United Nations

DISARMAMENT

Study Series

Developments in the Field of Information and Telecommunications in the Context of International Security

Contents

Introduction

The issue of "Developments in the field of information and telecommunications in the context of international security" has been on the United Nations Agenda since 1998 when the Russian Federation introduced a resolution in the First Committee of the United Nations General Assembly that was adopted without a vote.

Since that time there have been annual reports by the Secretary-General to the General Assembly in which United Nations Member States have expressed their views on this important matter and have stressed the need for collective action.

To date, there have been two Groups of Governmental Experts (GGE), the first one held its meetings in 2004 and 2005. The second Group began its work in 2009 and completed its discussions in 2010. Both Groups have examined the existing and potential threats from the cyber-sphere and have been exploring possible cooperative measures to address them. Given the relative "newness" of the cyber-sphere and the complexity of the issues involved, the first Group was unable to reach a consensus on a final report. The second more recent Group was able to agree a successful report issued in 2010.

In his forward to the report of the second GGE, the United Nations Secretary-General, notes that the "General Assembly has an important role to play in the process of making information technology and telecommunications more secure, both nationally and internationally." He adds that "dialogue among Member States will be essential for developing common perspectives," and that "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."

In 2010 the General Assembly unanimously approved a resolution calling for a follow-up to the last Group. Such a GGE which will begin its work in 2012, will continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, taking into account the assessments and recommendations contained in the 2010 Report. The third GGE will report to the 68th session of the General Assembly in September 2013.

This Study Series focuses on the report of the 2009/2010 GGE. It also includes the last two reports of the Secretary-General containing the views of Member States.

Part 1

A/65/201

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.

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.

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

Part 2

Background material

I. A/RES/63/37

Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling 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, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006 and 62/17 of 5 December 2007,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[1]

Bearing in mind also the results of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),[2]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54 and 62/17,

Taking note of the reports of the Secretary-General containing those assessments,[3]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening international meetings of experts in Geneva in August 1999 and April 2008 on developments in the field of information and telecommunications in the context of international security, as well as the results of those meetings,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meetings of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 58/32, established in 2004 a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

---

[1] See A/51/261, annex.

[2] See A/C.2/59/3 and A/60/687.

[3] A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373, A/59/116 and Add.1, A/60/95 and Add.1, A/61/161 and Add.1 and A/62/98 and Add.1.

Taking note of the report of the Secretary-General on the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, prepared on the basis of the results of the Group's work,[4]

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such measures could be served through the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

(*a*) General appreciation of the issues of information security;

(*b*) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(*c*) The content of the concepts mentioned in paragraph 2 above;

(*d*) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to 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 the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

5. *Decides* to include in the provisional agenda of its sixty-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

61st plenary meeting
2 December 2008

---

[4] A/60/202.

II. A/RES/66/24

Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling 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, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009 and 65/41 of 8 December 2010,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,[1]

---

[1] See A/51/261, annex.

Bearing in mind also the results of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),[2]

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25 and 65/41,

Taking note of the reports of the Secretary-General containing those assessments,[3]

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening international meetings of experts in Geneva in August 1999 and April 2008 on developments in the field of information and telecommunications in the context of international security, as well as the results of those meetings,

Considering that the assessments of the Member States contained in the reports of the Secretary-General and the international meetings of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 60/45, established in 2009, on the basis of equitable geographical distribution, a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context

---

[2] See A/C.2/59/3, annex, and A/60/687.

[3] A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1, A/57/166 and Add.1, A/58/373, A/59/116 and Add.1, A/60/95 and Add.1, A/61/161 and Add.1, A/62/98 and Add.1, A/64/129 and Add.1, A/65/154 and A/66/152 and Add.1.

of International Security and the relevant outcome report transmitted by the Secretary-General,[4]

Taking note of the assessments and recommendations contained in the report of the Group of Governmental Experts,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such strategies could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States, taking into account the assessments and 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,[4] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 2 above;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2012 on the basis of equitable geographical distribution, taking into account the assessments and recommendations contained in the above-mentioned report, 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 referred to in paragraph 2 above, and to submit a report on the results of this study to the Assembly at its sixty-eighth session;

5. *Decides* to include in the provisional agenda of its sixty-seventh session the item entitled “Developments in the field of information and telecommunications in the context of international security”.

71st plenary meeting
2 December 2011

---

[4] See A/65/201.

III. A/66/152

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

I. Introduction

1. In paragraph 3 of its resolution 65/41, the General Assembly invited all Member States, taking into account the assessments and 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,[5] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 2 of the resolution;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level.

2. Pursuant to that request, on 16 March 2011, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Any additional replies received will be issued as addenda to the present report.

[5] A/65/201.

II. Replies received from Governments

Australia

[Original: English]
[31 May 2011]

Australia welcomes the opportunity to submit this reply containing our views, pursuant to General Assembly resolution 65/41 on developments in the field of information and telecommunications in the context of international security.

Australia aspires to be a world leader in cybersecurity. We recognize the importance and benefits of the advances in technology to the global digital economy and the security of all nations. Australia aims to maximize economic and security gains for all nations as a result of our expertise.

As technologies have become more pervasive in our lives, Government, business and individuals have become increasingly dependent upon them for a variety of purposes and functions, ranging from online purchasing of goods and services, communicating with others, searching for information and managing finances through to controlling equipment in the mining and manufacturing industries. To maximize the benefits of the Internet and the digital economy, and to enhance cybersecurity around the globe, it is imperative nations work together to achieve a trusted, secure and resilient cyberspace. Australia strives to be a proactive and engaged player in enhancing cyberspace for all users — States, business and individuals.

General appreciation of the issues of information security

Australia recognizes cybersecurity as a top-tier national security priority. The global community continues to experience an increase in the scale, sophistication and successful perpetration of cybercrime. As the quantity and value of electronic information has increased, so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying on their activities.

Confronting and managing these risks must be balanced against individual civil liberties, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realizes the full potential of the digital economy.

Australia's, and each individual nation's, national security, economic prosperity and social well-being are critically dependent upon the availability, integrity and confidentiality of a range of information and communications technologies. In response, the Australian Government has committed significant resources to proactively promote the maintenance of a trusted, secure and resilient electronic operating environment for the benefit of all users.

While the Australian Government's cybersecurity policy is primarily concerned with the availability, integrity and confidentiality of Australia's information and communications technologies, it is coordinated with those of other related policies and programmes such as cybersafety, which is focused on protecting individuals, especially children, from offensive content, bullying, stalking or "grooming" online for the purposes of sexual exploitation.

Efforts taken at the national level to strengthen information security and promote international cooperation in the field

Domestic efforts to strengthen information security

Australia recognizes that it must model best practice domestically to be able to promote international cooperation in cyberspace. Australia has a government-led, integrated approach to protecting and strengthening cybersecurity. In 2009, the Government released its inaugural cybersecurity strategy that articulates the overall aim and objectives of the Australian Government's cybersecurity policy and sets out the strategic priorities that the Australian Government will pursue to achieve these objectives. The strategy also describes the key actions and measures that will be undertaken through a comprehensive body of work across the Australian Government to achieve these strategic priorities.

The aim of Australia's cybersecurity policy is to maintain a trusted, secure and resilient electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy. Key initiatives of the strategy include the establishment of two mutually supporting organizations: a new national computer emergency response team and the Cyber Security Operations Centre. Established in 2010, the computer emergency response team provides a single point of contact for cybersecurity information for all Australians and Australian businesses and ensures that Australian Internet users have access to information on cyberthreats, vulnerabilities in their systems and information on how to better protect their information and communications technologies. The team maintains close working relationships with owners and operators of critical infrastructure and businesses that operate systems important to Australia's national interest. It provides these businesses with targeted information about cybersecurity threats and vulnerability to assist in better protecting their information and communications technologies infrastructure. The operations centre, also established in 2010, provides the Australian Government with all-source cybersituational awareness and an enhanced ability to facilitate operational responses to cybersecurity events of national importance. The Centre identifies and analyses sophisticated cyberattacks and assists in responding to cyberevents across government and critical private sector systems and infrastructure.

A key priority of the strategy is to educate and empower all Australians with the information, confidence and practical tools to protect themselves online. The strategy is guided by the principle of shared responsibility where all users, in enjoying the benefits of information and communications technologies, should take

reasonable steps to secure their own systems, should exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users. To enable individuals to play an active role in information security, it is essential individuals maintain an awareness and understanding of the cyberenvironment and its risks. To achieve this, Australia has an ongoing programme of awareness-raising, which includes a website for cybersecurity information for Australian home users and small businesses, including for those with limited cyberknowledge and skills (see www.staysmartonline.gov.au) and a cybersecurity awareness week conducted in partnership with business, consumer groups and community organizations. The awareness week helps Australians to understand cybersecurity risks and educates home and small business users on the simple steps they can take to protect their personal and financial information online. During the 2010 National Cyber Security Awareness Week around 150 government agencies, industry, community and consumer organizations partnered to deliver events and activities in metropolitan, regional and rural Australia. In 2011, the awareness week was held from 30 May to 4 June.

In acknowledging that the security of cyberspace is a shared responsibility, the Australian Government has worked proactively with the Internet Industry Association to develop an innovative voluntary Internet service provider cybersecurity code of practice (the "icode"), which commenced in December 2010. The code provides a consistent approach for Australian Internet service providers to help inform, educate and protect their clients in relation to cybersecurity issues. Australia has presented on the successful implementation of the code and shared its lessons learned from developing this code in multilateral forums. Presentations have been made in the Organization for Economic Cooperation and Development (OECD) Working Party on Information Security and Privacy in December 2010, the Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group and the Asia-Pacific Telecommunity. Australia is eager to share this code with other States, through bilateral capacity-building exercises and multilateral forums, to assist other States in better collaborating with Internet service providers and to make those providers more responsible for educating and protecting end-users.

Promotion of international cooperation

Australia gives high priority to international cooperation on cybersecurity. Given the transnational nature of the Internet, in which effective cybersecurity requires coordinated global action, Australia has adopted an active, multilayered approach to international engagement. This includes, among other things, engaging with foreign Governments and organizations bilaterally and via multilateral forums to help promote international best practice, share lessons, build capacity and foster a coordinated global approach to combating cybersecurity threats.

Australia's involvement in the United Nations includes co-sponsoring resolutions on the creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, and on developments in the field of information and telecommunications in the context of international security. Australia has also responded to General Assembly resolution 64/211 by providing input on best practices for the protection of critical information infrastructure, including information and communications technologies, with a view to promoting global improvement in cybersecurity. Australia is a member of the International Telecommunication Union (ITU), and contributes to study groups under the Standardization and Development sectors. Australia provides funding to the Development sector for capacity-building work in the Asia and Pacific region, including cybersecurity initiatives. Australia is an active contributor to and the previous Chair of the OECD Working Party on Information Security and Privacy, and currently a volunteer country for the Working Party's comparative analysis of cybersecurity strategies. Australia was an integral leader in the development and implementation of the Seoul-Melbourne Anti-Spam Agreement on cooperation between Asia-Pacific nations in countering spam and the London Action Plan, which is the pre-eminent international enforcement and cooperation network for combating spam.

Australia enjoys a collaborative relationship and is committed to working with its regional partners. We are closely engaged with other countries in our region in building capacity to achieve a trusted, resilient and secure cyberspace. Australia participates in activities of the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL) and the Association of Southeast Asian Nations (ASEAN) Regional Forum work on cybersecurity. Australia is the deputy convenor for the APEC TEL Security and Prosperity Steering Group. Australia is currently seeking to co-lead the cyberterrorism and transnational crime core area under the ASEAN Regional Forum workplan.

At an operational level, the computer emergency response team maintains close working relationships with national computer emergency response team organizations around the globe. In Australia, the team actively participates in and facilitates trusted and timely information sharing on a global level, including threat and vulnerability information, to ensure the maintenance of situational awareness and a consistent and coordinated global response to online threats. The team actively contributes to capacity-building initiatives, particularly in the Asia-Pacific region, including through its membership of the Asia-Pacific Computer Emergency Response Team. Recognizing that information security is not geographically limited, the team also works closely with other partners through its membership of the Forum of Incident Response and Security Teams and the International Watch and Warning Network.

Possible measures that could be taken by the international community to strengthen information security at the global level

All States, including Australia, need to continue to seek out both traditional and innovative measures to strengthen information security. The global challenge of cybersecurity requires an increased effort in multilateral forums to improve the security of interoperable networks. This includes efforts within the United Nations and the ITU, regional forums such as APEC and more subject specific international groups such as the Forum of Incident Response and Security Teams and the International Watch and Warning Network.

Australia supports the development of international principles of responsible behaviour in cyberspace, including agreeing a broad set of principles for normative behaviour in cyberspace that will facilitate better international cooperation and promote trust in cyberspace and lead to the development of agreed international norms on cyberspace. Australia, as a member of the global community, will continue to support progress on this issue through bilateral and multilateral forums to help achieve a more secure, resilient and trusted cyberenvironment.

Specific efforts that could be taken by the international community to strengthen information security at the global level include:

(a) The development of global standards, including agreement to a broad set of international principles for normative behaviour in cyberspace to facilitate better international cooperation and promote trust;

(b) Expansion of the international legal system's capacity to combat cybercrime, including consistency in legal frameworks (for example, wider accession to the Council of Europe Cybercrime Convention, the requirements of which Australia anticipates to meet by the end of 2011), and enhancing law enforcement cooperation to allow countries to effectively institute domestic law;

(c) The development and promotion of best practice in situational awareness and strategic warning and event response, including the development of national computer emergency response teams to conduct and coordinate these activities between all nations;

(d) Awareness-raising initiatives and capacity-building exercises by experienced and established States to assist developing States to achieve a trusted, secure and resilient cyberspace for the benefit of all;

(e) A more consistent approach to partnering with industry to develop guidelines around conduct in cyberspace, for example, the Australian Internet industry code of practice.

Relevant international concepts

Existing international law provides a framework for protection from information security threats arising from a variety of actors. A range of existing

international legal principles may be applicable to the use of cyberspace, including the principles of sovereign equality of States and the prohibition on the use of force and acts of aggression, as well as international humanitarian law. Further discussion among States, in international and regional forums, is necessary to determine more precisely the scope and applicability of these principles to threats emanating from the cyber realm.

Georgia

[Original: English]
[1 June 2011]

In the context of Georgia, the information security issues were given particular attention after August 2008, when the Russian Federation carried out a heavy distributed denial-of-service attack against Georgia.

Given the assessment of these events and under the recent rapid and large-scale development of e-governance projects and services, information security has become one of the significant aspects of the national security concept. For the improved regulation of information security, the Government of Georgia has been carrying out a number of significant initiatives in recent years.

In 2010, a legal entity, the Data Exchange Agency, was established under the Ministry of Justice of Georgia, which is directly responsible for the development and implementation of information security policy in the Government sector. With the establishment of the Data Exchange Agency, the Government of Georgia has developed the institutional mechanism for coordinated realization of e-governance and information security.

The Data Exchange Agency, within the framework of functions provided for by the law and its own charter, cooperates with the Ministry of Justice of Georgia in pursuing and introducing of an information security policy, which should conform to International Organization for Standardization (ISO) 27000 standard. The Agency also coordinates the enforcement and introduction of either mechanisms or standards necessary for information security in the State and business sectors, particularly by carrying out activities of various levels of significance. Out of these events, one the most important is the annual Georgian information technology innovations conference, the agenda of which always deals with information and cybersecurity; the conference also has the mandate of the Agency to develop and carry out the policy of public awareness enhancement regarding information and cybersecurity issues.

In the context of everyday cybersecurity, the Data Exchange Agency is responsible for the establishment and operation of the computer emergency response team, which currently is functioning at the Agency with a view to managing the information security incidents in Georgia's cyberspace. The Agency

also monitors the functioning of the Georgian governmental network for the safeguarding of its security.

The functions of the Agency, in the context of information and communication technologies, also provide for raising the levels of professional education (in order to train information security specialists), preparing proposals, monitoring security and issuing digital signature certificates. Given the sphere of professional education, the Agency plans to carry out a number of special projects with the help of international donors (such as the European Union (EU) and the World Bank). These projects will ensure the appropriate level of professional education; as for digital signature security, the Agency will perform this function upon the beginning of issuance of citizens electronic identity cards (bearing digital signatures) by the Civil Registry Agency.

Besides the activity of the Data Exchange Agency, which is the leading and coordinating agency for information security, one should underline other initiatives carried out currently by the Government of Georgia, in which the Data Exchange Agency is actively engaged:

(a) The expert working group, which is working on the cybersecurity strategy and action plan (defined concretely in the next part), has been established under the National Security Council of Georgia;

(b) A number of legislative initiatives have been developing, including the administrative law and the law regulating State secrets, which are planned to be initiated at the Parliament of Georgia in 2011. One should make special mention of the Bill on information security, which is currently being developed by the Data Exchange Agency and is to be submitted for consideration by the Parliament in 2011;

(c) In 2010, the Ministry of Justice and the Ministry of Finance of Georgia, with the help of the Agency, developed and are now introducing information security internal regulations (policy and guidelines). Similar initiatives are also expected to be implemented in other governmental institutions.

Germany

[Original: English]
[6 June 2011]

The security situation in cyberspace has fundamentally changed over recent years. On the one hand, we can see a technology-driven process of innovation at work, as more and more business processes are managed electronically and interconnected, sometimes directly or indirectly connected to the Internet. Information technology systems are constantly becoming more complex. Innovation cycles are getting shorter and shorter. On the other hand, organized crime and other non-state actors are attacking information technology networks,

databases and websites. In some cases, these attacks are having impacts that have not yet been realistically assessed.

For this reason, in February 2011 the Federal Government adopted a new cybersecurity strategy. The core of the strategy is critical infrastructure protection. All Government authorities that deal with cybersecurity issues are to work closely and directly with each other and with the private sector within a new cyber response centre to rapidly detect and analyse major information technology incidents and recommend protective measures. With regard to policy, the new Cyber Security Council at the State secretary level addresses key cybersecurity issues and Germany's position on them.

This includes coordinating cyber foreign policy, including aspects of foreign, defence, economic and security policy. International interconnections in cyberspace mean that coordinated action at the international level is essential. Within the EU and in international organizations, Germany will therefore strongly advocate greater cybersecurity.

In its cybersecurity strategy, in view of the global interconnection of information technology, Germany advocates developing broad, non-contentious, politically binding norms of State behaviour in cyberspace. They should be acceptable to a large part of the international community and should include measures to build trust and increase security.

Confidence and security-building measures in cyberspace

Cyberspace is a public good and a public space. As such we have to consider cyberspace security in terms of the resilience of infrastructure as well as the integrity and failure safety of systems and data. Being a public space, States have to promote security in cyberspace, particularly regarding security against crime and malicious activities, by protecting those who choose to use authenticity tools against identity theft and securing the integrity and confidentiality of data and networks.

Cyberspace is global by nature. Ensuring cybersecurity, enforcing rights and protecting critical information infrastructures require major efforts by the State both at the national level and in cooperation with international partners.

Against this backdrop, Germany is ready to work on a set of behavioural norms addressing State-to-State behaviour in cyberspace, including, in particular, confidence, transparency- and security-building measures, to be signed by as many countries as possible.

Germany outlined possible elements of such a code of conduct on international norms recently at the Organization for Security and Cooperation in Europe (OSCE) conference on cybersecurity, held on 9 and 10 May 2011, as follows:

(a) Confirm the general principles of availability, confidentiality, competitiveness, integrity and authenticity of data and networks, privacy and protection of intellectual property rights;

(b) Respect the obligation to protect critical infrastructures;

(c) Enhance cooperation aiming at confidence-building, risk reducing measures, transparency and stability by:

- Exchanges of national strategies, best practices and national perceptions referring to the international regulation of cyberspace;
- The exchange of national views of international legal norms pertaining to the use of cyberspace;
- The setup and notification of points of contact;
- The setup of early warning mechanisms and the enhancement of cooperation between computer emergency response teams;
- The upgrade of crisis communication links to encompass cyberincidents, the support of the development of technical recommendations that advance robust and secure global cyberinfrastructures;
- The responsibility to combat terrorism comprising the exchange of practices and enhanced cooperation to address non-State actors;
- The support of cybersecurity capacity-building in developing countries, and the development of voluntary measures for cybersecurity support to large-scale events (e.g. the Olympic Games).

Moreover we see the necessity to start a debate on an international cooperation in the framework of attribution of cyberattacks, which are usually very difficult to trace, State responsibility for cyberattacks launched from their territory when States do nothing to end such attacks despite being informed about them and States' responsibility not to facilitate areas of lawlessness in cyberspace, for example by knowingly tolerating the storage of illegally collected personal data on their territory.

Military aspects of cybersecurity

As military forces increasingly rely on information technology to master ever more complex scenarios at all levels of command, the protection of the information and the means to process it has become a first order task.

However, in military thinking, information security is challenged not only by a potential adversary, in an operational understanding, using weaponry for the physical destruction of information infrastructure, but also by irresponsible users, malfunctioning technology, criminals or simply accidents.

Hence, the efforts to be undertaken range from awareness-raising of each single user and securing the trustworthiness of the supply chain for information technology, to responsive defences to fend off cyberattacks and an overall resilient information technology architecture.

In essence, a comprehensive risk management is required, with measures to strengthen information security on a national and global scale.

At an early stage, the German armed forces (Bundeswehr) established resilient command and control architectures, security techniques and procedures as well as an information technology-security organization, encompassing all branches of the armed forces, and including an independent computer emergency response team with the capacity to intervene in case of critical disruptions to the operations of information technology. Adapting personal and technical abilities to the continually increasing level of threat is a perpetual task.

The German armed forces are collaborating closely with the Federal German Ministry of the Interior in its efforts and strongly support the strengthening of information security in the North Atlantic Treaty Organization (NATO) and the EU and the formation of policies and capacities to this end. Furthermore, the armed forces hold regular exchanges with a number of countries in the context of information security, both at the policy and working levels.

The German armed forces welcome initiatives and work together with other departments of the Federal German Government on international motions to further protect the utility of worldwide information networks, for example, the development of a voluntary international code of conduct in cyberspace.

Cyberdefence in NATO

Cybersecurity has been identified by NATO as one of the key emerging security challenges. The Strategic Concept adopted by Heads of State and Government at the NATO Summit, held in November 2010, in Lisbon, states that "cyber attacks ... can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability".

Heads of State and Government tasked the North Atlantic Council, in the Summit Declaration, "to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyberdefence policy by June 2011 and to prepare an action plan for its implementation".

As a first step to the new policy, NATO Defence Ministers adopted a concept on cyberdefence in March 2011.

The concept focuses on the protection of NATO networks and national networks of member States that are connected to NATO networks or process NATO information (including the development of common principles and criteria to ensure a minimum level of cyberdefence in all member States). To reduce the

global risks emanating from cyberspace, NATO intends to cooperate with partner nations, relevant international bodies such as the United Nations and the European Union, the private sector and academia.

Germany welcomes NATO commitment regarding cybersecurity and actively supports the discussions.

Cybersecurity in the Organization for Security and Cooperation in Europe

The Organization for Security and Cooperation in Europe has been discussing cybersecurity issues for several years. At the OSCE Summit held in 2010, in Astana, the Heads of State and Government of the 56 participating States of the OSCE underlined that ''greater unity of purpose and action in facing emerging transnational threats" must be achieved. The Astana Commemorative Declaration mentioned cyberthreats as one of these emerging transnational threats.

Germany actively participated in the OSCE conference on a comprehensive approach to cybersecurity: "Exploring the future OSCE role", held on 9 and 10 May 2011, in Vienna. In the course of the conference, concrete recommendations for OSCE follow-up activities were discussed.

Germany will continue to actively support OSCE discussions on exploring the future OSCE role in the field of cybersecurity.

Greece

[Original: English]
[6 June 2011]

Information security issues have been more extensively addressed than in the past. Counter-measures to the threats inherent in the current globalization of networks and systems are being considered. Measures to preserve the free flow of information are studied and applied in both the national and international contexts.

Current international and multinational concepts are followed and studied. International guidance on risk assessment is needed. Cyberdefence should also be addressed. National sovereignty rights regarding information security in global information sharing should be maintained.

It is understood that all Member States should continue to inform the Secretary-General of their views and assessments on the corresponding questions. In this respect the following points are noted:

(a) All information security-related issues are given high priority;

(b) Ways to preserve the free flow of information and provide for the required degrees of confidentiality, integrity and availability are studied and applied across national and international boundaries;

(c) The concepts for the interconnection of networks that provide for capabilities enabled and shared at both the national and international levels should be drafted and agreed. Risk assessment for the interconnection of networks must prevail and relevant international guidance should be available. Further to that, and since a very serious concern for every nation has been the need to take measures for its cyberdefence, coherent international guidance is needed for cooperation, efficiency and economy. Last but not least, the requirement for a nation to preserve its sovereignty and maintain its own base of information cannot be overlooked and every concept drafted should account for that;

(d) Possible measures to be taken by the international community to strengthen information security at the global level are the following:

(i) Relevant international concepts should be detailed and agreed;

(ii) A guidance plan for a harmonized generic infrastructure, covering basic legislation matters, could be proposed, in order to deliver the required information security for the electronic handling of all correspondence and messaging, providing multiple ways of communication;

(iii) Concepts followed by multinational alliances and groupings of small nations should be harmonized and expanded to be applicable at the global level. The agreement to specify the threat and its negative effect on humanity could be more important than the engineering of any sophisticated measures devised, since they could also be used by adversaries;

(iv) In parallel to all of the above, the nation's sovereignty should be understood to be the basic reference for every attempt of globalization. An international concept for defining the national information exchange gateways, with scenarios reflecting the desired level of integration, should be drafted and used as a guide, for all efforts at the national, multinational and international levels.

Kazakhstan

[Original: Russian]
[7 June 2011]

In 2010, the Republic of Kazakhstan set up a computer emergency response team to ensure cybersecurity for information and communications technologies.

In this connection, any information received from Kaznet users on viruses, security codes, bot systems or violations of legal requirements (pornography, violence, copyright infringements and so on) detected in the kz domain or on sites

hosted by Kazakhstan is sent to the computer emergency response team for analysis.

Netherlands

[Original: English]
[6 June 2011]

General appreciation of the issues of information security

The Netherlands supports safe and reliable information and communications technologies and the protection of an open, free Internet and respect for human rights. Safe and reliable information and communications technologies are essential for our prosperity and well-being and serve as a catalyst for sustainable economic growth.

Information and communications technologies offer opportunities, but also make our society more vulnerable. The cross-border nature of threats makes international cooperation crucial. Many measures will be effective only if implemented or coordinated internationally. In this connection, the Netherlands attaches great importance to public-private partnerships and individual responsibility on the part of all users of information and communications technologies.

Efforts taken at the national level to strengthen information security and promote international cooperation in the field

The Netherlands is working nationally and internationally for a secure digital environment. At the national level, in February 2011, the Dutch Government presented a national cybersecurity strategy, entitled “Strength through cooperation”. In July 2011, as part of the strategy, the Government will establish a national cybersecurity council to ensure a collaborative approach between the public sector, the private sector and academic and research institutions. The Government will also establish a national cybersecurity centre to identify trends and threats and help manage incidents and crises. A major task of the centre will be to conduct cyberthreat analyses based on information from public and private parties. The centre will include the existing Government computer emergency response team.

Internationally, the Netherlands contributes actively to the efforts of EU, NATO, the Internet Governance Forum, ITU and other partnerships. The Netherlands promotes practical cooperation between cybersecurity centres (including computer emergency response team organizations) and a strengthening of the International Watch and Warning Network. The rapid growth in cybercrime calls for effective enforcement to maintain confidence in the digital society. As to enforcement, the Netherlands aims to encourage more cross-border investigation with enforcement agencies from other European countries, and beyond. The

Netherlands is a party to the Council of Europe's Convention on Cybercrime and encourages others to accede to this convention.

Possible measures that could be taken by the international community to strengthen information security at the global level

The Netherlands realizes the importance of continuing dialogue on the development of standards of State behaviour aimed at the safe use of cyberspace. It is keen to contribute actively to this dialogue. The Netherlands' starting point is an open Internet that promotes innovation, stimulates economic growth and safeguards fundamental freedoms.

The Netherlands attaches great importance to involving the private sector and knowledge institutions in this dialogue and is keen to share experience and best practices with others. The intensive international exchange of knowledge and information among all stakeholders and organizations is essential for making cyberspace more secure and reliable. Consistency in the application of existing international legal frameworks is another important issue meriting international attention.

United States of America

[Original: English]
[7 June 2011]

I. Introduction

Information and communications technologies are crucial to the development of all Member States. Linked together to create a cyberspace, these technologies help to realize the common vision of an information society as envisaged at the World Summit on the Information Society, held in 2003 and 2005. Information and communications technologies contribute to the essential functions of daily life, to commerce and the provision of goods and services, research, innovation, entrepreneurship, and to the free flow of information among individuals, organizations and Governments. They are a powerful new tool, allowing e-government, promoting economic development, facilitating the delivery of humanitarian assistance and enabling critical civil, public safety and national security infrastructures. Moreover, the promise that networked communications offer to reduce barriers to international understanding and cooperation cannot be overstated.

Even as reliance on information and communications technologies grows, risks associated with this dependency grow as well. A diverse range of events and activities, natural and man-made, threaten the reliable functioning of critical national infrastructures, global networks and the integrity of the information that

travels over or is stored within them. Man-made threats are increasing in number, sophistication and gravity. Some are State-based, but many come from non-State actors and involve criminal or terrorist activity. Motivations vary, from the theft of money or information, or the disruption of competitors, to nationalism and the extension of traditional forms of State conflict into cyberspace. These threat actors target individuals, corporations, critical national infrastructures and Governments alike, and their effects carry significant consequences for the welfare and security of individual nations and the globally linked international community as a whole.

Whatever national steps Governments may take domestically to protect their information networks, international collaboration on strategies to reduce risks to information and communications technologies is essential to ensure the security of all. Governments must have confidence that the networks that support their national security and economic prosperity are safe and resilient. Achieving a trusted infrastructure for information and communications technologies will ensure that all achieve the potential of the information revolution.

That task will not be easy. The international community faces the challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity and free trade while also promoting safety, security, civil liberties and privacy rights. The difficulty of the task is compounded by the unique attributes of information and communications technologies. Accessible to all, networks are often owned and operated by the private sector, rather than by Governments. Unlike traditional weapons, disruptive information technology tools are stealthy and cannot be seen. Their use can be routed through many nations, with the origin, identity and sponsorship of the perpetrator difficult to determine. Increasingly, non-State actors are developing capabilities that raise the possibility of States or non-State actors using proxies to engage in disruptive activities in cyberspace. These attributes make traditional strategies, such as measures similar to those used for arms control, ineffective in controlling or constraining threat actors and therefore, creative new approaches are required to mitigate the risks. Notwithstanding the difficulty of the task, Member States must unite in the common goal of preserving and enhancing the contribution that information technologies make by assuring their security and integrity.

The tasks of Member States are twofold: domestic and international. Securing national information infrastructures is a responsibility Governments must lead on domestically, in coordination with relevant civil society stakeholders. At the same time, domestic efforts should be supported by international collaboration on strategies that address the transnational nature of the various threats to networked information systems. These efforts should include cooperation on incident management, mitigation and response; transnational criminal investigation and prosecution; technical recommendations to improve the robustness of cyber infrastructure; and affirmation of internationally shared norms of behaviour supported by confidence-building measures designed to enhance stability and reduce risks of misperception.

II. Threats, risks, vulnerabilities

Threats to the network of systems that together constitute cyberspace, and the information that travels over them, is one of the serious global challenges of the twenty-first century. State and non-State actors can target ordinary citizens, commerce, critical industrial infrastructures and Governments through information and communications technologies. The convergence between information and communications technologies, the Internet and other infrastructures creates unprecedented opportunities to cripple telecommunications, electrical power, pipelines and refineries, financial networks and other critical infrastructures.

The unique characteristics of information technology facilitate its use for disruptive activities and severely challenge Governments that seek to reduce risk. Unlike traditional military technologies, the networks that constitute cyberspace are not the monopoly of Governments, but are in many cases owned and operated by the private sector. Information technology itself is a widely available technology that is neither inherently civil nor military in nature, where its use depends exclusively on the motivation of the user.

Software tools used for disruption, at least in their basics, are freely available to all. More sophisticated approaches can be developed by anyone with the requisite skill. Moreover, these tools evolve rapidly to take advantage of newly discovered vulnerabilities. Such tools are not visible in the conventional sense, are quite stealthy and may have latent "signatures" that can be easily mimicked. Because of the nature of the Internet, malicious code can be routed through many national territories before delivery to target, making identification of their origin onerous, time-consuming and often requiring substantial transnational cooperation. Even if their origin is discovered, the identity of the perpetrator or the sponsors can remain elusive. Consequently, malicious actors can and do operate in secrecy, with substantial impunity, from virtually anywhere on the planet.

This obscurity of identity is compounded by an obscurity of the motive underlying an intrusion in cyberspace. Organized criminals and other individuals or groups may act to advance their own interests but also can be enlisted to serve as proxies by both State and non-State actors alike. The lack of timely, high-confidence attribution and the possibility of "spoofing" can create uncertainty and confusion for Governments, thus increasing the potential for crisis instability, misdirected responses and loss of escalation control during major cyberincidents.

The primary actors that together constitute threats to the reliable functioning of cyberspace include:

(a) **Criminals**. Many of the malicious tools originate in the entrepreneurial efforts of organized criminals and hackers. The growing sophistication and scope of criminal activity highlight the potential for malicious activity in cyberspace to affect national competitiveness, to cause a general erosion of trust in the use of the Internet for commerce and trade, even to cripple civil infrastructure. The volume and scope of such activities are increasing;

(b) **States**. There is increased anecdotal public reporting that States are developing and using capabilities that extend traditional forms of state conflict into, using, or through cyberspace. However, conclusive evidence regarding the source or intentions behind events commonly assumed to be State-sponsored remains elusive. As is often the case, the identity and motivation of the perpetrator(s) can only be inferred from the target, effects and other circumstantial evidence surrounding an incident;

(c) **Terrorists**. Terrorist capability to compromise information networks or to execute operations with physical effects through the use of information and communications technologies is currently lacking, although the possibility that such capabilities may emerge in the future cannot be ruled out. Most experts agree that, currently, terrorists rely on information and communications technologies to recruit, to organize and to solicit funding. Specific threats arising from terrorist use of the Internet may include use of the Internet for organizing and carrying out a specific kinetic terrorist attack;

(d) **Proxies**. Of increasing concern are individuals or groups who engage in malicious online activities on behalf of others, whether State or non-State actors, for financial gain or for nationalist or other political motivation. So-called "bot-masters" are reported to offer various malicious services to the highest bidder. The unique attributes of information technology offer a high degree of anonymity to such actors and effectively obscure any relationship to a sponsor, offering the sponsor plausible deniability.

The challenges States face in addressing such threats are formidable. The attributes of information and communications technologies mean that the actions of each of these threat actors are likely visible only in their effects. Thus, high-confidence attribution of identity to perpetrators cannot be achieved in a timely manner, if ever, and success often depends on a high degree of transnational cooperation. The increasing role of proxies further complicates the process of attribution, as an affected party must identify not only the perpetrator but also the sponsor, promising to make this challenge even more troublesome in the future.

Such challenges require that national Governments organize and lead domestic efforts to develop and deploy resilient, layered defences for communications and information infrastructures, regardless of the source of the threat. At the same time, the complex transnational nature of these threats requires international collaboration on strategies to address risks on a global basis.

III. Principles, rules and norms of behaviour

A. Responsibilities of States in assuring cybersecurity

Over the past decade, Member States have recognized their national responsibility to take systematic domestic steps to defend themselves from cybersecurity threats and have affirmed the need for international cooperation. Five General Assembly resolutions have drawn attention to essential defensive measures

that Governments can perform to reduce risks to their security. While intended to raise awareness, these resolutions nonetheless advance some useful norms for individual and State behaviour in the interest of cybersecurity:

(a) Resolution 55/63 on combating the criminal misuse of information technologies, in which the General Assembly underscores the need to have modern effective national laws to adequately prosecute cybercrime and facilitate timely transnational investigative cooperation;

(b) Resolution 56/21, in which the General Assembly specifically notes the work of international and regional organizations in combating high-technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime:

> There has been intensive activity by the United Nations and other organizations in this area. United Nations organizations that principally focus on criminal misuse of the Internet include the United Nations Office on Drugs and Crime, the Commission on Crime Prevention and Criminal Justice, the United Nations Congress on Crime Prevention and Criminal Justice, the International Telecommunication Union and others;

(c) Resolution 57/239, in which the General Assembly affirms the need for the creation of a global culture of cybersecurity, recognizes the responsibility of Governments to lead all elements of society to understand their roles and responsibilities with regard to cybersecurity, and highlights complementary elements that all participants in the information society must address;

(d) Resolution 58/199, in which the General Assembly focuses in particular on actions that Member States should consider in their efforts to create a global culture of cybersecurity and to protect critical information infrastructures. These too can be considered a set of norms to which Governments should ascribe, and they provide an essential basis or precursor in order to facilitate international collaboration on risk reduction;

(e) Resolution 64/211, in which the General Assembly invited all Member States to take detailed stock of their national cybersecurity efforts to date, in the above areas as well as others, using an annexed self-assessment tool, and to share those successful measures and best practices that could assist other Member States in their efforts.

B. Norms applicable in the context of hostilities

Despite the unique attributes of information and communications technologies, existing principles of international law serve as the appropriate framework within which to identify and analyse the rules and norms of behaviour that should govern the use of cyberspace in connection with hostilities. There are two distinct but related bodies of law to consider in this regard: *jus ad bellum* and *jus in bello*. The

first provides the framework for considering whether an incident in cyberspace rises to the level of a use of force triggering a nation's right to self-defence. The second provides the framework for identifying the rules governing the use of cyberspace in the context of an armed conflict.

Jus ad bellum. Much of the legal framework governing the use of force and self-defence is derived from three provisions of the Charter of the United Nations:

(a) Article 2(4) of the Charter provides that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state …";

(b) Article 39 of the Charter establishes the Security Council as the arbiter of whether a threat to the peace, breaches of the peace, or acts of aggression have occurred, and charges the Security Council with making recommendations or decisions as to what measures under Articles 41 or 42 of the Charter are appropriate in response;

(c) Article 51 of the Charter recognizes and reinforces the principle that "[n]othing in the present Charter shall impair the right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".

It may be difficult to reach a definitive legal conclusion as to whether a disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defence. For example, where the threat actor and the motive are unknown, and effects result that do not directly cause substantial death or physical destruction, it may be possible to reach differing conclusions about whether an armed attack has occurred. However, such ambiguities and room for disagreement do not suggest the need for a new legal framework specific to cyberspace. Instead, they simply reflect the challenges in applying the Charter framework that already exists in many contexts. Nevertheless, under some circumstances, a disruptive activity in cyberspace could constitute an armed attack. In that context, the following established principles would apply:

(a) The right of self-defence against an imminent or actual armed attack applies whether the attacker is a State actor or a non-State actor;

(b) The use of force in self-defence must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced;

(c) States are required to take all necessary measures to ensure that their territories are not used by other States or non-State actors for purposes of armed activities, including planning, threatening, perpetrating or providing material support for armed attacks against other States and their interests.

Jus in bello. The law of armed conflict set forth the rules, known as *jus in bello*, that apply to the conduct of armed conflict, including the use of information technology tools in the context of an armed conflict. In particular, the following key principles of the law of armed conflict would play an important role in judging the legality of cyberattacks during an armed conflict:

(a) The principle of distinction requires attacks to be limited to legitimate military objectives and that civilian objects shall not be the object of attack;

(b) The prohibition on indiscriminate attacks includes a prohibition on attacks that employ a means or method of warfare that cannot be reasonably directed at a specific military objective;

(c) The principle of proportionality prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects, which would be excessive in relation to the concrete and direct military advantage anticipated.

These principles prohibit attacks on purely civilian infrastructure, the disruption or destruction of which would produce no meaningful military advantage. In addition, the potential for collateral damage would have to be assessed before attacking a military target. In other words, targeting analysis would have to be conducted for information technology attacks just as it traditionally has been conducted for attacks using kinetic (conventional and strategic) weapons.

While the principles above are well-established and apply in the context of cyberspace, it is also true that interpreting these bodies of law in the context of activities in cyberspace can present new and unique challenges that will require consultation and cooperation among nations. This is not unusual. When new technologies are developed, they often present challenges for the application of existing bodies of law.

C. The use of proxies

The use of proxies to conduct disruptive operations is an example of an area where the unique attributes of information and communications technologies present new challenges for States. Acting through proxies significantly increases States' ability to engage in attacks with plausible deniability. While existing international law has provisions governing the use of mercenaries, the use of proxies in cyberspace raises new and significant issues with wide-ranging implications. States will need to work together to develop effective solutions to this problem.

D. Responsibility to allow free flow of information

The rights to freedom of expression and the free flow of information are embodied in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which generally provide, subject to certain

limitations, that everyone has the right to freedom of expression, including the freedom to hold opinions without interference and to seek, receive and impart information through any media and regardless of frontiers. These principles have been affirmed in numerous international forums, including the General Assembly, the International Telecommunication Union and the World Summit on the Information Society, among others.

E. Responsibility to combat terrorism

At least 16 existing Security Council resolutions call on States to combat terrorism. These obligations apply fully when terrorists or terrorist facilitators use cyberspace to recruit, raise funds, move money, acquire weapons or plan attacks. All States are obliged to share information about, and to take action against, online terrorist financing, recruitment, planning and facilitation activities, while respecting the sovereignty of other States and their own responsibilities to allow the free flow of information.

IV. Transparency, stability and risk reduction and cooperative measures

As outlined above, Member States face the challenge of managing a highly varied and complex threat environment. Over the last decade, extensive efforts to combat the threat of cybercrime have been conducted internationally. Efforts in training in the investigation and prosecution of cybercrime have been taken up in the Organization of American States, the Asia-Pacific Economic Cooperation, the Economic Community of West African States, the African Union and the Council of Europe, among others. Extensive international cooperation in the investigation and prosecution of cybercrime has been accomplished through the Convention on Cybercrime, as well as through bilateral efforts between affected countries, and continues to be the most effective way of dealing with the threat to information and communications technologies by criminal activity.

Other areas of transnational concern have yet to receive similar attention. These include risks of misperception resulting from a lack of shared understanding regarding international norms pertaining to State behaviour in cyberspace, which could affect crisis management in the event of major cyberevents. This argues for the elaboration of measures designed to enhance cooperation and build confidence, reduce risk or enhance transparency and stability:

Transparency measures

- Exchanges of national cybersecurity strategies and best practices (lessons learned)
- Exchanges of national views of international norms governing the use of cyberspace
- Exchanges of national organizational structures devoted to cybersecurity and points of contact.

Stability and risk reduction measures

- Establishing or upgrading communications links and associated protocols to encompass cyberincidents
- Enhancing cooperation to address organized non-State actors (criminals, terrorists, proxies)
- Establishing procedures to permit routine exchange of information between national computer security incident response teams.

Cooperative measures

- Support cybersecurity capacity-building in less developed nations

IV. A/65/154

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

I. Introduction

1. In paragraph 3 of its resolution 64/25, the General Assembly invited all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 2 of the resolution;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level.

2. Pursuant to that request, on 26 February 2010, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Any additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

Cuba

[Original: Spanish]
[27 May 2010]

1. Cuba fully shares the concern expressed in General Assembly resolution 64/25 with respect to the use of information technologies and media for purposes incompatible with international stability and security and which adversely affect the

integrity of States, to the detriment of their security in the civilian and military spheres. This resolution also appropriately stresses the need to prevent the use of information resources and technologies for criminal or terrorist purposes.

2. Cuba reiterates that the hostile use of telecommunications with the declared or hidden intent of undermining the legal and political order of States is a violation of the internationally recognized norms on this subject and a negative and irresponsible use of such means, which may give rise to tension and situations that are not conducive to international peace and security and thereby undermine the principles and purposes enshrined in the Charter of the United Nations.

3. Cuba draws attention with concern to the fact that information and telecommunication systems may be turned into weapons when they are designed and/or used to damage the infrastructure of a State and, as a result, may endanger international security and peace.

4. In this regard, Cuba reiterates its condemnation, already expressed in various international forums, of the aggressive escalation by successive United States administrations of their radio and television war against Cuba, in clear violation of the international rules in force governing the radio-electric spectrum.

5. The United States Government did not care about the damage which it might cause to international peace and security by creating dangerous situations, such as the use of a military aircraft to transmit television signals to Cuba without its agreement.

6. The radio-electric aggression against Cuba from United States territory violates the principles of international law governing relations between States and the norms and regulations of the International Telecommunication Union (ITU), which establish the conduct to be adopted by member countries of that specialized agency of the United Nations system.

7. Each week, broadcasters located in United States territory transmit thousands of hours of radio and television programmes on 34 different medium-wave, short-wave, FM and TV frequencies. In March 2010, there were 2,156 hours of illegal transmissions each week. Several of these broadcasters belong to or offer their services to organizations linked with known terrorist elements who live in and act against Cuba from United States territory, with the full agreement of the United States authorities.

8. The illegal radio and television broadcasts against Cuba do not provide information; on the contrary, they falsify and distort it for subversive purposes. For actions of this kind, the United States Congress annually approves a budget of over $30 million in federal funds. Since the two broadcasters commenced activities, the United States Government has spent $659.8 billion for this purpose.

9. These provocative broadcasts against Cuba constitute violations of the following international principles:

– The fundamental principles of the International Telecommunication Union, expressed in the preamble to its Constitution, on the growing importance of telecommunication for the preservation of peace and the economic and social development of all States, with the object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunication services. The content of the television programming broadcast by the Government of the United States of America against Cuba is subversive, destabilizing and deceptive in character, contradicting those principles.

– Provisions CS 197 and CS 198 of the Constitution of the International Telecommunication Union stating that all stations must be effectively established and operated in such a manner as not to cause harmful interference to the radio services or communications of other member States.

– Agreement at the ninth plenary meeting of the World Radiocommunication Conference (WRC) held in November 2007, which stated in paragraph 6.1 (g) "that a broadcasting station operating on board an aircraft and transmitting solely to the territory of another administration without its agreement cannot be considered in conformity with the Radio Regulations".

– ITU Radio Regulation 8.3 establishing that internationally recognized frequency assignments recorded must be taken into account by other administrations when making their own assignments, in order to avoid harmful interference.

– ITU Radio Regulation 42.4, prohibiting the operation of a broadcasting service by an aircraft station at sea and over the sea.

– A ruling of the ITU Radio Regulations Board, which at its 35th meeting in December 2004 established that United States emissions on 213 MHz resulted in harmful interference with Cuban services and requested the United States Government to take the relevant measures to halt them. Furthermore, since September 2006 the Radio Regulations Board has been requesting the United States Government to take measures to eliminate interference on 509 MHz, with no response to date. In the Summary of Decisions of the fiftieth meeting of the Board, which ended on 20 March 2009 (document RRB09-1/5), it was once again stated that the transmissions are illegal and the United States Government was requested to take all necessary steps with a view to eliminating these two cases of interference with television services in Cuba. On 26 March 2010, at its fifty-third meeting, the ITU Radio Regulations Board reiterated its conclusion that the broadcasts from

the United States cause interference harmful to the Cuban stations included in the International Frequency Register and urged the United States administration to eliminate this harmful interference, requesting the Radiocommunication Bureau to monitor the situation and to act in accordance with the procedures established in the Radio Regulations.

– ITU Radio Regulation 23.3, limiting television broadcasting outside national frontiers.

10. A report issued in January 2009 by the General Accounting Office (GAO) of the United States of America, an official government agency, recognizes the violations of international norms and domestic legislation committed by the programme of radio and television broadcasts by the United States Government against Cuba.

– The report recalled that the International Telecommunication Union had determined in 2004 and 2006 that United States broadcasting on channels 13 and 20 was causing harmful interference to Cuban stations and that the State Department had taken no action in response to the ITU determination. The report also stated that the World Radiocommunication Conference, held in November 2007, had found that transmission from an aircraft was not in conformity with ITU regulations.

– The report had stated that, although United States legislation prohibited the domestic dissemination of broadcasts of that type, both the radio and television broadcasts were received in the territory of the United States, principally in Miami, and that the stations under contract aired paid political advertisements and commercials for sex services. In addition, it noted that the broadcasts against Cuba did not adhere to journalistic standards of balance and objectivity and used incendiary and offensive language.

11. Cuba recalls, moreover, that the World Radiocommunication Conference (WRC-07), which met in Geneva, Switzerland, from 22 October to 16 November 2007, adopted conclusions that found transmissions from aircraft from the United States to Cuba to be in violation of the Radio Regulations. The conclusions endorsed by the plenary stated that "*a broadcasting station operating on board an aircraft and transmitting solely to the territory of another administration without its agreement cannot be considered in conformity with the Radio Regulations*".

12. These conclusions were agreed in the plenary of the 2007 Conference and have legal standing in the work of ITU. The World Radiocommunication Conference thus endorsed the 1990 ruling of the former International Frequency Registration Board that television broadcasts from an aerostat with programming directed to Cuban national territory were in violation of the regulations.

13. The hostility of the Government of the United States of America towards Cuba has been manifested through the economic, financial and trade embargo imposed for almost 50 years, which also affects information and telecommunications.

- Cuba is not able to access the services provided by many websites; when it is recognized that the link is being established from an Internet address with the Cuban domain name .cu, access is denied.
- Without prior notification, the Office of Foreign Assets Control (OFAC) has blocked .com domains related to Cuba.
- Because of the laws on the economic, trade and financial embargo imposed by the Government of the United States of America, Cuba is unable to connect to the fibre-optic cables that surround the Cuban archipelago, forcing the country to pay for satellite services involving bandwidth restrictions, serious problems acquiring the necessary technologies and high connection costs.
- The Internet is being used to conduct defamatory campaigns against Cuba for subversive purposes and in order to discredit the country.

14. This attitude erodes the spirit, the intentions and the conclusions that prevailed among the nations of the entire world when they met in Switzerland and Tunisia during the World Summit on the Information Society, in 2003 and 2005.

15. The Summit strongly urged States, in building the information society, to take steps with a view to the avoidance of, and refrain from, any unilateral measure not in accordance with international law and the Charter of the United Nations that impedes the full achievement of economic and social development by the population of the affected countries and that hinders the well-being of their population.

16. The discussion in the United Nations General Assembly about developments in information and telecommunications in the context of international security is very relevant and becoming ever more timely and important. Actions by the United States against Cuba such as those described above confirm the need for this debate and the urgency of finding ways to end such manifestations.

17. Cuba strongly supports this exercise by the General Assembly and will continue to spare no effort to contribute to the peaceful global development of information and telecommunication technologies and their use for the good of all humanity. It is also ready to collaborate with other countries, including the United States of America, to find solutions that will overcome the obstacles preventing the achievement of these goals.

Greece

[Original: English]
[28 June 2010]

1. Information security issues have been more extensively addressed than in the past. Counter-measures to the modern threats that are inherent to the advent of the globalization of networks and systems are certainly considered. Measures to preserve the free flow of information are studied and applied in the national and cross-border context.

2. Current international and multinational concepts are followed and studied. International guidance on risk assessment is needed. Cyber defence should also be addressed. National sovereignty rights for information security in global sharing should be maintained.

3. It is understood that all Member States should continue to inform the Secretary-General on their views and assessments on the corresponding questions. In this respect the following points are noted:

(a) All information security issues are highly appreciated in general;

(b) Ways to preserve the free flow of information and provide for the required degrees of confidentiality, integrity and availability are studied and applied within the national and cross-border context;

(c) The concepts for the interconnection of networks that provide for capabilities enabled and shared at both the national and international levels should be drafted and agreed. Risk assessment for the interconnection of networks must prevail and relevant international guidance should be available. Further to that, and since a very serious concern for every nation has been the need to take measures for its cyber defence, coherent international guidance is needed for cooperation, efficiency and economy. Last but not least, the requirement for a nation to preserve its sovereignty and maintain its own base of information cannot be overlooked and every concept drafted should account for that;

(d) Possible measure to be taken by the international community to strengthen information security at the global level are the following:

(1) Relevant international concepts should be detailed and agreed;

(2) A guidance plan for a harmonized generic infrastructure, covering basic legislation matters, could be proposed, in order to deliver to a number of certified users the required information security for electronic handling of all correspondence and messaging, providing multiple ways of communication;

(3) Concepts followed by multinational alliances and small nations' constellations should be harmonized and expanded to be

applicable at the global level. The agreement to specify the threat and its negative effect could be more than the engineering of any sophisticated measures devised, since they could also be used by adversaries;

(4) In parallel to all of the above, the nation's sovereignty should be understood as the basic reference for every attempt of globalization. An international concept for defining the national information exchange gateways, with scenarios reflecting the desired level of integration, should be drafted and used as a guide, for all efforts at the national, multinational and international levels.

Mexico

[Original: Spanish]
[18 May 2010]

General overview of information security problems

1. In Mexico, the banking and financial institutions, as well as the units of the Federal Government dealing with public security and national security, are the organizations making the greatest effort in the area of computer security. There is a Cybercrime Unit and a cyberpolice unit within the Federal Public Security Secretariat to deal with public security cybercrime.

2. On the other hand, although individual efforts to combat cybercrime are being made in the three branches of government, the Federal Government does not have a cybersecurity policy governing strategies to combat cybercrime in Mexico, the legislation on the subject must be strengthened, judges need more tools for dealing with and punishing cybercrime, and the regulations on Internet service providers also need to be expanded so that they are required to keep a record of activity on their platforms and to provide information in the event of an incident. There is also a need for domestic agreements and cooperation arrangements with other countries for combating cybercrime and cyberterrorism undermining national security.

Measures adopted at the national level to enhance information security and contribute to international cooperation in this area

3. Efforts are being made in Mexico to create certainty as regards information security:

(a) Certain cybercrimes are covered in the following laws: Federal Criminal Code, Federal District Criminal Code, Federal Code of Criminal Procedure, Coloma Data Protection Act, and Criminal Codes of the states of Aguascalientes, Sinaloa, Tabasco and Tamaulipas;

(b) On 30 April 2009, the Official Gazette of Mexico published the Decree adding section XXIX-O to article 73 of the Political Constitution of the United Mexican States, authorizing Congress to legislate on the protection of personal data in the possession of individuals;

(c) On 1 June 2009, the Decree was published adding a second paragraph to article 16 of the Constitution, recognizing that all individuals are entitled to protection of their personal data and the right to access, correct and delete such data, as well as to express their objection, in the manner established by the law, which establishes grounds for waiving the principles governing data processing for reasons of national security, law and order, public safety and health or to protect the rights of third parties;

(d) The Computer Security Incident Response Team of the National Autonomous University of Mexico deals with security problems in academia and provides support and technical advice to the Mexican authorities in dealing with cybercrime;

(e) There is a cyberpolice unit in the federal police force to follow up investigations on public security crimes;

(f) An executive report on cybervulnerability is being prepared by the Federal Government to inform senior government authorities about global cyberincidents in order to organize and support initiatives promoting cybersecurity in Mexico;

(g) It is planned to create a national CSIRT[1] within the Federal Government to coordinate efforts to combat cybercrime at home and abroad;

(h) Cybervulnerability is an item on the National Risk Agenda;

(i) There are programmes, coordinated by public and private bodies, to raise the awareness of the general public for the prevention of cybercrime;

(j) Mexico participates in various forums and has goodwill agreements with other countries on the subject of cybercrime.

Measures which the international community could take to strengthen global information security

4. The following are measures to strengthen global information security:

(a) Adoption of suitable legislation or updating of existing legislation as necessary for the protection of information in cyberspace;

(b) Training of judges in cybersecurity issues so that they can understand the nature of cybercrime and deliver appropriate sentences;

[1] CSIRT Computer Security Incident Response Team.

(c) Establishment of national Computer Security Incident Response Teams to coordinate efforts to deal with major security incidents and serve as contact points with other countries;

(d) Ongoing communication between national Computer Security Incident Response Teams so that they can coordinate their response in the event of a regional or global incident;

(e) Organization of forums for sharing experience and training security teams that are members of the international community;

(f) International arrangements for collaboration to combat cybercrime in order to facilitate investigations and form a united front.

Panama

[Original: Spanish]
[21 June 2010]

1. There are institutions in the Republic of Panama combating inappropriate use of the Internet for criminal purposes including terrorist acts, including the National Security Council and the Institute of Forensic Medicine and Science with its Department of Law and Order.

2. The National Security Council does intelligence work to combat organized crime, including terrorism, in connection with a possible attack on the property and integrity of the national territory.

3. The Institute of Forensic Medicine and Science has a Department of Law and Order, created by Act No. 69 of 27 December 2007, which investigates cybercrime.

4. Our Criminal Code criminalizes, suppresses and punishes use of the Internet for terrorist purposes. Article 289 states "Any person using the Internet to provide training for the commission of terrorist acts or to recruit others to commit such acts shall be punished by imprisonment for five to ten years."

5. Other legal texts punish the use of the Internet for criminal purposes and provide criminal, civil and administrative penalties, governed by Act No. 14 of 18 May 2007, title VIII, chapter I (Computer security crimes), Act No. 51 of 22 July 2008 regulating electronic documents and electronic signatures and provision of services and include other provisions on the development of e-trade and Act No. 38 of 8 February 1996 enacting rules to govern telecommunications in the Republic of Panama.

Qatar

[Original: English]
[25 May 2010]

1. The State of Qatar is convinced that information and communication technology should be used in accordance with the Charter of the United Nations and the basic principles of international relations. Moreover, free flow of information must be guaranteed without prejudice to national sovereignty and while maintaining security and respect for cultural, political and moral differences among nations.

2. Efforts at the national level are based on the interest in security communications and to enhance it from time to time in order to keep up with its advancement at the national and international levels.

3. National efforts can be summarized as follows:

– Setting security strategies and policies and promulgation of laws to restrict the use of this technology for purposes that are not in accordance with the goals of the protection of the stability of security

– Establishing a mechanism to reinforce the security of information in order to guarantee the protection of the infrastructure of the sensitive information of Qatar

– The Office of Internet Security and Intelligence seeks to monitor government networks and the national network in order to address threats to the State of Qatar through the Internet

– Management of Internet incidents and coordinating efforts to resolve them aims to guarantee the resolution of Internet-related issues after reporting them, with minimum downtime. In the State of Qatar this is done by the Qatar Computer Emergency Response Team (Q-CERT)

– A more effective role for information and awareness to improve the level of technical skills and qualifications of employees in Qatari institutions

–Providing support to Qataris in dealing with Internet-related issues

– Follow-up on the latest advancements in the field of modern technological science related to the security and safety of the Internet, and ensuring the assessment of technical products, its security and services

– Advancing international relations in order to deal with Internet-related issues. The State of Qatar has participated in the Forum of

Incident Response and Security Teams (FIRST) and the Meridian Process.

4. The most important measures that the international community can take to promote the security of information at the national level are the following:

- The United Nations should continue to lead the discussion and provide more clarification regarding the use of information and wired and wireless communication technology in electronic warfare, and whether existing principles of international law are sufficient to provide an appropriate framework to determine appropriate behaviour online regarding aggressive acts
- The establishment of an international ad hoc committee for the security of wired and wireless information and providing comprehensive studies related to this issue
- The State of Qatar encourages all Member States to create teams to address computer emergencies at the national level
- Contracting with specialized security institutions in the communication field
- Raising security awareness through symposiums and meetings at the local and international levels
- Encouraging States to cooperate in order to combat espionage and electronic piracy
- Usage of encrypted and secured equipment to transfer information and documents in a secured manner to ensure its confidentiality when it is exchanged
- Updating protection systems and convening regular workshops to take stock of the latest in science in the area of the advancement of information security.

Ukraine

[Original: Russian]
[12 May 2010]

Achievements in the use of information technology and telecommunications in the context of international security

1. The growing role of information technology in the various spheres of activity in society has led to concern for information security. As advanced information

technology enters the everyday life of States and societies, the opportunities for cyberattacks against information and telecommunications systems, against the information resources of State bodies and against commercial entities on the part of criminal elements and individuals, seeking to commit criminal acts, have grown.

2. Half of all recorded computer crimes involve unauthorized access to computer information. Computer crime for profit is growing, as is the material damage it causes. The number of crimes committed by transnational hacker groups is also growing.

3. Computer crimes are rarely reported and efforts to determine the full extent of such crimes are usually frustrated, as the government and business entities that fall victim to such attacks always try to hide that fact, so as not to risk losing their authority, and they are reluctant to reveal the losses suffered and the weakness of their information protection systems. As a result, cases of such crimes are often not reported, which speaks to the need to develop concerted prophylactic and preventive measures, which should be at the core of information protection systems.

4. A computer crime is usually only the first step in a series of criminal acts, like the traditional types of crime, namely, theft, extortion, fraud and so forth. These crimes are constantly becoming more sophisticated and hidden and their execution improving, causing huge economic and political harm in practically all countries of the world. Furthermore, most experts see a direct link between the information sovereignty of States and matters of national security.

5. Efforts to combat crime in the field of information technology encounter many problems of a legal nature resulting from the non-material and frequently ephemeral nature of computer evidence. The complex issues involved in dealing with the problems encountered in cybercrime make international cooperation even more necessary. For that reason all countries must in the end establish appropriate and mutually compatible legal, procedural and normative tools.

6. In practice the investigation of computer crime has shown the imperative need for cooperation between the law enforcement agencies of States.

7. In international practice joint measures are usually taken to investigate computer crime. The Ukrainian Security Service participates actively in joint operations by law enforcement agencies and special services as part of efforts to combat child pornography, fraud perpetrated via the Internet and international terrorism.

8. Furthermore, there is a need to strengthen efforts aimed at further developing cooperation in the provision of information security, protecting shared interests and introducing steps for their protection, mainly in the form of bilateral and multilateral agreements. A successful solution to the problems of information security can be found only if there is effective cooperation between the government

bodies of the various States, especially since the required legal basis is already in place.

9. Given the need to combat the threats of cybercrime and cyberterrorism, the Ukrainian Security Service maintains contacts with the law enforcement agencies and special services of foreign States.

10. It should be pointed out that cybercriminals often select as their targets networks established by government offices. Furthermore, the success of efforts to track down and punish criminals depends on the quality of the international links that are established and on the optimization of national legislation to meet current standards.

11. Bearing in mind the continuous global growth in computer crime, the existence of links between criminal hacker groups in various countries and the fact that cyberthreats bear no relation to national borders, it is vital that international cooperation in the fight against cyberthreats be expanded.

12. With a view to implementing the decisions of the World Summit on the Information Society (first phase held in Geneva from 10 to 12 December 2003; second phase held in Tunis from 16 to 18 November 2005), Ukraine adopted an Act on basic principles for the development of the information society in Ukraine for 2007-2015. Its fundamental priorities are integration into the global information environment and development of the information society. The Act is intended to enable the latest information and communication technologies to be used in an atmosphere of better security.

13. In addition, a plan for the development of telecommunications in Ukraine has been drawn up and adopted. It provides for logistical and technical efforts to ensure the secure operation of all components of Ukraine's telecommunications infrastructure, including:

- establishing and introducing gradually a normative and legal basis to protect information, through technical means and encryption, ensuring harmonization with European and global standards;
- developing up-to-date information protection methods using technology to address comprehensively the task of protecting information in telecommunication networks;
- establishing systems to legally intercept information in telecommunication networks in the instances provided for by the law;
- establishing a State coordination centre for security in public information and telecommunication networks and helping to establish State and non-governmental centres to react and respond to incidents on those networks.

14. The normative and legal basis for information protection in Ukraine also includes Acts on the fundamental principles of national security; on information; on information protection and information and telecommunication systems; issuances of the President and Cabinet of Ministers on the technical protection of information in Ukraine; rules for the protection of information and telecommunication systems and networks and procedures for connection to global data-transmission networks. It also includes a large number of normative acts registered with the Ministry of Justice and having as their purpose to regulate connection of information systems to global data-transmission networks, licensing of particular types of activity and procedures for assessing information protection.

15. Normative and legal acts provide that the requisite protection of information should be achieved using only protected information and communication technology systems, in other words, those incorporating a comprehensive information protection system as a single body of legal and logistical measures, software and hardware, intended to counter threats. The comprehensive system, and its information-protection components, must be certified as compliant with information-protection standards.

16. In order to regulate the requirements for comprehensive information protection systems and their components, Ukraine has developed and introduced some 50 technical standards laying down criteria for the assessment of information protection, the classification of information and communication technology, procedures for achieving information protection requirements for the individual components of a comprehensive information protection system depending on the variety of information and communication technology involved, the ultimate purpose, the field of use and the type of information processed.

17. Ukraine has also created its own national system of criteria for assessing the security of information technologies. The system is based on a set of regulatory instruments on protecting information in information and telecommunications systems from unauthorized access; these instruments have been harmonized with similar instruments of European Union countries and with international standards, in particular standard 15408 of the International Organization for Standardization/ International Electrotechnical Commission.

18. In addition, a national system of organizational and technical measures is being established in Ukraine with a view to preventing unauthorized acts against the information and telecommunications systems of the State authorities, law enforcement, customs and tax authorities, credit and financial institutions and others, in particular attempts to interfere with their work through the Internet.

19. As specified in article 16, paragraphs 10 and 11, of the Act on the State Service for Special Communications and Information Protection, and in order to improve coordination between State agencies for the detection of threats to information in information and telecommunications systems, to deal with the consequences of implementation of such threats and to organize international cooperation in such

matters, the appropriate Computer Emergency Response Team (CERT-UA) has been created within the Service and is operational.

20. Reflecting the global trend towards networks of rapid reaction facilities, CERT responds to computer emergencies. International coordination of the activities of such facilities is provided by the international Forum for Incident Response Security Teams (FIRST), a forum for teams responding to security incidents.

21. On 13 July 2009, CERT-UA (www.cert.gov.ua) became a full member of FIRST.

22. Among its activities for 2009, CERT-UA processed 461 reports from CERTs in 30 countries (Australia, Austria, Belgium, Canada, China, Denmark, Finland, France, Estonia, Germany, Hungary, India, Israel, Italy, Japan, Korea, Lithuania, Malaysia, Netherlands, Norway, Pakistan, Poland, Portugal, Romania, Russian Federation, Saudi Arabia, Spain, Taiwan, Turkey, United States of America) of unauthorized acts in the Ukrainian segment of the Internet (distribution of harmful software, distributed denial-of-service (DDoS) attacks and other attempts to commit unauthorized acts).

23. It should be added that Ukraine has created a legal and regulatory framework and made efforts to ensure cooperation between the State Service for Special Communications and Information Protection and the law enforcement agencies with a view to implementing measures to safeguard the security of State information resources in information and telecommunications systems and improving the effectiveness of the system for responding to unauthorized acts against those information resources.

24. Thus, in Ukraine, information can now be protected at all stages of the establishment of information and telecommunications systems and the comprehensive information protection systems within them, irrespective of the type and criticality of the information being processed and the type and complexity of the information and telecommunications system. Moreover, all the basic approaches to the elaboration of requirements, design, development, security assessment and protection of information resources in information and telecommunications systems as a whole correspond to the approaches employed by the State security services of the Member States of the United Nations and the member States of the European Union.

25. With a view to training specialists in the field of information security and computer engineering, an Institute for Information Protection has been set up as an academic and scientific department of the State University of Information and Communications Technologies.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[2 June 2010]

1. The United Kingdom is pleased to respond to General Assembly resolution 64/25, Developments in the field of information and telecommunications in the context of international security.

2. We consider this to be a most important topic, vital to individual nations, their commerce, the protection of their citizens and in the broader context of international security. The United Kingdom devotes considerable effort so as to make cyberspace a safer place for all nations and we welcome international activities in this sphere, as we believe that all nations should cooperate in promoting a safe and resilient environment in cyberspace.

General appreciation of the issues of information security

3. We believe that a secure cyberspace is vital to today's world. Citizens, commerce, critical national infrastructure and government are increasingly dependent on the Internet. Any event that adversely affects the Internet service within a nation is likely to have consequences for that nation, perhaps of a severe nature. It is an unfortunate fact that there is likely to be a number of threat actors, both external and internal to any nation, who may attempt to disrupt or manipulate the Internet service for any of a number of reasons.

Efforts taken at the national level to strengthen information security and promote international cooperation in the field

4. The United Kingdom continues to work domestically and internationally so as to promote safer cyberspace. Domestically, we published our National Cyber Security Strategy in June 2009. This document underpins the national effort on information security. The Strategy calls for two new organizations, the Office of Cyber Security and the Cyber Security Operations Centre. The organizations have been established and continue to grow. There are three computer emergency response teams (CERTs) run by the United Kingdom government and which provide a specialist service to United Kingdom critical national infrastructure, military and other government networks. Internationally, we are also active in this work. Our United Nations involvement includes membership of the Group of Governmental Experts. We co-sponsored the United Nations resolution on the creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. We have membership of relevant International Telecommunication Union (ITU) bodies. We participate in activities of the Organization for Security and Cooperation in Europe. With our full support and participation, the European Union (EU) has begun work on several initiatives on the protection of critical national infrastructure in the EU. We participated in the EU engagement with the ASEAN Regional Forum work on cybersecurity. Similarly

we participate in a number of activities within NATO as part of protecting that organization's networks. The United Kingdom has long been a leading nation within MERIDIAN (www.meridian2007.org), FIRST (Forum on Incident Response and Security Teams, www.first.org) and the EGC (European Government Certs Group, www.egc-group.org).

5. The United Kingdom National Cyber Security Strategy is available for download from the Cabinet Office web page at www.cabinetoffice.gov.uk.

Possible measures that could be taken by the international community to strengthen information security at the global level

6. We encourage all nations to establish national computer emergency response teams. We encourage all nations to enact effective domestic legislation on cybercrime. We believe that whereas e-crime is not the only malicious activity in cyberspace, it is the most prevalent, and that a reduction of criminal activity will benefit all. We believe that the Council of Europe Convention on Cybercrime represents a suitable instrument for combating international e-crime. Additionally, we believe that the toolkit developed by the ITU and promoted in the United Nations provides a good basis for nations to perform a self-assessment of their readiness to cope with potential attacks on critical national infrastructure. We welcome efforts within many forums to promote information security best practice.

Relevant international concepts

7. The primary international concept is that of international law. There is considerable debate, particularly at cyber conferences, about the applicability of existing international law to cyberspace. The United Kingdom has examined this issue, and our view is that the existing principles of international law, on both the use of force and the law of armed conflict, provide an appropriate framework within which to identify and analyse the use of cyberspace in the context of hostilities.

List of "Blue Book" *Study Series*

No.		
33	2011	Developments in the Field of Information and Telecommunications in the Context of International Security
32	2008	Verification in all its aspects, including the role of the United Nations in the field of verification
31	2005	The relationship between disarmament and development in the current international context
30	2003	Study on disarmament and non-proliferation education
29	2003	The issue of missiles in all its aspects
28	1999	Small Arms
27	1994	Study on the Application of Confidence-building Measures in Outer Space
26	1993	Study on Defensive Security Concepts and Policies
25	1993	Potential Uses of Military-Related Resources for Protection of the Environment
24	1992	Study on Ways and Means of Promoting Transparency in International Transfers of Conventional Arms
23	1991	South Africa's Nuclear-Tipped Ballistic Missile Capability
22	1991	Effective and Verifiable Measures Which Would Facilitate the Establishment of a Nuclear-weapon-free Zone in the Middle East
21	1991	Nuclear Weapons: A Comprehensive Study
20	1991	The role of the United Nations in the Field of Verification
19	1989	Study on the Economic and Social Consequences of the Arms Race and Military Expenditures
18	1989	Study on the Climatic and Other Global Effects of Nuclear War
17	1987	Study on Deterrence
16	1986	The Naval Arms Race
15	1986	Reduction of Military Budgets
14	1986	Concepts of Security
13	1985	Unilateral Nuclear Disarmament Measures
12	1985	Study on Conventional Disarmament
11	1983	Economic and Social Consequences of the Arms Race and of Military Expenditures
10	1983	Reduction of Military Budgets
9	1983	The Implications of Establishing an International Satellite Monitoring Agency
8	1982	Relationship between Disarmament and International Security
7	1982	Comprehensive Study on Confidence-building Measures
6	1982	Study on Israeli Nuclear Armament
5	1982	The Relationship between Disarmament and Development (see also No. 31, 2005)
4	1981	Reduction of Military Budgets
3	1981	Study on all the aspects of Regional Disarmament
2	1981	South Africa's plan and capability in the nuclear field
1	1981	Comprehensive Study on Nuclear Weapons (see also No. 21, 1991)

Printed copies may be obtained by consulting your local bookstore or through the United Nations Publications website: https://unp.un.org.

DISARMAMENT

Study Series 33

USD 15
ISBN 978-92-1-142281-8

Printed at the United Nations, New York
11-59426—December 2011—850