United Nations A/74/120

General Assembly

Distr.: General
24 June 2019
English
Original: English/French/Spanish

Seventy-fourth session
Item 95 of the preliminary list*

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

Report of the Secretary-General

Contents

* A/74/50.

19-10580 (E) 100719 230719

I. Introduction

1. At its seventy-third session, the General Assembly adopted two resolutions under agenda item 96 on developments in the field of information and telecommunications in the context of international security.

2. On 5 December 2018, the General Assembly adopted resolution 73/27 on developments in the field of information and telecommunications in the context of international security and on 22 December, it adopted resolution 73/266 on advancing responsible State behaviour in cyberspace in the context of international security.

3. In paragraph 4 of resolution 73/27, the General Assembly invited all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 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 3 of the resolution;

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

4. In paragraph 2 of resolution 73/266, the General Assembly invited all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts, to continue to inform the Secretary-General of their views and assessments on the following questions:

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

(b) The content of the concepts mentioned in the reports of the Group of Governmental Experts.

5. Pursuant to that request, on 6 February 2019, 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. Additional replies received after 15 May 2019 will be posted on the website of the Office for Disarmament Affairs (www.un.org/disarmament/ict-security) in the original language received.

II. Replies received from Governments

Argentina

[Original: Spanish]
[15 May 2019]

General appreciation of the issues of information security

Information and communications technology (ICT) provides unprecedented opportunities for economic, social, cultural, scientific and political progress, and the development of such technology is inextricably linked to higher levels of development and well-being. Cyberspace has become a fundamental part of the lives

of individuals and organizations, and essential services increasingly depend on computer networks.

However, while cyberspace has made possible unprecedented levels of interaction and progress, it is also subject to a multiplicity of different threats, and actors who jeopardize the security of people, companies, institutions and States, as well as international peace and security.

Economic development, the provision of essential services, the well-being of citizens and the proper functioning of State bodies rely heavily on cybersecurity.

New risks are on the rise as a consequence of the widespread use of relatively low-cost smart devices that make it possible to access the Internet without a minimum level of security, expanding the scope for potential cyberattacks.

This growth needs to be accompanied and addressed by State policies and corporate responsibility strategies.

Similarly, some States' plans to develop mechanisms for decrypting devices/applications and/or backdoors pose an additional risk.

Efforts taken at the national level to strengthen information security

In 2017, the Argentine Government, through Decree No. 577/2017, established the Cybersecurity Committee, chaired by the Government Secretariat for the modernization of the Executive Office of the Cabinet of Ministers, and with the following members: the Secretariat for Strategic Affairs of the Executive Office of the Cabinet of Ministers, the Ministry of Defence, the Ministry of Security, the Ministry of Foreign Affairs and Worship and the Ministry of Justice and Human Rights. Part of the role of the Committee is to develop a national cybersecurity strategy, as well as a plan of action for its implementation.

The establishment of the Cybersecurity Committee facilitated the creation of forums for the exchange of information about incidents, resulting in responses that were better coordinated; this proved its effectiveness when the Group of 20 was held in Argentina in 2018.

Argentina has a National Critical Information and Cybersecurity Infrastructure Programme established by Resolution 580/2011 of the Executive Office of the Cabinet of Ministers. The Programme is designed to define and protect public and private sector strategic and critical infrastructure, as well as that of international organizations, manage all information on reports of security incidents and direct potential solutions in an organized and consolidated way, among other objectives.

In this context, a protocol has been established for situations where public agencies are highly vulnerable to digital security risks, and which provides for linkages to the private sector.

Work is currently under way to develop a norm that will establish a definition of "critical information infrastructure", criteria for determining whether infrastructure is critical, and categorize the infrastructure of various sectors.

In the framework of the National Critical Information and Cybersecurity Infrastructure Programme, Order No. 2/2013 established the National Computer Security Incident Response Team.

In terms of legislation, cybercrime was incorporated into the Criminal Code in 2008 through Act No. 26.388. In 2013, the National Congress passed Act No. 26.904, criminalizing grooming and increasing the severity of the penalties for offences relating to child pornography on the Internet. In 2017, through Act 27.411, adopted by the National Congress, Argentina acceded to the Convention on Cybercrime. In

January 2019, the National Congress passed Act No. 27.482, amending the Federal Code of Criminal Procedure, which now includes tools for obtaining digital evidence (interception of digital communications, data recording and retention, and computer systems).

Work is currently under way on a draft law to amend the Criminal Code, which will criminalize a number of information technology-related offences, in particular, damaging critical infrastructure.

In order to increase capacity to combat cybercrime, the Ministry of Justice and Human Rights, with the support of international bodies such as the Organization of American States (OAS) and the Council of Europe, gave a number of training workshops on cybercrime, processing of digital evidence and modern investigation methods, for actors in the criminal justice system. The workshops were held in various regions of the country, and were aimed at judges, prosecutors and members of the federal and provincial security forces. From 2016 to now, almost 500 judges and prosecutors throughout the country have participated in these training programmes.

One of the objectives of the Argentine Digital Agenda, adopted by Decree No. 996/2018, is to develop cybersecurity capacity in order to create trust in digital environments. In this connection, to strengthen capacity for awareness-raising on the risks of using social media and the Internet, with a focus on the general population, and particularly the groups considered to be at risk, programmes have been developed to train trainers, in collaboration with the *Punto Digital* programme. Topics including cyberbullying, grooming, phishing, cybersecurity, and strategies for the care and containment of victims and the prevention and detection of computer-related crime, have been addressed, with a focus on youth, adolescents and older adults.

With respect to the protection of personal data, Argentina was one of the first countries of the region to have a regulatory framework for the protection of personal data, through the adoption of Act No. 25.326. Argentina has acceded to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

On 1 June 2019, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its Additional Protocol, will enter into force in the Argentine Republic.

Measures taken to promote international cooperation in the field of information security

Argentina promotes the establishment of agreements at the bilateral, regional and multilateral levels intended to contribute to making cyberspace peaceful and secure, and seeks to participate in all the work of international agencies in the area of cybersecurity and to participate actively in all the international academic and technical spheres where cybersecurity is addressed.

In this regard, Argentina is actively engaged in the activities of the Cybercrime Convention Committee, and supports States that are not yet parties but want to accede to the Convention. Among the tangible advantages that this treaty offers its members is inclusion in the 24/7 Network, which provides a channel for assistance and facilitates criminal investigations between States parties.

However, taking into account the transnational nature of cybercrime and the need for mechanisms to enable a global response, Argentina supports both the processes under the Convention on Cybercrime, and the discussion forums that seek to advance, within the framework of the United Nations, towards the negotiation of an universal legal framework in this area (the Vienna process).

Argentina participated in the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013 and 2014, and seeks to contribute to the discussions in the General Assembly on this topic.

Aware of the vital need for capacity-building, Argentina is a member of the Global Forum on Cyber Expertise and along with the OAS, Chile, Mexico, Estonia and Spain, it participates in the OAS Cybersecurity Initiative.

In November 2018 Argentina acceded to the Paris Call for Trust and Security in Cyberspace.

At the regional level, Argentina participates in the meetings of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace of the OAS Inter-American Committee against Terrorism, and has contributed to the activities of the Observatory for Cybersecurity in Latin America and the Caribbean, providing information for the second edition of the joint OAS-Inter-American Development Bank study entitled *Cybersecurity: Are We Ready in Latin America and the Caribbean?*.

Argentina hosted the second International Forum on Gender and Cybersecurity, co-organized with the OAS, on 29 and 30 May 2018.

Within the context of the Southern Common Market (MERCOSUR), Argentina has promoted the creation of the MERCOSUR Digital Agenda, which also addresses cybersecurity.

At the bilateral level, in 2017 Argentina signed an inter-agency memorandum of understanding on cybersecurity with Spain. The same year, it agreed with the United States to form the intergovernmental, bilateral Cyber Policy Working Group to focusing on cybersecurity issues, and in 2018 Argentina signed an agreement on cooperation in cybersecurity, cybercrime and cyberdefence with Chile. Argentina considers it important to maintain open channels of dialogue on cybersecurity with all countries and regions.

Comments regarding the content of the reports of the Group of Governmental Experts, General Assembly resolution 73/27 and possible measures that could be taken by the international community to strengthen information security at the global level.

Argentina supports and agrees with the content of the concepts mentioned in the reports of the Group of Governmental Experts.

It is the responsibility of States to ensure that cyberspace is peaceful and secure; this makes it critical that they behave responsibly, through the application of existing international law and the development of new voluntary standards, international cooperation and confidence-building measures, in accordance with United Nations General Assembly resolutions 69/28, 70/237, 71/28, 73/187, 73/266 devoted to that issue.

Bilateral, regional and multilateral cooperation is critical for building the capacity of the States that need to strengthen their prevention, detection, alert and response systems for threats in cyberspace.

Effectively combating cybercrime is essential to ensuring that cyberspace is peaceful and secure, and therefore it is a matter of the highest priority to be addressed by inter-State cooperation.

Argentina agrees with the importance of General Assembly resolution 72/27, in particular the set of international rules, norms and principles of responsible behaviour

of States contained in paragraph 1 of the resolution. It should be noted, however, that the nature of threats in cyberspace and the pace at which they evolve make it appropriate to request States to do their best to prevent their territory from being used by non-State actors for internationally wrongful acts using ICTs. However, it is not possible to guarantee that they will be able to do so.

Furthermore, in the light of the global and transnational nature of threats in cyberspace, the emphasis that the international community attaches to capacity-building for all States should be increased, and in particular developing countries should be supported to strengthen their prevention, detection, alert and response systems for threats in cyberspace.

Argentina believes that it is necessary to continue to work within the framework of the United Nations processes, such as the Group of Governmental Experts and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security established by General Assembly resolution 73/27. It is essential to achieve consensus on how international law applies to cyberspace, which requires dialogue and transparency regarding the vision of each State. It is also crucial to develop mechanisms and instruments that can quickly adapt to the changes and new challenges continuously generated by the rapid progress of technology.

Colombia

[Original: Spanish]
[15 May 2019]

General appreciation

The Government of Colombia agrees that it is necessary to strengthen coordination and cooperation between States in order to consider threats and possible cooperative measures to address them; the application of international law to the use of information and communications technology (ICT) by States; and the rules, norms and principles of responsible behaviour of States.

It is of the greatest importance to international stability that States make responsible use of ICT and that its use is promoted as a tool for economic and social development.

Colombia is in favour of a free, open and secure Internet, making it vital that countries possess the tools they need to cooperate effectively to combat cybercrime, that they strengthen their national capacities, and that confidence-building measures between countries are reinforced.

It is essential to recognize and address the challenges associated with matters including digital identity; cooperation with Internet service providers; digital evidence and techniques for its collection, storage, chain of custody, certification and validity; and data protection, privacy and respect for the rights and freedoms of individuals.

However, we believe that cybercrime should continue to be discussed from a technical and political standpoint by the Commission on Crime Prevention and Criminal Justice of the United Nations, through the intergovernmental group of experts on cybercrime as the principal forum, and that new alternative groups that limit countries' participation, such as the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, should not be created.

Colombia is interested in participating in the international discussions of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts. Colombia has nominated a candidate for the latter. Should its participation in the Group of Governmental Experts not be possible, the contributions of Colombia will be channelled through the regional consultation forums established by the Organization of American States (OAS) for that purpose.

Observations relating to General Assembly resolutions 73/266, on advancing responsible State behaviour in cyberspace in the context of international security, and 73/27, on developments in the field of information and telecommunications in the context of international security

The Government of Colombia agrees that coordination and cooperation among States must be improved to promote the responsible use of ICT by States; this is fundamental both for international stability and for ICT playing a real role in social and economic development.

Colombia was an active participant in the Group of Governmental Experts in the period from 2014 to 2015, during which time it obtained the latest context document, and it fully agrees with the concepts, considerations, interpretations and recommendations contained therein.

The Government of Colombia believes that international law should apply to the virtual world as well as the physical world. This stance, or vision, has not only been considered by the United Nations Governmental Groups of Experts, which reached consensus regarding the fundamental ways in which international law is applicable: it is also reflected in the confidence-building measures of the Organization for Security and Cooperation in Europe and the Association of Southeast Asian Nations, the Group of Seven Lucca Declaration on responsible State behaviour in cyberspace, and the unanimous support of the group of experts who authored the Tallinn Manual 2.0. In any event, the applicability of international law to cyberoperations requires further study in order to ensure there are no grey areas or differences in interpretation regarding how it applies.

For countries that are less advanced technologically it is of the utmost importance to establish agreements to ensure that cyberspace does not become a stage for incrementally increasing conflict, because of the potential effects on such countries, whether they become targets of cyberoperations or become victims of use as "proxy States" because they lack sufficient preventive capacity.

In less technologically advanced countries, any harm to critical cyberinfrastructure can have an enormous impact. This is not only because of dependence on ICT and the shift towards the automation of industrial processes using technologies connected to the Internet, but also because of the lack of awareness of risks and threats and the lack of the resources needed to strengthen the digital security of the companies that manage such infrastructure.

We believe it is essential to initiate discussions at the highest level regarding the implications of the Charter of the United Nations and its applicability to the maintenance of peace and stability, in order to foster an open, secure, stable, accessible and peaceful ICT environment.

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

In order to address uncertainties, risks, threats, vulnerabilities and digital incidents, in 2011, the Government issued National Council for Economic and Social

Policy document no. 3701, “Policy guidelines for cybersecurity and cyberdefence”. This policy has focused the country’s efforts to counter the increase in digital threats, which were affecting it significantly, and to develop a regulatory and institutional framework to address cybersecurity-related challenges. The following is an overview of the progress made in the implementation of these policy guidelines, and the revision of the guidelines in 2014 and 2015.

The overall objective of document no. 3701 was to strengthen State capacity to address threats to national security and defence in the cyberdomain (cybersecurity and cyberdefence), to create an environment and conditions where cyberspace is protected. Three specific objectives were set in order to achieve this general objective: (a) establish suitable bodies for prevention, coordination, response, monitoring and control of cyberincidents and emergencies and the formulation of recommendations to address threats or risks to national cybersecurity and cyberdefence; (b) provide specialized training on information security and broaden the scope of cyberdefence and cybersecurity research; and (c) strengthen legislation on cybersecurity and cyberdefence, and international cooperation; and accelerate the accession of Colombia to the various international instruments in this area.

To develop this policy, and with a new vision based on international best practice and, in particular, on principles and recommendations of multilateral organizations such as the North Atlantic Treaty Association (NATO), the Organization for Economic Cooperation and Development, the International Telecommunication Union and the OAS, and global private sector organizations which have analysed how to address digital security in the current digital environment, the national Government, in 2016, issued National Council for Economic and Social Policy document no. 3854, “National digital security policy”, which is valid up to December 2019 and in which the following objective is set: to enhance the capacity of the various stakeholders to identify, manage, address and mitigate the risks to the digital safety in their online socioeconomic activities, in a framework of cooperation, collaboration and assistance. It is expected that this will contribute to the growth of the national digital economy, which in turn will boost the country's economic and social prosperity.

To develop the overarching objective of this public policy, the following specific objectives were set:

(a) establish an institutional framework for digital security consistent with an emphasis on risk management;

(b) create the conditions to enable the various stakeholders to manage the digital security risk in their socioeconomic activities, and build confidence in the use of the digital environment;

(c) enhance the security of individuals and the State in the digital environment, at the national and transnational levels, with an emphasis on risk management;

(d) strengthen national defence and sovereignty in the digital environment, with an emphasis on risk management; and

(e) establish permanent and strategic mechanisms to promote cooperation, collaboration and assistance in digital security matters at the national and international levels.

From the time the National Council for Economic and Social Policy adopted the action and monitoring plan for the national digital security policy, in April 2016, the competent public entities have been carrying out the activities envisaged in the Plan, with a view to achieving the overall goal and specific objectives of the policy.

In summary, out of the set of actions taken, the following achievements are worth highlighting:

- We have initiated the establishment of a coordinated institutional framework, which involves the various stakeholders, for the implementation of the national digital security policy; in particular, we have established the position of National Digital Security Coordinator within the Office of the President of the Republic and ensured that the work of the Cyber Emergency Response Group of Colombia will continue.
- We have begun the process of designing, and putting into practice in the national Government, a digital security risk-management model, which takes into account the conceptual framework of this policy, international security standards and the comprehensive national risk management framework.
- We have begun to create the conditions to enable the various stakeholders to manage the digital security risk to their socioeconomic activities, and to build confidence in the use of the digital environment; in particular we are conducting a study on the impact of digital crimes and offences in the country and adjusting the regulatory framework for the ICT sector to enhance digital security.
- We have drafted plans to strengthen operational, administrative, human and scientific capacity, as well as the physical and technological infrastructure of the bodies that comprise the current national government institutions.
- We have signed international cooperation agreements with partner countries and important industry representatives aimed at strengthening capacity and the exchange of information regarding threats. In 2017, NATO unanimously approved the signing of an individual collaboration and cooperation programme with Colombia, making our country the first in Latin America to acquire this status and become a global partner. One of the points included in this legal instrument is the improvement of cyberskills. Colombia considers it essential to strengthen the existing initiatives that are operational in various settings within the United Nations system.

With regard to the objective of establishing an institutional framework for digital safety consistent with an emphasis on risk management, we have made the following progress: the establishment of the position of National Digital Security Coordinator (equipped with technical and legal tools), as well as the establishment of a Digital Security Committee, which will provide guidance on management and performance to the civil service, and serve as the highest-level inter-institutional and intersectoral entity in the national Government for high-level guidance on digital security issues. We have also designed key instruments such as the digital security risk-management model, which the national entities of the executive branch are obligated to adopt and put into practice, and which the Administrative Department of the civil service included in the *Guide for Addressing Management-, Corruption- and Digital Security-related Risk and Designing Audits for Public Entities*, in August 2018.

Challenges identified include the need to implement and strengthen digital security risk management in the bodies responsible for the cybersecurity and cyberdefence of the institutional framework established. It is also necessary to strengthen sectoral capacity by establishing a more efficient method for the promotion and creation of sectoral Computer Security Incident Response Teams, establish a road map for the effective development of the Digital Security Committee, establish an effective protocol for links between sectoral and local liaison facilities and national digital security coordination facilities, as well as enable all the various stakeholders to identify, assess and effectively manage risk.

With regard to the second objective, on creating the conditions to enable the various stakeholders to manage the digital security risk in their socioeconomic activities, and build confidence in the use of the digital environment, some progress has been made on developing a draft national digital security agenda. However, it is necessary to continue strengthening the linkages between the discussions of all the various stakeholders, have more academic contributions (research) on the topic and support public entities to adopt the digital security risk-management model. Several awareness-raising campaigns have been carried out, such as the programme "I trust ICT", and, with the support of the OAS, the *Study of the Economic Impact of Cyber Incidents, Threats and Attacks in Colombia* for 2017 was produced, and the same study is being conducted for 2018.

As challenges, we recognize the need to identify areas related to digital security in which research should continue and be strengthened, identify a clear and effective model for coordination and communication that facilitates the establishment of the necessary legal framework on digital security that will support the digital transformation of the various stakeholders, efficiently communicate the outcome of strategic studies at high levels within the Government to guide decision-making and to reorient the strategy for the development of educational content to be included in the academic curricula used at the different levels in the educational system.

With respect to the third objective, enhancing the security of individuals and the State in the digital environment, at the national and transnational levels, with an emphasis on risk management, progress has been made on plans for building the capacity of key actors, reports on cybercrime statistics and strengthening of the risk-management capacity of those responsible for cybersecurity in the country.

The challenge is the urgent need to implement the plans to strengthen operational, administrative, human and scientific capacity, as well as the physical and technological infrastructure of the bodies and entities responsible for cybersecurity, and to establish guidelines for adjusting the existing legal and regulatory framework to match needs relating to: (a) analysis, anticipation, prevention, detection, response to and investigation of cyberoffences, cybercrime and phenomena, in the digital environment, and offences and crimes involving the use of the digital environment; (b) prosecution and criminalization of new forms of crime, including cyberoffences that facilitate money-laundering, and (c) modernization of the agencies for security, national defence and intelligence in the digital environment, in accordance with the basic principles of the national digital security policy.

With regard to the fourth objective, strengthening national defence and sovereignty in the digital environment, with an emphasis on risk management, progress has been made in the development of plans for enhancing the capacity of key actors, the regular updating of the catalogue of national critical cyberinfrastructure, the creation of some of the content for the critical cyberinfrastructure protection plans, the establishment of a number of sectoral cybersecurity incident response teams to facilitate the appropriate management of digital incidents that affect national critical cyberinfrastructure (such as government, financial sector and electricity sector infrastructure) and the participation of certain stakeholders in simulation and training exercises, at the national and international levels, with a view to developing the skills and abilities of the various stakeholders responsible for the national critical cyberinfrastructure and national defence in the digital environment.

The challenges to achieving this objective are the need to reshape, from the highest level, the guidelines for the protection and defence of national critical cyberinfrastructure, taking into account the new situation, and the need to issue a formal protocol for managing and responding to digital security incidents that affect

such infrastructure. Equally, it is necessary to draw up a national Government strategy for the centralization of awareness-raising and training on digital security in relation to national defence.

Lastly, with regard to the fifth objective, the establishment of permanent and strategic mechanisms to promote cooperation, collaboration and assistance in digital security matters at the national and international levels, we have made progress in adhering to mechanisms that foster cooperation, collaboration and assistance in relation to digital security at the international level. For instance, we can highlight the process of accession to the Convention on Cybercrime, and the progress in the development of a draft strategic agenda for international cooperation, collaboration and assistance.

With respect to the challenges, it is necessary to identify and prioritize the bodies in which Colombia should participate on digital security matters, and to identify a clear and effective model for coordination and communication between stakeholders that will enable the drafting and implementation of strategic documents for the promotion of cooperation, collaboration and assistance at both the national and international levels in digital security matters.

In the light of all of the above, and as the national digital security policy established in National Council for Economic and Social Policy Document No. 3854 of 2016 contains a plan of action that expires in 2019, the national Government, with the support of the OAS, is in the process of drafting a new policy that will address the challenges cited.

Cuba

[Original: Spanish]
[29 April 2019]

New ICT should be used in a peaceful manner for the common good of humankind and to further the sustainable development of all countries, irrespective of their level of scientific and technological development.

Such scientific and technological developments can have civil and military uses and it is necessary to prevent this progress from jeopardizing the international security of States.

The only way to prevent cyberspace from becoming a stage for military operations is through joint cooperation among all States.

In this regard, we support the establishment of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security pursuant to General Assembly resolution 73/27, with a view to making the United Nations negotiation process on security in the use of ICT more democratic, inclusive and transparent.

We consider it necessary to establish a legally binding international regulatory framework which is complementary to existing international law but applies to ICTs.

All States must respect existing international standards in this field. Access to the information or telecommunications systems of another State should be in line with the international cooperation agreements concluded and should be based on the principle of consent of the State concerned. The nature and scope of exchanges must respect the laws of the State which is granting access.

The hostile use of telecommunications, with the declared or hidden goal of subverting the legal and political order of States, is a violation of internationally agreed norms in this area and an illegal and irresponsible use of this media.

Through illegal radio and television broadcasts, the United States has been constantly attacking Cuban airwaves, disseminating programming specifically designed to incite the overthrow of the constitutional order established by the Cuban people.

On average in 2018, 1,653 hours of programming against Cuba per week were transmitted illegally, using 20 frequencies, from the United States, in contravention of the purposes and principles of the Charter of the United Nations, international law and the rules of the International Telecommunications Union.

Once again, Cuba calls for an immediate end to these aggressive policies which violate the sovereignty of Cuba and which are, furthermore, incompatible with the development of ties based on mutual respect and cooperation between States.

The economic, commercial and financial embargo imposed by the United States Government against Cuba for nearly 60 years has caused severe losses to the Cuban people, including in the use and enjoyment of ICTs.

The Heads of State and Government of Latin America and the Caribbean, at the second Summit of the Heads of State and Government of the Community of Latin American and Caribbean States (CELAC), 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 in their levels of development, to practice tolerance and to live together in peace with one another as good neighbours.

At the fifth Summit of the Heads of State and Government of CELAC, held in Punta Cana (Dominican Republic), in January 2017, the importance of ICTs, including the Internet, as tools to foster peace, human well-being, development, knowledge, social inclusion and economic growth was again highlighted.

Egypt

[Original: English]
[9 May 2019]

Introduction

In the last three decades, the world has witnessed a dramatic surge in the use of the Internet, smartphones and modern information and communications technology (ICT) gadgets, coupled with an overwhelming amount of ICT uses in the fields of business, commerce, government services, education, knowledge, entertainment, tourism, health care and other economic, social and cultural activities. Alongside the opportunities brought about by the continuous growth in telecommunications and Internet usage and the proliferation of e-transactions and e-services, it is important to be cognizant of the threats and challenges that target the ICT infrastructure and e-transactions in general and face them, as they undermine confidence and trust in e-services and e-business in particular.

Hence, Egypt attaches immense importance to the considerable role of developing and applying the latest information technologies and means of telecommunication in order to achieve economic and social progress at both the national and international levels. Egypt also actively supports the use of ICTs for the common good of mankind and to further the sustainable development of all countries,

irrespective of their levels of scientific and technological development. Moreover, Egypt believes that the United Nations should play a central role in leading the relevant international efforts and promoting dialogue among Member States to develop a common international understanding of the application of international laws and norms, rules and principles for responsible State behaviour in the information sphere, including the implementation of legally binding instruments.

The most significant cyberchallenges and threats

1. Threat of penetrating and sabotaging ICT infrastructure

New types of extremely serious cyberattacks have recently emerged, aimed at disrupting critical services and deploying malware and viruses to destroy or disrupt ICT infrastructure and critical industrial control systems, especially in key facilities, including entities of nuclear power, oil, natural gas, electricity, aviation, various forms of transportation, key national databases, government services, health care, and emergency aid services. Such cyberattacks deploy several channels, including wireless networks and mobile memory, and other common channels such as emails, websites, social media and telecommunications networks, which may have a significant impact on the utilization of critical infrastructure and associated services and businesses. In practice, critical facilities may be vulnerable to advanced cyberattacks, even if they are not directly connected to the Internet.

2. Threat of cyberterrorism and cyberwarfare

Recently, dangerous types of cyberattacks and cybercrimes have spread, using advanced technologies, such as cloud computing, wiretapping and network intrusion devices, advanced encryption, and automated hacking tools targeting computer systems and databases. Additionally, advanced malicious software (malware) may be deployed to undermine network security systems and compromise computer systems to form botnets, which can be used later on in a variety of criminal and illegal activities. An automated botnet may consist of tens, hundreds of thousands or millions of compromised computers that can be used to launch serious cyberattacks, such as Distributed Denial of Service attacks on targeted networks and websites for destructive, terrorism and/or extortion purposes.

The development of complex and sophisticated computer viruses often requires advanced knowledge levels and non-conventional expertise, available only in technologically advanced countries, to be used for tactical, strategic and warfare purposes as well as in addition to, or sometimes instead of, conventional military attacks, in what is known as cyberwarfare. However, such malicious technologies are being transferred, copied or reproduced by terrorist organizations for use in terrorist operations and organized crime, as well as in threatening and disrupting the ICT infrastructures for extortion and/or industrial espionage purposes. Egypt reaffirms the positions stated by leading cybersecurity experts who expect an increased proliferation of ferocious and sophisticated cyberattacks in the coming period.

3. Threat of digital identity and private data theft

Digital identity theft is one of the most serious crimes that threaten Internet users and the future of e-services. Stolen credentials and personal data can facilitate impersonating individuals in cyberspace and may result in monetary and property loss or may entangle the names of the victims in suspicious or illegal activities. The identity thief usually uses information already available on the Internet, especially on open social media and professional networks; national databases; networks of government services, social security services and health care; e-commerce websites; virtual markets; e-payment networks; automated teller machines (ATMs); and stock

exchanges. In addition, tools and systems used in performing e-transactions may be compromised, stolen or damaged, which poses a serious threat to the interests of users and the future of e-services. Extensive and widespread attacks may affect the national financial sector. Data of public institutions and companies may also be stolen, resulting in considerable material and credibility losses, damage to reputations, customer attrition and reduction in the value of intangible assets, which may harm the national economy at large.

Key aspects of the seriousness of emerging cyberthreats

Emerging cyberthreats may be very serious due to three main aspects:

1. They often deploy advanced and sophisticated technologies; highly developed countries and large companies often have a monopoly on these technologies. Many of these technologies are top secret and not available for export. Furthermore, the exportable versions of some technologies may contain backdoors or vulnerabilities that make them a source of additional threats.

2. They can spread easily, and rapidly spreading malicious viruses and launching Distributed Denial of Service attacks and other advanced cyberattacks can occur very quickly and easily, due to the widespread use of ICTs and because of the ease of launching these attacks remotely and transmitting viruses across borders from anywhere and at a low cost. It is also difficult and often impossible to trace the main origin of those threats and risks in time to address and overcome them.

3. They can have a widespread impact; cyberattacks may have an extensive direct and indirect impact on the infrastructure, causing substantial damage and losses. In addition, they may be executed remotely and expand suddenly in an unpredictable manner, while potentially affecting critical entities and large numbers of citizens (thousands or millions).

The way forward: towards facing the cyberchallenges

Cyberattacks and cybercrimes may transcend the geographical boundaries of countries and usually rely on both traditional and technical organized crime networks. Confronting such attacks and crimes must therefore include the traditional mechanisms of international cooperation to combat crimes and face cyberthreats, as well as legislative and regulatory frameworks with special mechanisms to handle the emerging technical developments. Effective response to cyberattacks and cybercrimes necessitates cooperation and coordination at the national level, among partners providing and operating infrastructure at critical sectors and partners providing services, including government agencies, institutions and companies. Additionally, international and regional cooperation and coordination are highly essential and need to include key international organizations, regional gatherings and professional and specialized international forums.

Egypt's contributions

Egypt realizes the importance of international cooperation in addressing cybersecurity challenges. Egyptian experts have contributed to a number of relevant governmental groups of experts mandated by the General Assembly to reach agreed recommendations on cybersecurity from the international security perspective. Furthermore, as a member of the International Telecommunications Union (ITU), Egypt was part of the ITU's High-Level Experts Group on Cybersecurity and took part in its Global Cybersecurity Agenda activities. In addition, Egypt proposed the establishment of ITU's Council Working Group on Child Online Protection and chaired the Group from 2010 until 2017. Egypt also participates and hosts regional cyberdrills and cybersecurity conferences and workshops that are organized by

international organizations such as ITU, the Organization of Islamic Cooperation, the Organization for Security and Cooperation in Europe, the Organization for Economic Cooperation and Development and the Forum of Incident Response and Security Teams. Also, Egypt participates in international and regional cybersecurity studies with professional organizations such as the Global System for Mobile Communications Association. Moreover, Egypt actively participates in regional efforts in African and Arab contexts to promote confidence-building and capacity-building transparency measures and the dissemination of best practices. Egypt has also engaged in bilateral consultations and negotiations with a number of States and international organizations and partners to conclude agreements on bilateral cooperation in this strategic domain.

At the national level, and in the light of article (31) of the Egyptian Constitution, a Supreme Council for Critical Information Infrastructure Protection and Cybersecurity (namely, the Egyptian Supreme Cybersecurity Council), was established at the cabinet-of-ministries level late in 2014. The Council is chaired by the Minister of Communications and Information Technology and has members from the critical sectors as well as from key security agencies. At the operational level, the national Computer Emergency Readiness Team has become the Council's technical arm. The Council developed Egypt's first national cybersecurity strategy in 2017. The scope, structure and objectives of the strategy are in line with the national requirements and abide by the international norms, rules and principles. Likewise, the implementation of the strategy follows the same spirit.

Conclusion

Egypt reiterates the urgent need to intensify capacity-building and technical assistance for developing countries in the field of ICT security, especially taking into consideration that in many instances, the security of cyberspace may be only as strong as its weakest link.

Moreover, the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General to the General Assembly represent significant steps in the right direction. Chief among them is highlighting the central importance of the commitments of States to the principles of the Charter of the United Nations and other principles of international law, including sovereign equality; the settlement of international disputes by peaceful means; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States. The final aim is to achieve a reliable and secure information and communications technology environment consistent with the need to preserve the free flow of information.

In light of the severity of emerging cyberthreats, Egypt highly values and supports the recommendation in resolution 73/27 that establishes an open-ended working group, acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States with a view to making the United Nations negotiation process on security in the use of information and communication technologies more democratic, inclusive and transparent. Moreover, Egypt looks forward to joining and supporting the efforts of the open-ended working group to develop ways for the implementation of these rules, norms and confidence-building measures.

Egypt also looks forward to engaging with the activities of the Group of Governmental Experts established pursuant to resolution 73/266, including the activities of collaboration with relevant regional organizations through a series of consultations.

France

[Original: French]
[14 May 2019]

1. General appreciation of the issues of cybersecurity

France wishes first to reiterate that it does not use the term "information security", preferring the terms "information systems security" or "cybersecurity". As an active proponent of freedom of expression online (as illustrated by its co-sponsoring of Human Rights Council resolution 38/7 in 2018), France does not consider information as such to be a potential source of vulnerability requiring the establishment of protective measures. That belief is without prejudice to measures taken in a proportionate and transparent way, under conditions strictly established by law, in accordance with article 19 of the International Covenant on Civil and Political Rights.

The term "cybersecurity" is therefore more accurate, as it refers to the ability of an information system to be resilient in the face of events originating in cyberspace that may threaten the availability, integrity or confidentiality of data stored, processed or transmitted, and related services provided or made accessible by these systems. Cybersecurity uses techniques to ensure the security of information systems and strengthens the fight against cybercrime and the implementation of cyberdefence.

France believes that the digital space must remain a space of freedom, exchange and growth, underpinning prosperity and progress in our societies. As previously emphasized in its national strategy for digital security[1] in 2015, France considers digital technology, through its new uses and services, to be a driver of innovation. It is engendering change in the majority of professional fields. It is transforming industries and businesses, making them more flexible and competitive. It offers opportunities to the members of society by improving daily lives through online communications, trade and information services, as well as bringing economic opportunities, thanks to increased competition and the sharing economy.

This open, secure, stable, accessible and peaceful cyberspace, which France has promoted over the past three decades and which holds economic, political and social opportunities, is now threatened by the development of new destructive practices. The specificities of the digital space (including relative anonymity, low costs and ease of access to malicious tools, easy operation and the proliferation of vulnerabilities) have allowed a number of actors to develop a digital arsenal used for espionage, illegal trafficking, destabilization and sabotage. While some low-level threats are not matters of national security, but rather a form of crime, the use of cyberweapons against State information systems, critical infrastructure or major businesses can have serious consequences.

Issues related to cybersecurity are now an integral part of the power strategies and power relationships that govern international relations; this is both a priority and a prime political issue. As highlighted in the 2017 strategic review of defence and

[1] Available at www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

national security[2], the mass digitization of our societies over the past decade and the worldwide network of information and communication systems are leading to the emergence of both new threats and new opportunities. They allow everyone to access powerful tools for expression, influence, propaganda and information, huge volumes of data but also significant means of attack. They promote the rise in power of new private actors establishing themselves in the international arena and becoming at times a challenge the sovereignty of States but also at times essential partners. They are de facto transformers of the power relationships between State actors, non-State actors and the private sector.

We all have a part to play in preserving, developing and promoting an open, secure, stable, accessible and peaceful cyberspace. In response to the common threats that affect international stability and security, France has been taking an active approach to policy and diplomacy for many years with a view to reinforcing security, trust and stability in cyberspace.

2. Efforts taken at the national level to strengthen cybersecurity and promote international cooperation in this field

(a) Improving cybersecurity in France

The strategic direction taken in recent years at the highest level of the Government of France continues to uphold cybersecurity as a priority area for action by the authorities.

France continues to scale up and develop its national strategy. Over the past decade, measures taken have included the creation and scaling-up of the national agency for information systems security since 2009; the establishment of the first strategy for defence and information systems security in France in February 2011; the strengthening of legal tools and a substantial increase in the resources allocated to cybersecurity through the latest military programming laws; the publication of a cyberdefence pact by the Ministry of the Armed Forces in February 2014; and the development of a centre of excellence for cybersecurity that aims to drive the development of training, academic research and the industrial and technological base for cybersecurity. In follow-up to such measures, France is also implementing a policy of transparency within its strategy that is both national and international in nature.

Since 2015, France has had a national strategy for digital security designed to support the digital transformation of French society. In terms of security, it puts forth the provision of a strong response to malicious cyberactivity and seeks to give French businesses a competitive advantage through digital security.

In December 2017, this document was supplemented by the international digital strategy of France,[3] which sets out the principles and objectives pursued by France in the digital sphere at the international level. This strategy is centred around three main pillars (governance, economics and security) and aims to:

- promote a digital world that is open, diversified and trusted at the global level;
- put forward a European model of balance between economic growth, fundamental rights and freedoms and security;
- strengthen the influence, attractiveness, security and trade positions of France and French actors in the digital world.

[2] Available at www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.

[3] Available at www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

The strategic review of cyberdefence,[4] presented in February 2018, establishes a doctrine for cybercrisis management and clarifies the national strategic objectives of cyberdefence. As a demonstration of the relevance of the French model and the primary responsibility of the State for cybersecurity, the review is structured around seven main principles:

- improving the protection of information systems in our country;
- fending off attacks through a set of defensive measures, strengthened resilience and capacity to react and respond;
- the affirmation and exercise of digital sovereignty in France;
- a more effective criminal justice response to cybercrime;
- the promotion of a shared culture of information security;
- participation in the development of a secure and trusted digital Europe;
- international action for collective governance and control of cyberspace.

The military programming law for 2019–2025[5] provides, in continuity with previous legislation, a significant increase in the resources allocated to cyberdefence, particularly in terms of staff. It contains a recruitment target of 1500 additional personnel, aiming to increase the number of personnel deployed to address these issues within the Ministry of the Armed Forces to 4000 by 2025.

The following actors contribute to the effectiveness of the technical and operational strategy in France:

- The national agency for information systems security is responsible for prevention (including through normative action) of information technology incidents that target the Government and essential operators, and for response to such incidents. It now employs 600 people and continues to grow. It has established itself as the focal point for the definition of relevant cybersecurity standards.
- The Ministry of the Armed Forces has the dual mandate to ensure the protection of networks that safeguard its activities and to integrate operations in cyberspace into military action. In order to consolidate the efforts of the Ministry in this area, a general commanding officer for cyberdefence, under the command of the Chief of Staff of the armed forces, was appointed in September 2017. In this connection, the Ministry of the Armed Forces issued a defensive policy to combat cybercrime at the beginning of 2019; at the same time, an initial public statement of the doctrine on the offensive fight against cybercrime for military operations was presented by the Chief of Staff of the armed forces.
- The mission of the Ministry of the Interior and the Ministry of Justice is to combat all forms of cybercrime, targeting institutions and national interests, economic actors and public authorities as much as private individuals.

(b) Promotion of international cooperation for the stability and security of cyberspace

Strengthening strategic stability and international security in cyberspace is a priority objective for France. As the strategic review of cyberdefence states, “cooperation within the international community in cyberspace is an effective way to

[4] Available at www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

[5] Available at www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte.

increase stability, through greater mutual knowledge and even trust between stakeholders, as well as establishing mechanisms for joint crisis management, communication and de-escalation." France's efforts in the promotion of international cooperation on issues of cybersecurity take place at the European and international levels.

Preventing crises by strengthening cooperation and capacity development

France considers crisis prevention to be the main objective of its work within the digital space. Thus, as highlighted in the strategic review of cyberdefence, "strengthening protection, resilience and the cooperation of all actors in cyberspace directly contributes to the strengthening of our national security". Achieving this goal requires the strengthening of technical, operational and structural cooperation with State partners and international organizations in order to develop the respective capacities of these different actors and the resilience of cyberspace worldwide.

Owing to the high level of connectivity between networks and societies, France believes that cybersecurity for all will only be ensured once each State has sufficient capacity to secure its own information systems. It is therefore making investments in capacity-building for cybersecurity partners, through bilateral or multilateral initiatives. Such an investment in cooperation is beneficial to all parties: it allows us to remain up to date by engaging with our peers and learning from them, and fosters mutual enrichment of knowledge and expertise and the development of trust among the actors involved.

At the technical level, the national agency for information systems security is continuing the establishment of partnerships with its counterparts in many countries in order to encourage the sharing of critical data such as information regarding weaknesses or faults in products and services. In addition, the national agency for information systems security Computer Emergency Response Team is active in several multilateral networks (the Forum of Incident Response and Security Teams, the European Task Force of Computer Security and Incident Response Teams, the European Government Computer Emergency Response Team Group, the Computer Security Incident Response Team Network of the European Union), allowing it to maintain contact with other computer emergency response teams all over the world.

France is conducting a proactive policy for operational and structural cooperation. In recent years, France has deployed international technical experts in cybersecurity in the internal security forces of partner countries. France is also working with Senegal to launch the activities of the national school for cybersecurity in Dakar, an institution with a regional scope inaugurated at the end of 2018. The aim of the project is to provide short and adaptable training courses for cybersecurity professionals and senior officials from West Africa as a matter of priority.

In order to enhance cyberresilience at the European Union level, France is contributing to the development of a voluntary cooperation framework for the prevention and resolution of incidents. It is based in particular on the development of common operational standards and procedures for cooperation between partners, which are tested through pan-European exercises. France has also participated in the creation of a "cyber toolbox" which provides a European framework for a joint diplomatic response to cyberattacks, through the use of prevention, cooperation and stabilization measures.

France has also supported the adoption of European regulations that take into account the requirements for competitiveness and the potential of digital technology, while continuing to protect citizens, businesses and Member States (including the right to privacy and personal data protection, protection of critical infrastructure and the fight against terrorist content online). This was illustrated by the adoption of

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, as well as through the forthcoming entry into force of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). France also actively supports the adoption of a European Union regulation aiming to prevent the dissemination of terrorist content online and to impose uniform obligations on Internet providers.

Finally, France is working to ensure that the industrial policy of the European Union supports advanced research and development capacities in order to enhance the deployment of digital technology and services with reliable and assessed security.

Within the North Atlantic Treaty Organization (NATO), at France's initiative, the Allies adopted at the Warsaw Summit in June 2016 a commitment to cyberdefence, the "Cyber Defence Pledge". This Pledge ensures that every member State of NATO devotes an appropriate share of its resources to the strengthening of its cyberdefence capabilities, thereby improving overall security for all. In May 2018, France hosted the first ever conference on the Pledge. The allies recognized cyberspace as an area of operations, thus compelling NATO to defend itself in that area as it does in the areas of land, air and sea.

Preventing crises by developing standards that regulate the behaviour of actors in cyberspace

France believes that the emergence of a collective cybersecurity framework can only be built on balances defined by international law. The French international strategy for digital security also highlights the importance for France to pursue a cooperative dialogue, both bilaterally and multilaterally, with all relevant public and private stakeholders and all willing international partners.

France has played an active role in negotiations within the United Nations conducted within the framework of the last five meetings of Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. It will continue its commitment in the resumption of discussions both in the Group of Governmental Experts and in the open-ended working group to contribute its vision of a digital space of freedom, exchange and growth that determines the prosperity and progress in our societies. It is also engaged in other international forums where issues on the security of the digital space are addressed.

In 2006, France ratified the Budapest Convention, which provides a legal basis to establish various offences in connection with combating cybercrime and provides for flexible and modern means of international cooperation in this area, for example, the establishment of a network that runs day and night to expedite assistance procedures between States parties. France is now calling for universalization of the Budapest Convention, which today has 63 States parties representing all continents. It is actively participating in the negotiation of the Convention's second Additional Protocol, which aims to further strengthen international cooperation in this area, developing police cooperation and mutual assistance in criminal matters, notably in terms of access to electronic evidence. Furthermore, France supports the work of the open-ended intergovernmental group responsible for conducting an in-depth study of

the issue of cybercrime, confirming the central role of the United Nations Office on Drugs and Crime in that area.

The Paris Call for Trust and Security in Cyberspace[6], submitted by the President of France at the Internet Governance Forum held at the United Nations Educational, Scientific and Cultural Organization on 12 November 2018, testifies to the country's active role in the promotion of a secure, stable and open cyberspace. This text, today supported by 66 countries and nearly 500 non-State entities, aims to promote certain fundamental principles for the regulation of the digital space, including the application of international law and human rights law in cyberspace, the responsible behaviour of States, the monopoly on legitimate violence by States and recognition of the specific responsibilities of private actors.

France has also been involved from within the Organization for Economic Cooperation and Development (OECD). It organized the first meeting of the OECD Global Forum on Digital Security for Prosperity in December 2018, on the theme of the responsibility of private sector actors for digital security.

The Group of 7 (G7) Ise-Shima Cyber Group, created in 2016, led to the adoption of an ambitious declaration in 2017 known as the Lucca Declaration, concerning standards for responsible behaviour in cyberspace. During its presidency in March 2019, France proposed the launching of a follow-up mechanism for the implementation of approved standards and recommendations at the United Nations level, affirmed through the Dinard Declaration on the cybernorm initiative.[7]

France is working to ensure that the work of the Group of 20 (G20) addresses the fundamental issues of competition in the digital economy, new methods of regulation, governance and digital security, in line with the Paris Call for Trust and Security in Cyberspace.

As an active participant in the informal working group on cybersecurity of the Organization for Security and Cooperation in Europe (OSCE), France continues to promote the implementation of the 16 confidence-building measures developed by the OSCE on cyberissues. This includes piloting of the implementation of the confidence-building measure on the protection of critical infrastructure.

In order to strengthen the fight against the proliferation of malicious tools and techniques, France has supported the inclusion of intrusion software on the list of dual-use goods of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. France believes that regulatory efforts must be pursued in this way by including certain cybertools on the list of war materiel, determined in accordance with the gravity of their effects.

France believes that many of the challenges related to cybersecurity should be addressed through a multi-actor or multi-stakeholder approach, in order to taken into account the role and the specific responsibilities of non-State actors. In that regard, France supports the work of the Global Commission on the Stability of Cyberspace. The Commission develops proposals for standards and policies that aim to strengthen international security and stability and to guide responsible State behaviour in cyberspace.

[6] Available at www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf.
[7] Available at www.diplomatie.gouv.fr/IMG/pdf/g7_-_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf.

3. Relevant international concepts aimed at strengthening global cybersecurity

(a) Concepts related to preservation of international peace and security

In order to ensure an open, secure, stable, accessible and peaceful cyberspace, France reaffirms its commitment to the applicability of international law, including the Charter of the United Nations in its entirety, international humanitarian law and international human rights law, to the use of information and communications technology by States.

Public international law

In its 2013 report, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security set out the principles and rules of international law governing the actions of States in cyberspace. Even given the specific characteristics of cyberspace, such as anonymity and the role of private actors, international law provides the means necessary to responsibly control the behaviour of States in that environment. Failure of attribution should therefore not pose an insurmountable obstacle to the implementation of existing international law.

The principle of sovereignty applies to cyberspace. In this connection, France reaffirms its sovereignty over information systems, individuals and cyberspace-related activities on its territory, in accordance with its obligations under international law. Unauthorized penetration of French systems or the generation of effects in French territory through the use of cyberspace by a State entity or by non-State actors acting under the direction or control of a State may constitute a violation of sovereignty.

The scope of the measures that States can take to respond to a possible cyberattack is a function of the seriousness of the attack: the more serious the cyberattack, the wider the scope of the measures. A cyberoperation can be understood as a use of force prohibited under paragraph 4 of Article 2 of the Charter of the United Nations. Whether that threshold has been crossed is not a function of the means of the cyberattack, but rather its effects. If its effects are similar to those of conventional arms, a cyberoperation could constitute a use of force. In the view of France, if the scope or impact of a major cyberattack perpetrated by a State, or by non-State actors acting under the supervision or instruction of a State, reaches a sufficient threshold (such as substantial loss of life, significant material damage, insufficient critical infrastructure with significant consequences), and is attributable to a State, that could constitute "armed aggression" under article 51 of the Charter and thus justify a claim of self-defence. The right of self-defence could be exercised by conventional or electronic means, if necessary and proportionate. The characterization of a cyberattack as "armed aggression" under article 51 of the Charter is a political decision to be made on a case-by-case basis in the light of criteria established by international law.

France does not believe that it is necessary at this stage to establish a new international legally binding instrument dedicated to the challenges of cybersecurity. Existing international law applies to cyberspace, as it does to other spheres, and must be respected.

International humanitarian law

France supports the application of international humanitarian law to cyberoperations conducted in the context of and in relation to armed conflicts.

While offensive cyberoperations are currently carried out in tandem with conventional military operations, the possibility of an armed conflict consisting exclusively of digital activities cannot be excluded in principle, as it is based on the potential for cyberoperations to reach the threshold of violence required to qualify as an international or non-international armed conflict.

Despite their non-material nature, such operations remain subject to the geographic scope of application of international humanitarian law; in other words, their effects are confined to the territories of the States parties to an international armed conflict or, in the context of a non-international armed conflict, to the territory where hostilities are taking place.

Offensive cyberwarfare operations undertaken by the French armed forces must comply with the following principles of international humanitarian law:

- **The principle of distinction between civilian assets and military targets**. Cyberattacks not directed at a specific military target or carried out by means of cyberweapons that cannot be directed at a specific military target are prohibited. Certain data, although intangible, may constitute civilian assets protected under international humanitarian law.
- **The principle of humanity**. The civilian population in general and individual civilians must not be targeted unless they participate directly in hostilities, and except during that participation. In an armed conflict, any cybercombatant who is a member of the armed forces, any member of an organized armed group engaged in cyberattacks against another party or any civilians directly participating in hostilities through electronic means may be the target of a conventional attack or a cyberattack.
- **The principle of proportionality**. Constant vigilance must be exercised in order to protect persons and civilian assets from the effects of hostilities during such operations. Collateral damage must be commensurate with the concrete and direct military advantage anticipated. The principle of proportionality in cyberspace requires that all foreseeable effects of the weapon be taken into consideration, whether those effects are direct (such as damage to the targeted system or interruption of service) or indirect (such as impact on the infrastructure controlled by the system under attack, as well as on persons affected by the malfunctioning or destruction of systems or the alteration and corruption of data), provided that those effects have a sufficient causal link with the attack. This principle also prohibits the use of cyberweapons that are uncontrollable (in time or in space) and could therefore cause irreversible damage to civilian infrastructure, systems or data.

The above principles are contained in the public elements of French military doctrine on offensive computer warfare, published in early 2019.

Human Rights

France supports the principles that the rights people enjoy offline must also be protected online and that international human rights law applies to cyberspace. Those values are especially challenged by the online spread of illegal materials, such as those promoting terrorism, hate and anti-Semitism. It is particularly important to involve private digital actors in the fight against illegal content and to clarify their role and responsibilities at the international level to combat illegal content and protect human rights and fundamental freedoms online.

The principle of due diligence

A shared understanding is essential at the international level regarding the obligations of States whose infrastructure is suspected of being used maliciously against the interests of another State. The aim is to clarify the application of the principle of due diligence, which provides that every State has an obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other States"[8], to the online domain. Accordingly, States should not knowingly allow their territory to be used for acts committed by electronic means proscribed by international law or allow such territory to be used by non-State intermediaries (proxies) to violate international law. A better understanding of how the principle applies to electronic challenges would strengthen cooperation among States with respect to protecting certain critical infrastructure and eliminating major cyberattacks transiting via a third country.

(b) Concept of reinforcing cooperation and trust among States

Norms of behaviour

The various rounds of negotiations conducted within the framework of the Group of Governmental Experts have led to tangible progress in the international regulation of cyberspace. In its 2015 report, 11 norms of responsible behaviour for States in cyberspace are outlined. France believes that each State must respect those norms and develop mechanisms for their implementation. Other norms, applicable to the behaviour of States or to other actors in cyberspace, could also be developed in the future.

Confidence-building measures

Efforts made in various forums and regional organizations to develop confidence-building measures on cybersecurity need to be strengthened. France will continue to encourage its partners to adopt interministerial procedures to ensure effective communication among States in times of crisis. The development of procedures and mechanisms based on transparency and communication are essential to conflict prevention in cyberspace.

Capacity-building

France supports the strengthening of international cybersecurity capacity, which directly enhances the security of all and the stability of cyberspace. France will play its full part in these efforts through capacity-building initiatives undertaken at the bilateral, regional and multilateral levels.

(c) Role and responsibility of non-State actors

Multi-stakeholder approach

In the Paris Call for Trust and Security in Cyberspace, France stressed "the necessity for a strengthened multi-stakeholder approach". France believes that civil society, academia, the private sector and the ICT community possess expertise and resources useful for developing aspects of relevant cybersecurity policies.

[8] Corfu Channel case, Judgment of April 9th, 1949, I.C.J. Reports 1949, p. 4.

Security responsibilities on the part of private actors in the design and maintenance of digital products

The spread of digital technology as a new tool and sphere of conflict gives the private sector, including a number of systemic actors, a critical role and unprecedented responsibility in safeguarding international peace and security. The Paris Call recognized "the responsibilities of key private sector actors to build confidence, security and stability in cyberspace" and encouraged "initiatives to enhance the security of digital processes, products and services".

In the view of France, a principle should be elaborated at the international level regarding the accountability of private systemic actors in the development, integration, use and maintenance of their digital products, processes and services throughout their life cycles and throughout the supply chain.

Responsibility of digital platforms in the fight against terrorism

France also promotes accountability on the part of private digital actors for combating the misuse of their services for terrorist purposes. France has raised this issue with the G7 and the European Union, actively supporting the adoption of a draft European regulation governing the activities of Internet providers with respect to combating terrorist content online. The draft stipulates that terrorist content must be removed immediately upon request by a member State, that active measures be adopted by platforms that could be exposed to terrorist content, that a 24-hour contact point be established to process reports and removal requests and that penalties be imposed for systematic non-cooperation.

Preventing offensive activities by private actors

France believes that States must retain their monopoly on the legitimate use of physical violence, both in cyberspace and elsewhere. It therefore supports the prohibition on non-State actors, including in the private sector, on conducting offensive activities in cyberspace on their own behalves or on behalf of other non-State actors. Such practices, based on the principle of legitimate self-defence ("hacking back"), have potentially destabilizing negative impacts on third parties and could fuel escalation among States. France therefore believes that the latitude of private actors to respond to incidents should be elucidated.

4. Possible measures by the international community to strengthen global cybersecurity

Faced with new threats stemming from the digital revolution, France believes that cooperation and law are necessary to prevent cyberspace becoming a permanent conflict zone. States are obliged to respect international law in the digital space as in other domains. Additionally, the normative framework on the responsible behaviour of States in cyberspace that has emerged in recent years should be consolidated. France believes that the following steps could strengthen global cybersecurity:

- **Building on the work done during previous meetings of the Group of Governmental Experts**. Without prejudice to the norms and recommendations agreed by consensus during previous rounds of negotiations, it might be useful to clarify the how to implement those norms and recommendations and how to develop a better understanding internationally of relevant good practices.
- **Building on the Paris Appeal during upcoming United Nations discussions on cybersecurity challenges**. The Appeal has so far brought together over one third of United Nations Member States and hundreds of prominent non-State

actors on a common vision of the principles that should underpin the online conduct of various actors.

- **Universalizing the Convention on Cybercrime**. Adopted in November 2001 to enhance international cooperation, the Convention has been ratified by 63 States to date, and has influenced the national legislation of more than two thirds of United Nations Member States.
- **Encouraging States to demonstrate transparency**, especially with respect to cybersecurity strategy, crisis management and cyberattack response doctrines and the interpretation of the application of international law to cyberspace.
- **Implementing, in the relevant regional or international frameworks, confidence-building measures specific to ICT issues**.
- **Strengthening initiatives and mechanisms for the exchange of good practices and capacity-building**. Such mechanisms should ensure that all States have an effective cybersecurity system, by, inter alia:
  - Developing a cybersecurity strategy;
  - Developing a legislative framework to promote cybersecurity and combat cybercrime;
  - Creating a computer emergency response team;
  - Establishing procedures for cooperation with the private sector, particularly major digital technology firms;
  - Developing a framework for protecting critical infrastructure in cyberspace.
- **Recognizing, at the international level, the accountability of private systemic actors for security**. That accountability extends to the design, integration, use and maintenance of their digital products, processes and services, throughout their life cycles and throughout the supply chain.

Greece

[Original: English]
[15 May 2019]

In December 2018, the General Assembly adopted a resolution on advancing responsible State behaviour in cyberspace in the context of international security. The resolution requests the Secretary-General to seek the views and assessments of Member States on: (a) the efforts taken at a national level to strengthen information security and promote international cooperation in this field; and (b) the content of the concepts mentioned in the reports of the Group of Governmental Experts.

Greece supports the consensus view of the Group of Governmental Experts that international law, and in particular the Charter of the United Nations, are applicable also in cyberspace and are essential for maintaining peace and stability and promoting an open, secure, peaceful and accessible information and communications technology (ICT) environment. Greece also supports the continuation of the process to discuss norms for responsible State behaviour, confidence-building measures and international law under the United Nations First Committee, and the establishment of a new Group of Governmental Experts.

We recognize that the interconnected and complex nature of cyberspace requires joint efforts by governments, the private sector, civil society, the technical community, users and academia to address the challenges faced and call on all

stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace.

We also recognize the role of the United Nations in further developing norms for responsible State behaviour in cyberspace and recall that the outcome of the Group of Governmental Experts discussions has articulated a consensual set of norms and recommendations, which the General Assembly has repeatedly endorsed, and which States should take as a basis for responsible State behaviour in cyberspace.

Through our participation in international organizations such as the United Nations, the European Union, the North Atlantic Treaty Organization and the Organization for Security and Cooperation in Europe, we seek to establish universal rules and principles of responsible State behaviour in the use of cyberspace, to cooperate, to exchange experiences and best practices, and to jointly develop appropriate means to address threats and challenges related to cybersecurity. Our country contributes to the fullest possible extent to the formulation and implementation of relevant decisions adopted within the framework of international organizations with the aim of increasing cooperation and transparency and reducing the risk of conflict.

Recognizing that cybercrime is a global problem, Greece has signed and ratified the Convention on Cybercrime of the Council of Europe, also known as the Treaty of Budapest. This treaty provides an important framework both for the adoption of our national legislation and for international cooperation in the fight against cybercrime. The treaty was ratified by Law 4411/2016. Also, in the framework of our participation in the Organization for Security and Cooperation in Europe, our country has also signed the Confidence-building Measures Agreement, aiming at Member States' cooperation on cybersecurity issues, transparency, stability and the reduction of the risk of confrontation in cyberspace.

Within the framework of European Union commitments, Greece has incorporated into its national legislation Directive 1148 on the security of network and information systems, also known as the NIS Directive, which includes measures for a high common level of security throughout the Union, implementing cybersecurity measures, developing a national strategy and enhancing cooperation between Member States. As a result, the protection of all critical infrastructures in our country is strengthened, while the principles of open society, constitutional freedoms and individual rights are safeguarded. The National Authority for Cybersecurity, which operates under the auspices of the Ministry of Digital Policy, bears overall responsibility for the implementation of the national cybersecurity strategy.

The key targets of our national cybersecurity strategy are:

- The development and consolidation of a secure and resilient cyberspace on the basis of national, European and international standards and practices
- The continuous improvement of our capabilities to safeguard against cyberattacks, with an emphasis on critical infrastructures
- The development of a strong public and private security culture, exploiting the potential of both the academic community and the public and private actors
- Upgrading the level of evaluation, analysis and prevention of threats, towards the security of information systems and infrastructures
- The establishment of an effective framework for coordination and cooperation between public and private stakeholders

- The active participation of the country in international initiatives and cybersecurity actions of international organizations
- Raising awareness among all social stakeholders and informing users about safe cyberspace usage
- The constant adaptation of the national institutional framework to the new technological requirements as well as to the European guidelines
- The promotion of innovation, research and development on security issues.

Japan

[Original: English]
[14 May 2019]

1. General appreciation of the issues of information security

Knowledge, technologies and services in cyberspace, such as artificial intelligence, the Internet of things, Fintech, big data and 5G, are becoming established in society and leading to innovations that are transforming the existing structures in our socioeconomic activities and the daily lives of people, and these transformations are bringing about progress in the unification of cyberspace and real space. In order to enjoy the benefits of the knowledge, technologies and services of cyberspace, it is essential to control the latent uncertainties always therein. When such control is not possible, the potential exists for cybersecurity-related threats to increase rapidly.

Benefits of cyberspace

The number of Internet users in the world is rising, as is the spread of the Internet itself. Furthermore, in terms of devices, the rate of personal smartphone ownership has increased significantly, and the Internet usage rate is also rising. The ratio of social media users is also rising, as a result of which an environment now exists for easily communicating in cyberspace. The increasing adoption of services in cyberspace by society has promoted not only the free flow of information, but also the formation of diverse communities and the sharing of information. There has been progress in the area of financial activities as well, including online shopping, stock trading and online banking, while new services in the areas of Fintech and the sharing economy are appearing regularly and leading innovation. There has also been progress in the use of information and communications technology in medicine and nursing, welfare, education and other areas related to social issues such as the declining working-age population and the ageing of local communities.

Increasing threats in cyberspace

While artificial intelligence, the Internet of things and other technologies and services have the potential to bring many benefits to people, there is always the latent risk that the providers of these technologies and services will lose the ability to control them, in which case they can cause immeasurable economic and social loss or damage. As the unification of cyberspace and real space proceeds, the likelihood of this increases exponentially. Furthermore, cyberspace is a place unrestricted by space or time where anyone, including malicious actors, can misuse and abuse new information and communication technologies with ease. The very nature of digital technology allows malicious actors to easily copy and distribute sensitive data and information, launch attack programmes and flexibly incorporate and make free use of emerging technologies such as artificial intelligence and blockchain. For that reason, the attackers have an asymmetrical advantage over the defenders, and that advantage is expected to increase particularly when the defender's formation depends on

existing policies and technological systems. Given these conditions, attacks directed at the Internet of things, Fintech including cryptocurrencies, critical infrastructure, and supply chains have occurred, causing direct financial losses and the interruption of businesses and services in addition to the usual data breach and serving to threaten the safety and security of the sustainable development of socioeconomic activities and the lives of people. There have also been massive incidents suspected to have been State-sponsored. There is also concern that the credibility of the information infrastructure may be shaken if cyberspace is controlled and managed by the government in some countries from a superior position. It is believed that as cyberspace continues to become further unified with real space, there will be increased concerns over potential attempts to target weaknesses in the Internet of things, supply chains and open innovation, and that unintended behaviour will occur in these systems. This could seriously impact not only governmental bodies and critical infrastructure operators, but also other businesses and even individuals.

Adherence to the basic position on cyberspace

In order to continue to deter malicious actors' activities and guarantee people's safety and rights, Japan retains, as its options, political, economic, technological, legal, diplomatic and all other viable and effective means. Japan adheres to the five principles for developing and implementing cybersecurity measures, which are: (i) assurance of the free flow of information; (ii) the rule of law; (iii) openness; (iv) autonomy; and (v) collaboration among multi-stakeholders.

(i) Assurance of the free flow of information

For the sustainable development of cyberspace as a place for creation and innovation, it is imperative to build and maintain a world in which transmitted information reaches the intended recipient without being unfairly censored or illegally modified en route. Privacy considerations must also be ensured. As a basic condition for the free flow of information in cyberspace, morality and common sense are requested not to offend rights and interests of others.

(ii) The rule of law

As the unification of cyberspace and real space progresses, the rule of law should also be maintained in cyberspace in the same way as in real space. Various domestic rules and norms, including domestic laws and regulations, are applied in cyberspace. Similarly, existing international law is also applied in cyberspace. The application of existing international law and the development of norms continue to be essential for the sustainable development of cyberspace as a safe and reliable space.

(iii) Openness

To achieve the sustainable development of cyberspace as a space to generate new values, cyberspace must be open to all actors without restricting the possibilities of linking diverse ideas and knowledge. Japan adheres to the position that cyberspace must not be exclusively dominated by a small group of actors therein.

(iv) Autonomy

Cyberspace has developed through the autonomous initiatives of multi-stakeholders. It is inappropriate and impossible for a State to take on the entire role of maintaining order for cyberspace to sustainably develop as a space where order and creativity coexist. The only approach to maintain order and deter and address the behaviour of malicious actors is for various social systems to function autonomously. Japan will promote this approach.

(v) Collaboration among multi-stakeholders

Cyberspace is a multidimensional world established through the activities of multi-stakeholders, including the State, local governments, critical infrastructure operators, cyberrelated and other businesses, education and research institutions, and individuals. For the sustainable development of cyberspace, all actors are required to consciously fulfil their respective roles and responsibilities. This will require coordination and collaboration in addition to individual efforts. States have the leading role in promoting this coordination and collaboration and will promote measures enabling the fulfilment of such roles.

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

Efforts taken at the national level to strengthen information security

In Japan, the legal foundation for the utilization of data has been prepared, including the Basic Act on the Advancement of Public and Private Sector Data Utilization and the Amended Act on the Protection of Personal Information, etc. The Government has also adopted a policy of realizing an anthropocentric society that achieves both economic development and the resolution of social issues through the high level of integration of cyberspace with real space. Under these circumstances, the massive amounts of data generated by sensors and devices in real space are currently being accumulated and analysed in cyberspace. Furthermore, the provision in real space of new products and services that add value through the use of data can be seen cyclically emerging and developing in numerous domains. No longer do cyberspace and real space exist as independent entities, but as mutually interacting entities, such that they cannot be considered separate anymore. Therefore, the two spaces should be seen as a single continuously evolving organic entity.

The unification of cyberspace and real space significantly increases the potential for affording abundance to society. At the same time, it also increases the opportunities for malicious actors to abuse cyberspace. The risk of economic and social loss or damage in real space is expected to expand and accelerate exponentially. Under these circumstances, the security of cyberspace, which serves as the foundation of economic society, must be ensured, and at the same time, its autonomously sustained evolution and development have to be ensured in order to achieve sustainable progress and wealth for society.

Recently, there has been a trend for certain nations to respond to cyberthreats by emphasizing management and control by the State from a dominant position. However, the strengthening of management and control of cyberspace by the State have the effect of hindering the possibility of autonomous and sustainable development. Thus, the cyberspace of today that developed through the autonomous initiatives of all stakeholders must be respected, and cybersecurity must be secured through collaborative and cooperative initiatives with those stakeholders. Based on this understanding, mindful of the state of affairs to be pursued for 2020 and beyond and taking into consideration the hosting of such international events as the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games (hereinafter referred to as “the Tokyo 2020 Games”), Japan will spare no efforts regarding cybersecurity measures by clarifying the basic vision of cybersecurity, identifying new issues that need to be tackled and swiftly implementing measures.

Efforts taken at the national level to promote international cooperation

Because the effects of incidents in cyberspace can easily extend beyond national borders, cyberincidents overseas can always affect Japan. Japan will cooperate and

collaborate with governments and the private sector worldwide to ensure the security of cyberspace and work towards both the peace and stability of the international community and the national security of Japan. To this end, the Government will proactively contribute to various international discussions and work for the sharing of information and the development of a common understanding regarding cyberrelated issues. The Government will also share expertise with foreign countries, promote specific cooperation and collaboration and take action.

With regard to sharing expertise and coordination policy, the Government will work through bilateral dialogues and international conferences on cybersecurity to exchange information on cybersecurity policies, strategies and systems to respond, and utilize that knowledge in planning Japan's cybersecurity policy. We will also strengthen our cooperation and collaboration regarding cybersecurity policy with strategic partners that share basic principles on cybersecurity with us.

Regarding international collaboration for incident response, the Government will share information on cyberattacks and threats and strengthen cooperation between Computer Emergency Response Teams to enable a coordinated response when incidents occur. The Government will also work to improve coordinated response capabilities through joint training and participation in international cyberdrills and joint training. Furthermore, the Government will respond appropriately in the case of incidents through appropriate international collaboration.

In the light of the diplomatic aspects of cyberrelated international cooperation, our commitments consist of three pillars: the rule of law, confidence-building measures and capacity-building in cyberspace.

- The promotion of the rule of law is important for international peace and stability and Japan's national security. Japan's position is that existing international law, including the Charter of the United Nations, applies to cyberspace also, and Japan will proactively contribute to discussions on the individual and specific applications of existing international law and the development and universalization of norms. With regard to measures against cybercrime, the National Police Agency and other relevant ministries and agencies will collaborate to further promote international partnerships through international investigative cooperation and information-sharing with international organizations, law enforcement agencies and security information agencies in foreign countries, leveraging frameworks such as the Convention on Cybercrime, mutual legal assistance treaties and the International Criminal Police Organization (ICPO).
- Japan will work to build confidence among States in order to prevent the occurrence of unforeseen circumstances and the deterioration of the situation caused by cyberattacks. Due to the anonymity and secrecy of cyberattacks, there are risks that cyberattacks could unintentionally increase tensions among States and worsen the situation. To prevent such accidental and unnecessary confrontations, it is important to build up international communication channels during peaceful times in preparation for the occurrence of incidents that extend beyond national borders. It is also necessary to increase transparency and build confidence between States through the proactive information exchange and policy dialogues in bilateral and multilateral consultations. The Government will also cooperate with other States to consider a mechanism for coordinating issues regarding cyberspace. In this context, Japan eagerly promotes confidence-building measures, including by initiating the establishment of and co-chairing the Association of Southeast Nations (ASEAN) regional forum intersessional meeting in the field of cybersecurity, while steadily implementing capacity-building assistance mainly in the Asia-Pacific region.

- With regard to capacity-building, as interdependence across borders has deepened, it is not possible for Japan to secure peace and stability alone. Global coordination to reduce and eliminate cybersecurity vulnerabilities is essential to ensuring Japan's national security. From this standpoint, assisting capacity-building in other States ensures the stability of the lives of Japanese residents and the activities of Japanese companies in other countries that depend on critical infrastructure in those States as well as the sound development of the use of cyberspace there. At the same time, it is also directly connected to ensuring the security of all cyberspace and contributes to the improvement of the security environment for the entire world, including Japan. Also, in the field of cybercrime, Japan is one of the few non-European parties to the Convention on Cybercrime and takes a positive role in promoting the Convention, which is an important legal framework for countering cybercrime, through capacity-building assistance in the Asian region.

3. Relevant international concepts aimed at strengthening the security of global information and telecommunications systems

Japan supports the consensus agreements of the previous Groups of Governmental Experts that existing international law applies in cyberspace. We have seen the discussion on the development of normative behaviour, the operationalization of confidence-building measures, and capacity-building as the key approaches to shaping responsible State behaviour in cyberspace. In particular, Japan recognizes that the implementation of non-binding and voluntary norms of responsible State behaviour in cyberspace, as referred to in the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, must be the foundation for ensuring international stability and predictability, and for future discussions on this issue. In this regard, we believe any attempts to conclude newly comprehensive treaties or similar instruments would not positively enhance cybersecurity at present.

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

Japan, as a responsible State, while promoting coordination with relevant regional frameworks by the international community based on existing international law, and all concepts identified through the Group of Governmental Experts, believes that developing a common understanding of the voluntary and non-binding norms of responsible State behaviour, and the implementation of these norms, will contribute to the strengthening of international security.

5. The content of the concepts mentioned in the reports of the Group of Governmental Experts

Japan believes that it is effective and meaningful for all States to take into consideration the following concepts identified by the Group of Governmental Experts:

Influence on the international community by malicious cyberacts

To flexibly incorporate the rapid development of information and communications technologies into our lives and to prevent the damage stemming from malicious cyberacts, we should acknowledge the importance of foreseeing existing and potential threats in cyberspace and how the international community could be affected by them.

Implementation of voluntary, non-binding norms of responsible State behaviour

To minimize the effects of malicious cyberacts and to deter those who would commit them, we should recall the significance of the consensus Group of Governmental Experts report, including the voluntary and non-binding norms of responsible State behaviour referenced therein. We should deepen our discussions, in collaboration with relevant regional organizations, to make practical and effective use of these worthwhile efforts.

Promoting the implementation of voluntary, non-binding norms of responsible State behaviour and the cooperation for relevant confidence-building measures and capacity-building

To further enhance each State's effort to develop and maintain a free, fair and secure cyberspace in the context of international security, we should reaffirm that all nations have a strong will to eliminate security holes in cyberspace and prevent cybercrime and other malicious acts. In this context, the group members should dedicate themselves consistently to encouraging all States to steadily implement the voluntary, non-binding norms of responsible State behaviour, including confidence-building measures and cooperation to help build national capability to implement the above-mentioned voluntary, non-binding norms and recommendations, including through the process of the next Group of Governmental Experts and open-ended working group.

Singapore

[Original: English]
[13 May 2019]

Singapore recognizes that threats to an open, secure and peaceful cyberspace are increasingly sophisticated, transboundary and asymmetric in nature. As a small and highly connected State that has been the subject of several cyberattacks, Singapore is strongly committed to the establishment of an international rules-based order in cyberspace. This will serve as a basis for trust and confidence between Member States and enable economic and social progress. To reap the full benefits of digital technologies, the international community must develop a secure, trusted and open cyberspace underpinned by international law applicable to cyberspace, well-defined norms of responsible State behaviour, robust confidence-building measures and coordinated capacity-building. Collectively, these three streams create a mutually reinforcing triangular loop that will allow for a safe and resilient cyberspace. It is important that the efforts to discuss such laws, rules and norms continue to take place at the United Nations, which is the only universal, inclusive and multilateral forum in which all States, whether large or small, have a voice. Singapore is committed to this process.

Singapore welcomes the establishment of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the decision to convene an open-ended working group. Singapore's view is that the work of the Group of Governmental Experts and the working group can and should be complementary. It is important for the major players to work together, in the spirit of consensus, mutual respect and mutual trust. Singapore is optimistic that both platforms can positively supplement each other and is committed to contributing constructively to both processes.

At the regional level, Singapore worked with fellow member States of the Association of Southeast Asian Nations (ASEAN) to issue the first ASEAN leaders' statement on cybersecurity cooperation, during the thirty-second ASEAN Summit, held in April 2018. In the statement, ASEAN leaders reaffirmed the need for a rules-based international order in cyberspace. They also tasked relevant ministers with identifying a suitable mechanism or platform for coordinating cybersecurity policy, diplomacy, cooperation and technical and capacity-building efforts across ASEAN, as well as a concrete list of voluntary, practical norms of State behaviour in cyberspace that ASEAN can work towards adopting. Acting on the leaders' statement, in September 2018, participants at the third ASEAN Ministerial Conference on Cybersecurity, held in Singapore, agreed to subscribe in principle to the 11 norms in the 2015 report of the Group of Governmental Experts (A/70/174), as well as to focus on regional capacity-building in implementing these norms.

Capacity-building is essential to ensuring that States develop the ability to successfully implement rules and norms of behaviour. Singapore has a S$10 million ASEAN Cyber Capacity Programme, a modular, multidisciplinary and multi-stakeholder programme that is focused on building capacity in ASEAN countries on cyberpolicy, strategy and technical issues. Since its inception in 2016, 160 ASEAN officials have been trained under the Programme. Singapore has also partnered with the Office for Disarmament Affairs to develop a flagship online training course to promote understanding and implement agreements reached by the Group of Governmental Experts. It will also work with the Office on a United Nations-Singapore cyberprogramme to build awareness of cybernorms and policy planning on cyberscenarios in ASEAN member States. As an extension of the ASEAN Cyber Capacity Programme, Singapore will launch the S$30 million ASEAN-Singapore Cybersecurity Centre of Excellence in 2019 to further build cybersecurity policymaking, strategy development and technical and operational capacity in ASEAN countries. The Centre will be open and inclusive, and ASEAN member States can leverage it to engage more closely with international partners.

At the national level, Singapore has made significant strides in strengthening the cybersecurity of its systems and networks on the following three fronts, namely building resilient infrastructure, creating a safer cyberspace and developing a vibrant cybersecurity ecosystem:

(a) *Building resilient infrastructure*. Transboundary cyberthreats are increasingly putting countries' critical infrastructure at risk. This is especially true for supranational information infrastructure, such as in the financial, maritime, telecommunications and aviation sectors, where the consequences of a successful cyberattack could spread beyond national borders to affect interconnected centres across the globe. A key development in 2018 was the passage and implementation of the Cybersecurity Act, which established a legal framework for the oversight and maintenance of national cybersecurity in Singapore. In the Act, proactive protection against cyberattacks on critical information infrastructure, which means computers or computer systems that support the provision of essential services, is emphasized. This protection is achieved by imposing legal obligations on the owners of such infrastructure to, among other things, do the following: (i) establish mechanisms to detect cybersecurity threats and incidents and report such incidents; (ii) conduct regular risk assessments and audits of critical information infrastructure; and (iii) participate in cybersecurity exercises conducted by the national cybersecurity authority. In addition to strengthening the protection of such infrastructure, the national cybersecurity authority is also authorized, under the Act, to prevent, respond to and investigate cybersecurity threats and incidents;

(b) *Creating a safer cyberspace*. In January 2019, Singapore attained the status of a certificate-authorizing nation under the common criteria recognition

arrangement, which is an international arrangement for the mutual recognition of common criteria certificates across 30 nations. The common criteria are a technical standard applied to the evaluation and certification of information technology security products and are widely adopted by both Governments and the industry. Singapore is now one of 18 out of 30 certificate-authorizing nations under the arrangement. As such, Singapore is allowed to certify information technology security products locally, thereby helping to improve the quality of cybersecurity products of small and medium-sized enterprises in Singapore by benchmarking them against international security standards;

(c) *Developing a vibrant cybersecurity ecosystem*. Singapore recognizes that strengthening cybersecurity involves building the cyberecosystem and encouraging innovation within the industry. To this end, Singapore launched its first integrated cybersecurity entrepreneur hub in March 2018, called the Innovation Cybersecurity Ecosystem at Block71, which is aimed at strengthening Singapore's growing cybersecurity ecosystem by attracting and developing competencies and deep technologies to help to mitigate the rapidly increasing cybersecurity risks. It also helps to develop cybersecurity start-ups around the world, through a range of programmes designed to support entrepreneurs, from idea creation to acceleration and scaling-up of cybersecurity start-ups for the global market.

Turkey

[Original: English]
[10 May 2019]

Information and communications technology (ICT) has become an essential part of society and the economy. It is used in a broad network that includes the public sector, the private sector, critical infrastructure and individuals, and has become widespread in our country and as well as in the world. As a result of this, ICT plays an important role for sustainable growth and development. However, the more we use technology, the more we become dependent on it and prone to the risks it brings forth. Individuals, companies, critical infrastructure and States encounter serious problems because of cyberthreats.

The diffusion of technology throughout all dimensions of our lives has led us to a new stage with respect to associated risks in the context of cybersecurity. Ensuring cybersecurity is not only a necessity for coping with threats in technology-intensive areas but also a prominent factor affecting nations' prosperity and national security because of the risks it poses to the course of social and economic life.

Security weaknesses in ICT may cause such systems to go out of service or be exploited, or may lead to eventual loss of life, large-scale economic loss, disturbance of public order or compromises to national security.

Turkey focuses on taking measures necessary to improve national cybersecurity and has been implementing the national cybersecurity strategy and action plan that covers the period from 2016 to 2019 with the mission of establishing national cybersecurity, designating and coordinating efficient and sustainable policies and realizing the practice of these policies. The Ministry of Transport and Infrastructure is the body responsible for making policies and developing strategies and action plans on national cybersecurity in Turkey. Within this context, the national cybersecurity strategy and action plan were created by involving all the relevant stakeholders in study groups, under the coordination of the Ministry of Transport and Infrastructure.

The strategy and action plan have two main objectives: first, for all stakeholders to acknowledge the understanding that cybersecurity is an integral part of national

security; and second, for the competency to be acquired that will allow administrative and technological precautions to be taken to maintain the absolute security of all systems and stakeholders in national cyberspace.

Each action in the strategy and action plan has been conducted by the Ministry of Transport and Infrastructure and related bodies, and all the progress for each action has been monitored by the Ministry.

Furthermore, the Information and Communication Technologies Authority has been the national Computer Emergency Response Team of Turkey since 2013. It is responsible for all regulatory functions regarding electronic communications and postal services in Turkey. In addition, it has been given the power to take measures necessary to fight against cyberattacks to ensure national cybersecurity. The Team acts as the coordination centre at the national level, in order to identify threats against the country's cybersecurity, take measures for reducing or eliminating the impact of likely cyberattacks and share information with defined actors. It provides coordination with all stakeholders, such as public or private institutions and individuals, for the detection and removal of cyberthreats. Its main focus areas in cybersecurity are:

- Cybercapacity-building
- Technological measures
- Gathering and diffusing threat intelligence
- Protection of critical infrastructure

In capacity-building, activities include human resources, training and preparations. Within the context of these activities, we organize "capture the flag" competitions on cybersecurity. We believe that human resources are one of the most important factors in cybersecurity. Within the context of the national Computer Emergency Response Team, we carry out key projects for capacity-building. In this respect, we organize cybersecurity training for institutional Computer Emergency Response Teams from various critical sectors, such as energy, health and public institutions. We also conduct hands-on training and competitions for students and graduates. In the past two years, over 2,500 trainees have attended our cybersecurity training programmes.

We have also established a cyberrange laboratory in order to improve our training programmes and provide more opportunities for hands-on activities. The laboratory is also beneficial for measuring the expertise level and provides a certification programme for attendees.

Our studies relating to technological measures involve early detection, alarms and warning activities. For this purpose, we have developed some detection and prevention systems. These systems play a huge role in increasing the level of national cybersecurity in the country by providing visibility and detecting the command and control centres of botnets and malicious software.

In the scope of Turkey's approach to enhancing cybersecurity, cyberthreat intelligence is another main focus area to be underlined. Within this context, we work in coordination with several parties, such as Internet actors, international organizations, judicial authorities, research centres and private companies. In addition, sectoral Computer Emergency Response Teams for critical infrastructure and more than 1,000 institutional Computer Emergency Response Teams have been established under public and private institutions.

Furthermore, since cyberspace is a borderless field, it is hard for a party to ensure its cybersecurity on its own. It is a multi-stakeholder and interdisciplinary

issue. We work with users, the private sector, non-governmental organizations, academia and international counterparts in order to fight against cyberthreats. For example, the Computer Emergency Response Team of Turkey receives cybernotifications from various national Computer Emergency Response Teams and informs the relevant parties to take necessary measures. It also sends information about cyberthreats and shares intelligence with other national Computer Emergency Response Teams and international organizations.

From a secure Internet perspective, the Safe Internet Centre was established within the Information and Communication Technologies Authority in 2017, in order to increase awareness regarding the proper and safe use of the Internet.

The Internet helpline and a safe web website, where families can find advice for the efficient use of the Internet, were launched. In addition, the "safer Internet truck", equipped with ICT tools, has become available for children and young people who have limited access to ICT. The truck provides a platform for people where they can experience technology closely and helps to raise awareness about safe and conscious use of the Internet for children who are more engaged with the Internet and technology.

The Authority organizes an event for Safer Internet Day annually. The main theme in 2018 was "Create, connect and share respect: a better Internet starts with you". The Authority and Bahçeşehir University launched a board game contest to encourage young people aged between 12 and 18 to design a game under the international theme. Many game designs were sent throughout the contest, and the contest winners received their awards. During this event, Facebook and Google conducted workshops for students on digital games and a safer Internet.

In addition, the Authority signed agreements with the Ministry of Family and Social Policies, the Access Providers Association and the Ministry of Education regarding awareness-raising activities and training for trainers on the conscious and safe use of ICT and the Internet. Training content was included in distance education modules and made available to all teachers working in the Ministry of Education system. With this distance education service, teachers and thousands of students have been trained so far.

Furthermore, in providing and maintaining cyberspace security, not only national coordination but also international cooperation, information exchange and confidence-building play a crucial role.

Relevant work and studies in Turkey on the scope of the confidence-building measures mentioned in the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174) and the concept of the responsible behaviour of States defined in the report are outlined below.

In line with the dissemination of ICT usage among individuals, personal information or data have become an attractive target for cyberattackers. In the context of the fundamental rights and freedoms of people, personal information and data protection have also become of major concern.

Along with transparency, accountability and ethical values in the cyberenvironment, all stakeholders in Turkey look out for the rule of law principle, fundamental human rights and freedoms and the protection of privacy, while working to ensure cyberspace security.

In this regard, Law No. 6698 on the protection of personal data was published in the Official Gazette, No. 29681, on 7 April 2016 and came into effect. The purpose of the law is to protect the fundamental rights and freedoms of people, particularly

the right to privacy, with respect to the processing of personal data, and to outline the obligations, principles and procedures that are binding upon natural or legal persons who process personal data.

Turkey has taken important roles in many organizations, either by being a founding member or by contributing to cooperation efforts on cybersecurity and information security issues. Hence Turkey seeks to ensure cybersecurity by exchanging information and ideas in a large range of areas with various countries and organizations, on policymaking, capacity-building and information-sharing.

Since cyberspace is a borderless field, international cooperation is a must for fighting against cyberthreats. Because of this, Turkey regularly follows and participates in international studies on cybersecurity within the United Nations, the North Atlantic Treaty Organization (NATO), the European Union, the Organization for Security and Cooperation in Europe (OSCE) and other international organizations and institutions.

In addition, ensuring cybersecurity is targeted by setting up bilateral agreements with various States. The Ministry of Transport and Infrastructure, the Information and Communication Technologies Authority and the Computer Emergency Response Team of Turkey have signed memorandums of understanding on cybersecurity with some States, such as Georgia, Russia, Kyrgyzstan, Serbia, Bosnia and Herzegovina, Croatia and Greece.

The memorandum of understanding that describes cooperation between NATO and its allies is approved by the NATO Cyber Defence Committee, which considers the views of our State, and is signed by NATO and the Ministry of Defence of the Republic of Turkey. Points of contact have been established, and related work under the scope of the memorandum of understanding is ongoing.

The work of the NATO Civil Emergency Planning Committee and the Industrial Resources and Communications Services Group is followed. Moreover, Turkey has been a member of the NATO-accredited knowledge hub, think tank and training facility, the Cooperative Cyber Defence Centre of Excellence, as a sponsoring nation, since 2015.

Turkey participates in and contributes to meetings of the Organization for Economic Cooperation and Development about security and privacy and the OSCE informal working group on cybersecurity.

Meetings of the Regional Arms Control Verification and Implementation Assistance Centre are followed, and cooperation on various issues has been developing. The strategic goal of the Centre is to enhance the development of national security strategies by encouraging regional security cooperation and effective interaction to sustainably counter emerging security challenges, such as cybersecurity and other forms of transnational threats, including terrorism, the proliferation of weapons of mass destruction, trafficking, organized crime, border security and management and climate change, while particular attention will be paid to all emerging security threats deriving therefrom.

Turkey is involved in efforts to develop international cooperation. The Computer Emergency Response Team of Turkey is a member of the Forum of Incident Response and Security Teams, the Trusted Introducer service, the International Multilateral Partnership Against Cyber Threats of the International Telecommunication Union (ITU), the NATO malware information sharing platform and the Cybersecurity Alliance for Mutual Progress and seeks to cooperate as much as possible to enhance cybersecurity information and share expertise and threat intelligence at the international level.

Cybersecurity exercises are another important activity for cooperation and preparedness. These kinds of exercises performed at the national and international levels contribute to the strengthening of cyberspace and the testing of measures to be taken against potential cyberthreats. In this context, national cybersecurity exercises were held in 2011, 2012, 2013 and 2017 in coordination with the Ministry of Transport and Infrastructure. With the participation of 19 countries, the international cybershield exercise was completed successfully in Istanbul, with the cooperation of ITU and its International Multilateral Partnership Against Cyber Threats, on 15 and 16 May 2014.

Turkey regularly participates in and contributes to international exercises on cybersecurity, namely the NATO Cyber Coalition, NATO Locked Shields and NATO Crisis Management Exercise.

Since cyberspace is without frontiers, the sources and targets of cyberattacks may be in different countries, including allied countries. A command and control centre can be in one country while its target is in another one. For this reason, information-sharing on cyberattacks and cybercriminals plays a crucial role in fighting against cyberthreats globally.

The Convention on Cybercrime, the only binding convention, drawn up by the Council of Europe, was opened for signature in Budapest in 2001 and entered into force in 2004. Turkey signed it in Strasbourg in 2010. The Convention covers various crimes, such as those committed via the Internet and other computer networks, computer-related fraud, child pornography and violations of network security, which are now incorporated into the national legislation of Turkey. In addition, the Turkish criminal code covers unauthorized access to information technology systems and unauthorized interference with or interception, modification or destruction of such systems. Persons who are convicted of those crimes are subject to a prison sentence of up to three years or fines. Afterwards, it was approved via the Law on the Approval of Ratification of the Convention on Cybercrime, and the work on adaptation into domestic legislation was finalized by 2016.