United Nations A/70/172

General Assembly

Distr.: General
22 July 2015
English
Original: Arabic/English/Spanish

Seventieth session
Item 93 of the provisional agenda*

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

Report of the Secretary-General

Contents

[*] A/70/150.

I. Introduction

1. On 2 December 2014, the General Assembly adopted resolution 69/28, entitled "Developments in the field of information and telecommunications in the context of international security". In paragraph 3 of the resolution, the 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 (A/68/98), 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 to promote international cooperation in that 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 2 February 2015, a note verbale was sent to all Member States inviting them to provide information on the subject. The replies received at the time of reporting are contained in section II. Any additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

Canada

[Original: English]
[4 June 2015]

Cyberspace has enhanced social interaction and transformed industries and Governments, and continues to be an engine of economic growth, innovation and social development. It has also introduced new threats and challenges to our society.

Canada reiterates the clear affirmation by States in the report of 2013 of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of the applicability of international law in cyberspace as the cornerstone of norms and principles of responsible behaviour of States, and it encourages future work on peacetime norms.

Canada also believes that addressing the security of information and communications technology must go hand-in-hand with respect for human rights and fundamental freedoms. The same rights that people have offline must also be protected online.

Canada is committed to a free, open and secure Internet by means of the following:

(a) Implementing the cybersecurity strategy and action plan of Canada remains at the forefront of our efforts at the national level. Those help to secure the cybersystems of Canada and protect Canadians online through active engagement with major critical infrastructure sectors (e.g. finance, transportation and energy);

(b) Canada has developed a cyberincident management framework to provide a consolidated national approach to the management and coordination of potential or existing cyberthreats or incidents;

(c) The new anti-spam legislation of Canada assists in clarifying legal rights obligations and the respective duties of government agencies, as well as strengthening legislative provisions for enforcement and international collaboration;

(d) Internationally, Canada has committed $8 million to support cybersecurity capacity-building projects, primarily in the Americas and in South-East Asia. Canada has also provided more than $3.6 million through the Organization of American States (OAS) (2007-2016) to build capacity in OAS countries, including establishing computer security incident response teams. Canada has also joined the Global Forum on Cyber Expertise as a founding member;

(e) Canada supports the efforts of the North Atlantic Treaty Organization to strengthen the alliance's cybersecurity and that of individual allies;

(f) Canada works within the Regional Forum of the Association of Southeast Asian Nations (ASEAN) to build capacity on the importance of confidence-building and transparency measures for stability in cyberspace;

(g) Through the cybersecurity action plan between Canada and the United States of America, Canada partners with the United States to enhance the resiliency of our cyberinfrastructure and improve engagement, collaboration and information-sharing at the operational and strategic levels;

(h) Canada also participates in initiatives to combat cybercrime in the Group of Seven, the United Nations Office on Drugs and Crime, OAS and ASEAN, and is a member of the Global Alliance against Child Sexual Abuse Online;

(i) Canada recommends that all Member States wishing to enhance cybersecurity and prevent cybercrime refer to the Council of Europe Convention on Cybercrime.

The full text of the submission by Canada can be found at www.un.org/disarmament/topics/informationsecurity/.

Cuba

[Original: Spanish]
[26 May 2015]

Cuba shares the concern expressed in resolution 69/28 that information 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.

Resolution 69/28 also places emphasis on the need to prevent the use of information resources or technologies for criminal or terrorist purposes.

In this regard, Cuba expresses its great concern over the covert and illegal use, by individuals, organizations and States, of the computer systems of other nations for the purpose of attacking third countries, because of its potential for triggering international conflicts.

Joint cooperation between all States is the only way to prevent and tackle these novel threats and to avoid cyberspace from turning into a theatre of military operations.

The use of telecommunications with the declared or hidden intent of undermining the legal and political order of States is a violation of internationally recognized norms in this area and can give rise to tensions and situations that are not conducive to international peace and security.

The Heads of State and Government of Latin America and the Caribbean, at the second Summit of the Community of Latin American and Caribbean States (CELAC), held in Havana in January 2014, proclaimed the Latin American and Caribbean region to be a zone of peace, in order to, among other objectives, foster cooperation and friendly relations among themselves and with other nations, irrespective of differences in their political, economic, and social systems or development levels, to practice tolerance and to live together in peace with one another as good neighbours.

At the third CELAC Summit, held in Belén, Costa Rica, on 28 and 29 January 2015, member States highlighted the importance of information and communication technologies, including the Internet, and innovation as tools to encourage peace and promote well-being, human development, knowledge, social inclusion and economic growth, underscoring their contribution to improving the coverage and quality of social services. The peaceful use of information and communication technologies in compliance with the Charter of the United Nations and international law was also reaffirmed and it was stressed that these technologies should never be used with the purpose of subverting societies or creating situations that could promote conflicts between States.

Nevertheless, those efforts are threatened by the constant radio and television broadcasts transmitted by the Government of the United States against Cuba, in contravention of the purposes and principles of the Charter of the United Nations and various regulations of the International Telecommunication Union. Furthermore, and of no less significance, these broadcasts violate the sovereignty of Cuba.

Cuba reiterates that the use of information as propaganda or for the purposes of destabilization, with the aim of subverting the internal order of other States, violating their sovereignty and meddling and interfering in their internal affairs, constitutes an illegal act and must cease.

We reiterate our strongest rejection of the use of information and communication technologies in a manner contrary to international law, and all actions of that nature. We stress the importance of guaranteeing that the use of these technologies is fully consistent with the purposes and principles of the Charter of the United Nations and international law, in particular sovereignty, non-interference in internal affairs and internationally recognized standards of coexistence between States.

Cuba reiterates that international cooperation is essential for confronting the dangers associated with the misuse of information and communication technologies. Cuba also highlights the importance of the International Telecommunication Union in the intergovernmental debate on cybersecurity issues.

Cuba hopes that the new context of bilateral relations between Cuba and the United States, announced on 17 December 2014 by Presidents Raúl Castro Ruz and Barack Obama, including the decision to restore diplomatic relations between the two countries and to begin a process aimed at normalizing relations, will bring those aggressive policies to an end, and that the economic, commercial and financial embargo that has caused serious damage to the Cuban people will be lifted. The embargo has had a harmful impact in the area of information and communications, among other aspects of the daily life of the Cuban people.

As a part of the computerization programme in Cuba, the first national workshop on computerization and cybersecurity, on the theme "Becoming a computerized society", was held from 18 to 20 February 2015. More than 11,500 information and communication technologies professionals from all over the country attended the event. The issue of the security, monitoring and handling of information and communication technologies was one of the topics covered.

Cuba has established the Council of Computerization and Cybersecurity, directed by the highest State body, the Government and the Communist Party of Cuba. Its purpose is to recommend, coordinate and oversee the comprehensive policies and strategies for this process. Work is also under way to set up the Computer Users Union of Cuba.

Cuba supported resolution 69/28 and will continue to contribute to the peaceful global development of information and telecommunications technologies and their use for the good of all humanity.

El Salvador

[Original: Spanish]
[21 April 2015]

The Armed Forces of El Salvador, within the context of information and telecommunications security, have centralized public-network-independent voice, video and data telecommunications. A perimeter information security team has been acquired and configured; in addition, there is an encryption system for handling official information in order to protect all information from any external agent that may attempt to infiltrate the system, as well as from cyberattacks.

Georgia

[Original: English]
[26 May 2015]

The Government of Georgia puts information and cybersecurity high on its political agenda and considers addressing cyberthreats an integral part of the national security policy, especially in view of widespread e-government reforms throughout the country and the increased dependence of its critical infrastructure on information and communications technology tools. Voicing those concerns, and in order to strengthen information security, the Government of Georgia has introduced several strategic, legal, organizational and institutional measures.

The first strategy addressing cybersecurity at the national level is laid out in the cybersecurity strategy and action plan for 2013-2015, which is the principal document outlining the State's policy in the area of cybersecurity, including strategic goals and guiding principles, and laying down action points and tasks. Cybersecurity is one of the main priorities of the State's security policy, and the protection of cyberspace is considered as important for national security as the protection of land, water and airspace.

A further step in institutionalizing information security was the establishment of the Data Exchange Agency of the Ministry of Justice of Georgia, in 2010, as a central government entity responsible for the development and implementation of information and cybersecurity policies and standards, tasked in particular with:

- Adopting and implementating information security policies and standards in the public sector and critical infrastructure
- Carrying out a cybersecurity mandate though the creation of a national computer emergency response team
- Providing consultancy services in information and cybersecurity, performing information security audits and providing cybersecurity services
- Carrying out awareness-raising activities on information and cybersecurity

The legal and regulatory framework of Georgia on information security is composed of the Information Security Act and its supplementary subnormative acts adopted between 2011 and 2012. Major concepts used in Georgian legal acts detailing information security policies derive from the 27000 series of standards of the International Organization for Standardization. The law underlines certain rights and obligations for critical infrastructures in the process of implementing information security policies and lays down cooperation mechanisms with national governmental computer emergency response teams.

Georgia has taken important steps in building international cooperation and sharing accumulated knowledge with its partners. A notable example is a number of bilateral cooperation agreements and memorandums of understanding between the Data Exchange Agency and European Union Military Staff (from Austria, Estonia, Poland, etc.) as well as neighbouring countries (Azerbaijan, Armenia, the Republic of Moldova, Turkey, etc.).

Georgia acknowledges the increased importance of regional and international cooperation mechanisms in order to address information security challenges. In that perspective, much effort should be directed to extend the number of international events dedicated to those topics of high importance, increase the level of trust with major stakeholders, and continue to work on strategic doctrines and legal concepts with the engagement of the international community.

Germany

[Original: English]
[27 May 2015]

An open, free, secure and reliable Internet offers great opportunities for economic growth, social development and scientific progress, as well as for the promotion of democracy, good governance, and the rule of law. At the same time, concerns are growing about risks for international security emanating from cyberspace. Recent months have seen an increase in malicious software activities against highly visible targets, such as media outlets. Attacks against critical infrastructures, in particular, could have severe consequences.

An all-out “cyberwar” seems unlikely at present. However, the limited use of cybercapabilities as part of a larger war-fighting effort, including in the context of hybrid conflicts, has become a reality. In addition, incidents in cyberspace may escalate into real-world conflict.

Germany advocates a three-pronged approach to manoeuvre in that environment: agreeing rules of responsible State behaviour in cyberspace, engaging in confidence-building and increasing cyberresilience.

The United Nations is the crucial forum for establishing the rules of responsible State behaviour in cyberspace. An important starting point is the consensus of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 2012-2013 that international law, particularly the Charter of the United Nations, is applicable in cyberspace. The Group of Governmental Experts of 2014-2015, in which Germany has once again been actively engaged, has built on this.

A shared understanding of the rules, norms and principles of responsible State behaviour in cyberspace could enhance international transparency and predictability, thereby contributing to peace and stability. It would be useful, for example, to have a better common understanding of how the law on armed conflict applies to the use of those military cybercapabilities that more and more States are developing.

Concerning confidence-building, Germany attaches the utmost importance to regional organizations. In 2013, the Organization for Security and Cooperation in Europe agreed on an initial set of cyberconfidence-building measures. Implementation is proceeding well and negotiations are under way for a second set, which would address trust-building and cooperation. As part of its upcoming chairmanship of the organization, Germany plans to prioritize cybersecurity.

Germany is working on an information technology security act to increase cyberresilience at the national level. The draft text of that act defines minimum requirements for the information technology security of critical infrastructures. It establishes an obligation to report significant incidents with a view to improving the overall security of systems and public protection in general. Germany also offers support to other States in increasing their capacity to manage cybersecurity risks.

The full text of the submission by Germany can be found at www.un.org/disarmament/topics/informationsecurity/.

Netherlands

[Original: English]
[29 May 2015]

The international community has a shared interest and responsibility to ensure that cyberspace remains open, free and secure. In the view of the Netherlands, security would be served by the broad acceptance of and adherence to a set of norms of responsible behaviour of States. Much work has been done already by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. However, the following areas would benefit from further work and the following concrete measures:

- Enhancing States' understanding of how existing international law and norms for the rules of conduct for States apply to cyberspace, particularly the international legal framework that applies to cyberoperations that do not rise to the threshold of an armed attack
- Defining norms or additional measures of self-restraint or mutual assistance, particularly the idea to establish special normative protection for certain systems and networks, including critical infrastructure providing essential civilian services, civilian incident response structures and certain critical components of the global Internet
- Strengthening the legal, diplomatic and policy capacity and the exchange of best practises in the field of international peace and security in cyberspace. The Global Forum on Cyber Expertise, which was launched in The Hague during the fourth Global Conference on Cyberspace, can play an important role in this respect

As the Internet has become a strategic asset for all of us, broad international discussion on those topics is needed. The Netherlands will remain actively involved in helping to promote that dialogue.

The full text of the submission by the Netherlands can be found at www.un.org/disarmament/topics/informationsecurity/.

Panama

[Original: Spanish]
[3 June 2015]

Information and communications technologies today are expanding rapidly. As a result, technology and communications are gradually becoming a more accessible part of the daily life of all Panamanians.

It is a fact that our lives are now linked to these developments in how communications are sent and how information is processed.

The Government of Panama has acted in accordance with this trend, adapting it to the specific needs of this security agency. For that reason, it has been carrying out technological improvements to establish more efficient and secure connectivity.

As part of these improvements, the Government of Panama has gradually been developing a communications implementation plan, which includes network, security and telephony elements. These elements comply with international standards, as confirmed with their manufacturers.

The Government of Panama protects the integrity of its information in the area of the Internet, data and telephony by means of infrastructure based on internal firewall platforms and through connection with the national multiservices network.

The Government of Panama uses secure firewall-mediated data sessions in order to ensure the confidentiality and protection of information.

We consider that as increasingly advanced telecommunications solutions are adapted to the security requirements of security agencies, those agencies will have access to tools that foster harmony in the field of information, based on both active and preventative measures. Security agencies should take advantage of this technological situation, given that we have the mission of protecting society at the local and international levels.

Peru

[Original: Spanish]
[30 June 2015]

General appreciation of the issues of information security by the Information Technology Department

The corporate data network of the Peruvian National Police maintains control over its different systems through various security policies at different levels of its organic and functional structure.

- With regard to information security, the corporate data network has been outsourced through the managed security service, which is run by a security operations centre.
- Role and identity engineering work is planned; this will allow unique access control for users, ensuring traceability and providing audit tools.

Efforts taken at the national level to strengthen information security

Preventive measures:

- Designation of network administrators
- Staff training in information technology
- Software licensing for the servers of the National Police data centre
- Implementation of the “private cloud”
- Information backup
- Implementation of redundant electrical system (uninterrupted power supply)
- Upgrading of electrical distribution panels and electrical connections
- Outsourcing of perimeter security (external) in the event of attacks or denial of service.

Content of the concepts mentioned in the title of the resolution

- Upgrading of the National Police technological platform and the police information systems, which are aimed at consolidating the information means that effectively help to improve national public security, as well as contributing to international security through the availability of services that ensure interoperability between countries.

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

- Standardization of communication media, including with regard to the type of equipment and communication protocols
- Standardization of a technology platform guaranteeing high availability, dedicated to interoperability among countries involved in international security
- Standardization of information security mechanisms
- Within the concept of "field of information", definition of risk factors existing in each country involved in international security and the possibility of establishing common goals with regard to what should be combated and/or curbed, with the creation of automated information mechanisms. For example, in the case of the Peruvian State, such issues as drug trafficking, terrorism, organized crime, smuggling, money laundering and trafficking would be included.

Portugal

[Original: English]
[24 April 2015]

In its resolution 69/28 on the developments in the field of information and telecommunications in the context of international security, the General Assembly recalled the role of science and technology in the context of international security, recognizing that the developments in those areas could have civilian and military applications. While progress in the fields of information and telecommunications means more opportunities for the development of civilization, cooperation among States, the enhancement of the creative potential of humankind and the circulation of information in the global community, on the other hand, we find that those technologies and means can potentially be used for purposes inconsistent with international stability and security, and may adversely affect the national integrity of States.

In the same resolution, the General Assembly called for the contribution of Member States in four areas, taking into account the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98), namely:

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

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

(c) The content of the concepts aimed at strengthening the security of global information and telecommunications systems;

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

The report of the Group of Governmental Experts contained recommendations in the following areas: norms, rules and principles of responsible behaviour of

States; confidence-building measures and the exchange of information; and capacity-building measures.

Following those recommendations, we can describe our national context as follows.

Norms, rules and principles that characterize the responsible behaviour of States

Portugal considers that security in network information is important and has been increasing.

We must highlight the increasing efforts to implement legislation in network security and integrity, through the adoption of risk-assessment methods, which require the introduction of adequate cooperative security measures, at the technical and organizational levels, and the reporting of security violations or integrity loss that have a significant impact on the provision of services.

At the conceptual level, it is important to reinforce the idea that regulation should stem primarily from international rules.

At the international level, it is important to increase information-sharing and the conduct of training exercises in the field in border areas.

Confidence-building measures and information-sharing

It is crucial to promote information-sharing among all stakeholders (both public and private), taking into account the wider context of globalization.

At the national level, our efforts have been focused on the conduct of joint exercises in which public and private entities have participated, the promotion of technical standardization and the holding of conferences and seminars, some of which with the participation or international speakers.

Capacity-building measures

It is important to introduce capacity-building measures. Nevertheless, there are difficulties relating to the training and maintenance of human resources connected to those activities.

There is a need to facilitate the access to knowledge and to promote collective training in several areas, including security, among all the major stakeholders.

Qatar

[Original: Arabic]
[24 June 2015]

The State of Qatar continues to monitor existing and potential threats in the field of information security. It has set forth strategies to confront such threats in a manner consistent with the need to maintain the free flow of information. The State of Qatar believes that information security is crucial for national and global security. With a view to maintaining information security, the State of Qatar has taken a range of measures to update relevant technologies and improve legislation, regulation and enforcement. It also works to coordinate and cooperate on relevant issues at the regional and international levels, provided that domestic laws allow.

The State of Qatar believes that the international community can contribute to information security by continuing to work towards a binding international instrument to safeguard information security. Such an instrument should provide for the development of hacker-proof programmes and maintain the coherence of information systems.

Republic of Korea

[Original: English]
[11 June 2015]

Today, cyberspace is a new horizon with endless possibilities, offering unprecedented economic and social benefits. However, on account of its open, anonymous and borderless nature, cyberthreats are emerging as a serious challenge to international security.

The Republic of Korea has been experiencing a series of cyberattacks, including the recent attacks on its nuclear power plant operator in 2014. To respond more effectively to cyberthreats, the Republic of Korea introduced comprehensive plans to enhance cybersecurity posture in March 2015 and created the post of presidential secretary for cybersecurity affairs. The Republic of Korea firmly believes that it is important to agree on a set of international norms applied to cyberspace and implement confidence- and cybercapacity-building measures.

In that respect, the Republic of Korea welcomes the results submitted in 2013 the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which recognized the possibility of applying international law to State behaviour in cyberspace, and it expects further discussions on how the agreed principles can be applied to State behaviour in cyberspace. The Republic of Korea hosted the Asia-Pacific Regional seminar on International Law and State Behaviour in Cyberspace in 2014, together with the United Nations Institute for Disarmament Research, providing an opportunity for countries in the region to discuss cybersecurity-related matters.

The Government of the Republic of Korea has also worked to strengthen bilateral and trilateral cooperation with key countries and is actively participating in regional and international forums on cyberissues, such as the Regional Forum of the Association of Southeast Asian Nations and the Group of Governmental Experts of the United Nations. As the host of the Seoul Conference on Cyberspace held in 2013, the Republic of Korea closely cooperated with the Netherlands in preparation for the Global Conference on Cyberspace held in the Hague in 2015, and it will continue its contribution to the London Process Conferences.

The full text of the submission by the Republic of Korea can be found at www.un.org/disarmament/topics/informationsecurity/.

Spain

[Original: Spanish]
[29 May 2015]

Spain considers that information and communication technologies provide essential support for all societies worldwide, but their globalization entails serious risks and threats such as cyberespionage, cyberterrorism, "hacktivism" and cyberwarfare.

Following the establishment of the National Cybersecurity Council, Spain has continued to make progress in the development of plans derived from the National Cybersecurity Strategy to increase prevention, protection, detection, analysis, response, recovery and coordination capacities in the face of cyberthreats.

Spain continues to participate actively in the promotion of international cooperation and is closely monitoring all strategic initiatives that affect cybersecurity, both in the European Union and in major international forums such as the Organization for Security and Cooperation in Europe, the North Atlantic Treaty Organization and the Council of Europe.

Spain continues to uphold the importance of the United Nations in the process of achieving international consensus on cybersecurity issues and supports the holding of institutionalized dialogue, which should include other international forums, to promote regional cooperation and the establishment of global standards, best practices, rules of conduct among States and confidence-building measures, with the ultimate goal of guaranteeing the peaceful and secure use of information technologies.

Spain considers that States should achieve consensus in four areas. First, they should develop confidence-building measures of a cooperative nature with the ultimate goal of promoting transparency among States in the area of cybersecurity and strengthening their capacity to neutralize any possible attacks identified as coming from third countries.

Second, Spain considers that States should continue reflecting on how the principles and norms of international law should be interpreted and applied in cyberspace; especially those relating to the threat or use of force, to humanitarian law and to the protection of the fundamental rights and freedoms of the individual.

Third, Spain considers that international cooperation should be strengthened by improving channels of communication, establishing mechanisms for the coordination of Computer Emergency Response Teams, carrying out joint exercises and other similar operations, and promoting judicial and police cooperation mechanisms.

Finally, capacity-building in countries where it is needed should continue to be encouraged and assistance should be provided to recipient States for the development of national laws establishing cybersecurity standards.

The full text of Spain's submission can be found at http://www.un.org/disarmament/topics/informationsecurity/.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[29 May 2015]

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 69/28 entitled "Developments in the field of information and telecommunications in the context of international security", and its present submission builds on its response to resolution 68/243 in 2013. The United Kingdom uses its preferred terminology of "cybersecurity" and related concepts throughout its response, to avoid confusion given the different interpretations of the term "information security" in this context.

The United Kingdom recognizes that cyberspace is a fundamental element of critical national and international infrastructure and an essential foundation for economic and social activity online. Actual and potential threats posed by activities in cyberspace are of great concern. Our response details national and international approaches that have been and will be taken in order to strengthen security and promote cooperation in this field. Those approaches have been underpinned by the national cybersecurity strategy of the United Kingdom, published in November 2011.

The United Kingdom continues to take a leading role in the international debate on cybersecurity. We have provided experts for all four Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and consider that the consensus report of the previous Group showed valuable progress in reaching common understandings on norms of State behaviour in cyberspace and in affirming the applicability of international law in cyberspace. We look forward to the outcome of the current Group's discussions in June 2015. The United Kingdom also welcomes continued discussion of potential future confidence-building measures in cyberspace at the Organization for Security and Cooperation in Europe to build on those successfully negotiated in 2013, and similar work in other regional organizations.

The present response outlines the work of the United Kingdom to support and improve cybersecurity and share best practice, both domestically and worldwide, including working with international partners to tackle cybercrime and major incidents and building cybercapacity and capability. The United Kingdom looks forward to seeing further progress in all of those areas. The United Kingdom is pleased to be actively engaged in those important issues and looks forward to further participation in strengthening capability and international cooperation on cybersecurity.

The full text of the submission by the United Kingdom can be found at www.un.org/disarmament/topics/informationsecurity/.