strategies; to combat the use of ICTs for criminal and terrorist purposes; and to assist in the identification and dissemination of best practices;

(b) Creating and strengthening incident response capabilities, including CERTs, and strengthening CERT-to-CERT cooperation;

(c) Supporting the development and use of e-learning, training and awareness-raising with respect to ICT security to help overcome the digital divide and to assist developing countries in keeping abreast of international policy developments;

(d) Increasing cooperation and transfer of knowledge and technology for managing ICT security incidents, especially for developing countries;

(e) Encouraging further analysis and study by research institutes and universities on matters related to ICT security. Given their specific mandates to support States Members of the United Nations and the international community, States should consider how the relevant United Nations research and training institutes could play a role in this regard.

33. The Group recognized that progress in securing the use of ICTs, including through capacity-building, would also contribute to the achievement of Millennium Development Goal 8, to “develop a global partnership for development”.

VI. Conclusion

34. Progress in international security in the use of ICTs by States will be iterative, with each step building on the last. A technological environment shaped by change and a steady increase in the number of new ICT users make this iterative approach necessary. The present report contains recommendations that build on previous work. Their implementation and refinement will help increase confidence among all stakeholders. The Group recommends that Member States give active consideration to the report and assess how they might take up these recommendations for further development and implementation.

Annex

List of members of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the context of International Security

Argentina
Ambassador Alfredo Morelli
Coordinator, Energy and Technology Unit, Ministry of Foreign Affairs and Worship

Australia
Ms. Deborah Stokes
First Assistant Secretary, Department of Foreign Affairs and Trade

Belarus
Mr. Vladimir N. Gerasimovich
Head, Department of International Security and Arms Control, Ministry of Foreign Affairs

Canada
Mr. Michael Walma
Director, Policy Planning Division, Department of Foreign Affairs and International Trade

China
Mr. Lei Wang (first and second sessions)
Director, Department of Arms Control and Disarmament, Ministry of Foreign Affairs

Ms. Zhihua Dong (third session)
Counsellor, Department of Arms Control and Disarmament, Ministry of Foreign Affairs

Egypt
Dr. Sherif Hashem
Senior Cybersecurity Advisor to the Minister of Communications and Information Technology, Ministry of Communications and Information Technology

Estonia
Mr. Linnar Viik
Acting Director, Estonian IT College

France
Mr. Jean-François Blarel
Deputy Secretary-General, Coordinator for Cyber Affairs, Ministry of Foreign Affairs

Germany
Mr. Detlev Wolter
Head, Directorate of Conventional Arms Control and Confidence and Security Building Measures, Federal Foreign Office

India
Mr. Harsh K. Jain
Joint Secretary and Head,
E-Governance and Information Technology Division,
Ministry of External Affairs

Indonesia
Mr. Febrian A. Ruddyard (first session)
Director for International Security and Disarmament, Ministry of Foreign Affairs

Mr. Andy Rachmianto (third session)
Minister Counsellor of Permanent Mission of Indonesia to the United Nations, New York

Japan
Ambassador Tamotsu Shinotsuka (first session)
Ambassador, International Cooperation for Countering Terrorism, International Organized Crime and Cyber Policy, Ministry of Foreign Affairs

Ambassador Osamu Imai (second and third sessions)
International Cooperation for Countering Terrorism, International Organized Crime and Cyber Policy, Ministry of Foreign Affairs

Russian Federation
Andrey V. Krutskikh
Special coordinator for political affairs in the use of ICTs, Ambassador at Large, Ministry of Foreign Affairs

United Kingdom of Great Britain and Northern Ireland
Mr. Nicholas Haycock
Assistant Director, International Security, Office of Cyber Security and Information Assurance, Cabinet Office

United States of America
Ms. Michele G. Markoff
Deputy Coordinator for Cyber Issues, Office of the Secretary of State, United States Department of State