United Nations A/65/201

General Assembly

Distr.: General
30 July 2010

Original: English

**Sixty-fifth 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 60/45.

* A/65/150.

10-46957 (E) 180810

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

*Summary*

Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. Threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.

The growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Since ICTs are inherently dual-use in nature, the same technologies that support robust e-commerce can also be used to threaten international peace and national security.

The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence, and they can act from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities. Uncertainty regarding attribution and the absence of a common understanding creates the risk of instability and misperception.

There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. The growing sophistication and scale of criminal activity increases the potential for harmful action. While there are few indications of terrorist use of ICTs to execute disruptive operations, it may intensify in the future.

Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. The report of the Group of Governmental Experts offers recommendations for further dialogue among States to reduce risk and protect critical national and international infrastructure.

# Contents

## Foreword by the Secretary-General

A decade ago we could not have foreseen how deeply information technologies and telecommunications would be integrated into our daily lives, or how much we would come to rely on them. These technologies have created a globally linked international community and, while this linkage brings immense benefits, it also brings vulnerability and risk.

Considerable progress has been made in addressing the implications of the new technologies. But the task is arduous and we have only begun to develop the norms, laws and modes of cooperation needed for this new information environment.

With that in mind, I appointed a group of governmental experts from 15 States to study existing and potential threats in this sphere, and to recommend ways to address them. I thank the Chair of the Group and the experts for their diligent and careful work, which has produced this report, a concise statement of the problem and of possible next steps.

The General Assembly has an important role to play in the process of making information technology and telecommunications more secure, both nationally and internationally. Dialogue among Member States will be essential for developing common perspectives. Practical cooperation is also vital, to share best practices, exchange information and build capacity in developing countries, and to reduce the risk of misperception, which could hinder the international community's ability to manage major incidents in cyberspace.

This is a rich agenda for future work. The present report is meant to serve as an initial step towards building the international framework for security and stability that these new technologies require. I commend its analysis and recommendations to Member States and to a wide global audience.

## Letter of transmittal

16 July 2010

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 established in 2009 pursuant to paragraph 4 of General Assembly resolution 60/45. As Chair of the Group, I am pleased to inform you that consensus was reached on the report.

In that resolution, entitled "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 2009, 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, as well as concepts aimed at strengthening the security of global information and telecommunications systems. The Secretary-General was requested to submit a report on the results of that study to the General Assembly at its sixty-fifth session.

In accordance with the terms of the resolution, experts were appointed from 15 States: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, 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 met in four sessions: the first from 24 to 26 November 2009 in Geneva; the second from 11 to 15 January 2010 at United Nations Headquarters; the third from 21 to 25 June 2010 in Geneva; and the fourth from 12 to 16 July at United Nations Headquarters.

The Group had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security. Furthermore, the Group took into account the views expressed in the replies received from Member States in response to General Assembly resolutions 60/45, 61/54, 62/17 and 63/37, respectively entitled "Developments in the field of information and telecommunications in the context of international security", as well as contributions and background papers made available by individual members of the Group.

The Group wishes to express its 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 and Kerstin Vignard. The Group also wishes to express its appreciation to Ewen Buchanan, Information Officer of the Information and Outreach Branch of the Office for Disarmament Affairs of the Secretariat, who served as Secretary of the Group, and to other Secretariat officials who assisted the Group.

(*Signed*) Andrey V. **Krutskikh**
Chairman of the Group

# I. Introduction

1. Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. These threats may cause substantial damage to economies and national and international security. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.

2. Information and communication technologies (ICTs) have unique attributes that make it difficult to address threats that States and other users may face. ICTs are ubiquitous and widely available. They are neither inherently civil nor military in nature, and the purpose to which they are put depends mainly on the motives of the user. Networks in many cases are owned and operated by the private sector or individuals. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Malicious use of ICTs can easily be concealed. The origin of a disruption, the identity of the perpetrator or the motivation can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities.

3. Considering the implications of these developments for international security, the United Nations General Assembly asked the Secretary-General, with the assistance of governmental experts, to study both threats in the sphere of information security and relevant international concepts and to suggest possible cooperative measures that could strengthen the security of global information and communication systems.

# II. Threats, risks and vulnerabilities

4. The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non-State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security.

5. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions.

6. Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future. At the present time terrorists mostly rely on these technologies to communicate, collect information, recruit, organize, promote their

ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for attack.

7. There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception.

8. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. Such proxies, whether motivated by financial gain or other reasons, can offer an array of malicious services to State and non-State actors.

9. The growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services.

10. States are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect the normal, secure and reliable use of ICTs. The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.

11. The varying degrees of ICT capacity and security among different States increases the vulnerability of the global network. Differences in national laws and practices may create challenges to achieving a secure and resilient digital environment.

# III. Cooperative measures

12. The risks associated with globally interconnected networks require concerted responses. Member States over the past decade have repeatedly affirmed the need for international cooperation against threats in the sphere of ICT security in order to combat the criminal misuse of information technology, to create a global culture of cybersecurity and to promote other essential measures that can reduce risk.

13. Over the past decade, efforts to combat the threat of cybercrime have been conducted internationally, in particular, within the Shanghai Cooperation Organization, the Organization of American States, the Asia-Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Economic Community of West African States, the African Union, the European Union, the Organization for Security and Cooperation in Europe and the Council of Europe, as well as through bilateral efforts between States.

14. Non-criminal areas of transnational concern should receive appropriate attention. These include the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to State use of ICTs, which could affect crisis management in the event of major incidents. This argues for the elaboration of measures designed to enhance cooperation where possible. Such measures could also be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability.

15. As disruptive activities using information and communications technologies grow more complex and dangerous, it is obvious that no State is able to address these threats alone. Confronting the challenges of the twenty-first century depends

on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. Therefore, the international community should examine the need for cooperative actions and mechanisms.

16. Existing agreements include norms relevant to the use of ICTs by States. Given the unique attributes of ICTs, additional norms could be developed over time.

17. Capacity-building is of vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security. Close international cooperation will be needed to build capacity in States that may require assistance in addressing the security of their ICTs.

# IV. Recommendations

18. Taking into account the existing and potential threats, risks and vulnerabilities in the field of information security, the Group of Governmental Experts considers it useful to recommend further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions:

(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.

# Annex

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

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

Mr. Aleksandr Ponomarev (third session)
Counsellor of the Permanent Mission of the Republic of Belarus to the United Nations Office at Geneva

Mr. Alexandre Mariano Feitosa
Commander
Brazilian Marine Corps, Brazilian Navy
Policy, Strategy and International Affairs Secretariat
Ministry of Defence
Brazil

Mr. Li Song (first and second sessions)
Deputy Director General
Department of Arms Control and Disarmament
Ministry of Foreign Affairs
China

Mr. Kang Yong (third and fourth sessions)
Deputy Director General
Department of Arms Control and Disarmament
Ministry of Foreign Affairs
China

Mr. Linnar Viik
Associate Professor
Estonian IT College
Estonia

Mr. Aymeric Simon
Relations internationales
Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
France

Mr. Gregor Koebel
Head of the Division for Conventional Arms Control
Federal Foreign Office
Germany

Mr. B. J. Srinath
Senior Director
Indian Computer Emergency Response Team
Department of Information Technology
India

Ms. Rodica Radian-Gordon
Director
Arms Control Department
Ministry of Foreign Affairs
Israel

Mr. Vincenzo Della Corte (first and third sessions)
Director of Communication Security Sector
Presidency of the Council of Ministers
Italy

Mr. Walter Mecchia (second and fourth sessions)
Communication Security Sector
Presidency of the Council of Ministers
Italy

Mr. Rashid A. Al-Mohannadi (first session)
Commander of the Land Forces Signal Company
Amiri Signal Corps
Qatar

Mr. Saad M. R. Al-Kaabi
Lieutenant Colonel (Engineer)
Ministry of Defence
Qatar

Mr. Lew Kwang-chul
Ambassador
Ministry of Foreign Affairs and Trade
Republic of Korea

Mr. Andrey V. Krutskikh
Deputy Director
Department of New Challenges and Threats
Ministry of Foreign Affairs
Russian Federation

Ms. Palesa Banda (first session)
Deputy Director, Internet Governance
Department of Communication
South Africa

Maj. Gen. Mario Silvino Brazzoli
Government Information Technology Officer
Department of Defence
South Africa

Mr. Gavin Willis
International Relations Team
National Technical Authority for Information Assurance (CESG)
United Kingdom of Great Britain and Northern Ireland

Ms. Michele G. Markoff
Senior Policy Adviser
Office of Cyber Affairs
US Department of State
United States of America