United Nations A/66/152

General Assembly

Distr.: General
15 July 2011
English
Original: English/Russian

Sixty-sixth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

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

Report of the Secretary-General

Contents

* A/66/150.

11-41691 (E) 250711 290711

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,[1] 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.

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.

[1] A/65/201.

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 Kazkhstan 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 cyberinfrastructure; 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.