United Nations A/75/123

General Assembly

Distr.: General
23 June 2020
English
Original: Arabic/English/French/
Spanish

Seventy-fifth session
Item 98 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/75/50.

20-08285 (E) 170720 220720

I. Introduction

1. On 12 December 2019, the General Assembly adopted resolution 74/28 entitled advancing responsible State behaviour in cyberspace in the context of international security under agenda item 93 on developments in the field of information and telecommunications in the context of international security.

2. In paragraph 2 of resolution 74/28, 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) 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.

3. Pursuant to that request, on 27 January 2020, a note verbale was sent to all Member States inviting them to provide information on the subject. As a result of the ongoing coronavirus disease (COVID-19) crisis, in order to facilitate the submission of the views on the issues outlined above by Member States, the original deadline for submission of 15 May 2020 was extended to 31 May 2020.

4. The replies received at the time of reporting are contained in sections II and III. Additional replies received after 31 May 2020 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

Armenia

[Original: English]
[13 May 2020]

Armenia attaches great importance to open, free, stable and secure cyberspace based on full compliance with the principles and norms of international law and the Charter of the United Nations, in their entirety. Taking into account the global nature of cyberspace, it is important to protect human rights and freedoms online, particularly the freedom of opinion and expression, which includes the right to seek, receive and impart information. Meanwhile, the challenges stemming from the use of information and communications technologies (ICTs) and the cyberenvironment are wide and diverse. Therefore, the international community should stand united in its response to prevent the misuse of ICTs and contribute to their peaceful and cooperative use. Having this in mind, Armenia is actively engaged in international cooperative platforms to enhance transparency, predictability and stability in cyberspace and reduce the risks of threats stemming from the use of ICTs.

Armenia is fully committed to the thorough implementation of the Council of Europe Convention on Cybercrime and its Additional Protocol on the criminalization of acts of a racist and xenophobic nature committed through computer systems. Since 2019, Armenia has been actively involved in the implementation of the European Union and Council of Europe joint CyberEast project aimed at increasing capacities on cyberresilience, criminal justice and electronic evidence. Similarly, Armenia is implementing the Organization for Security and Cooperation in Europe (OSCE)

confidence-building measures (Permanent Council decision 1202) in good faith to reduce the threats stemming from the use of ICTs. In July 2019, Armenia hosted a team of experts from the OSCE Transnational Threats Division to conduct an assessment of its national capacities in the investigation and prosecution of cybercrimes. In November 2019, the OSCE Transnational Threats Division organized a joint round table in Yerevan to discuss the findings of the above-mentioned assessment with Armenian stakeholders. Based on the assessment report of the experts and the conclusions of the round table meeting, the OSCE Transnational Threats Division has prepared a concept note dedicated to the topic, which may develop into a project in the future.

The contents and findings of the Group of Governmental Experts reports from 2013 and 2015 express the positions of a limited number of States Members of the United Nations involved in the process of development of the reports of the Groups of Governmental Experts, which, therefore, did not contribute to producing a universal and comprehensive set of norms acceptable for all Member States. In this vein, we believe that the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, as an inclusive and transparent platform for discussions between Member States, can elaborate a comprehensive consolidated list of rules, norms and principles of responsible State behaviour in the use of ICTs acceptable for all Member States.

Australia

[Original: English]
[29 May 2020]

Australia welcomes the opportunity, in response to the invitation in General Assembly resolution 74/28, to provide its views on advancing responsible State behaviour in cyberspace in the context of international security. This submission builds upon information provided by Australia in response to resolution 70/237 in 2016, to resolution 68/243 in 2014 and to resolution 65/41 in 2011 on developments in the field of information and telecommunications in the context of international security.

Cumulatively, the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security from 2010 (A/65/201), 2013 (A/68/98) and 2015 (A/70/174) affirm that existing international law – and in particular, the Charter of the United Nations in its entirety – is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment. The reports also articulate voluntary non-binding norms of responsible State behaviour, while recognizing the need for confidence-building measures, and coordinated capacity-building. Combined, these measures (international law, norms, confidence-building measures and capacity-building) provide the basis for a secure, stable and prosperous cyberspace, and are often referred to as a framework for responsible State behaviour.

Australia reaffirms its commitment to act in accordance with the cumulative Group of Governmental Experts reports from 2010, 2013 and 2015 (A/65/201; A/68/98; A/70/174). Australia is actively participating in the sixth Group of Governmental Experts and the inaugural Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (established pursuant to resolution 73/266 and resolution 73/27, respectively).

International law

Australia's position on how international law governs State conduct in cyberspace is presented in the International Cyber Engagement Strategy (2017), as supplemented by the 2019 International Law Supplement (both available on the website of the Department of Foreign Affairs and Trade: www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf).

In February 2020, Australia published a non-paper entitled "Case studies on the application of international law in cyberspace" (available on the websites of the Open-ended Working Group: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-studies-final-5-february-2020.pdf; and the Department of Foreign Affairs and Trade: www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf).

Implementation

Recalling that, in 2015, the General Assembly called on all Member States "to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts" (see resolution 70/237), Australia has published an overview of how Australia observes and implements the four key pillars of the 2015 Group of Governmental Experts report: international law, norms of responsible State behaviour, confidence-building measures and capacity-building (available on the websites of the Open-ended Working Group: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf; and Australia's Department of Foreign Affairs and Trade: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace).

The 2015 Group of Governmental Experts report articulated best practice activities, which many countries were or are already implementing. Australia encourages all countries to conduct a stocktaking of ongoing activities that align with the 2015 Group of Governmental Experts report (application of international law, implementation of norms of responsible State behaviour, confidence-building measures and capacity-building), as well as to identify gaps and (if applicable) capacity required to fill those gaps. With Mexico and 24 other countries, Australia was pleased to submit a proposal to the Open-ended Working Group (established pursuant to resolution 73/27) to establish a survey of national implementation of General Assembly resolution 70/237 (available on the websites of the Open-ended Working Group: https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf and the Department of Foreign Affairs and Trade: www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf).

Gender

As recognized by the women and peace and security agenda, women are differently and uniquely affected by conflict and threats to international peace and security. Australia commends the recent report of the United Nations Institute for Disarmament Research on gender balance in arms control, non-proliferation and disarmament diplomacy entitled "Still behind the curve", which notes that the First Committee has the lowest proportion of female diplomats of any of the Main Committees of the General Assembly. The Women in International Security and Cyberspace Fellowship is a joint initiative of the Governments of Australia, the United Kingdom, Canada, the Netherlands and New Zealand. It promotes greater participation by women in discussions at the United Nations on international security

issues related to responsible State behaviour in cyberspace. Australia will continue to take tangible steps to support the active and effective participation of women in multilateral discussions related to international security and disarmament.

Bosnia and Herzegovina

[Original: English]
[11 May 2020]

Information on efforts taken at the national level in Bosnia and Herzegovina to strengthen information security and promote international cooperation in this field

This report is made based on the data collected from the following institutions in Bosnia and Herzegovina: Ministry of Security of Bosnia and Herzegovina, Ministry of Defence of Bosnia and Herzegovina, Ministry of Transport and Communications of Bosnia and Herzegovina, Federal Police Administration, Ministry of Interior of Republika Srpska and Ministry for Scientific and Technological Development, Higher Education and Information Society of Republika Srpska. The relevant institutions that had not delivered the data to the Ministry of Security of Bosnia and Herzegovina before the report was sent are: the Brčko District Police and the Federal Ministry of Transport and Communications.

Bosnia and Herzegovina has signed international agreements and conventions relevant to information and cybersecurity. The most prominent ones are the Convention on Cybercrime and the Stabilisation and Association Agreement. The Convention was opened for signature on 23 November 2001 in Budapest, while the Presidency of Bosnia and Herzegovina reached the decision on ratifying the document at its eighty-ninth session, held on 25 March 2006. Thereby, Bosnia and Herzegovina was obliged to adopt legislation and other necessary measures for combating cybercrime in order to harmonize them with other signatories of the Convention in terms of felony treatment, data acquisition, processing and storage.

The following legislation is relevant in Bosnia and Herzegovina when it comes to the topics covered by the Convention:

- Criminal Code of Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, 3/03
- Criminal Procedure Code, Official Gazette of Bosnia and Herzegovina, 3/03, 32/03, 36/03, 26/04,63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09 and 72/13
- Criminal Code of the Federation of Bosnia and Herzegovina, Official Gazette of the Federation of Bosnia and Herzegovina, 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 and 75/17
- Criminal Procedure Code of the Federation of Bosnia and Herzegovina, Official Gazette of the Federation of Bosnia and Herzegovina, 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 and 59/14
- Criminal Code of Republika Srpska, Official Gazette of Republika Srpska, 64/17 and 104/18
- Criminal Procedure Code of Republika Srpska, Official Gazette of Republika Srpska, 53/12, 91/17 and 66/18
- Criminal Code of Brčko District, Official Gazette of Brčko District, 33/13, 26/16, 13/17 and 50/18

• Criminal Procedure Code of Brčko District, Official Gazette of Brčko District, 33/13, 27/14 and 3/19

State level

The Ministry of Security of Bosnia and Herzegovina, motivated by the above-mentioned and aware of the risks that can occur in cyberspace, has conducted the following activities.

Upon the proposal of the Ministry of Security of Bosnia and Herzegovina, the Council of Ministers of Bosnia and Herzegovina at its ninety-third session held, on 8 March 2017, adopted the Decision on the establishment of the Computer Emergency Response Team for the institutions of Bosnia and Herzegovina, which was published in the Official Gazette of Bosnia and Herzegovina, 25/17, thereby establishing the Computer Emergency Response Team and placing it in the Ministry of Security of Bosnia and Herzegovina, Department for Information Technology and Telecommunication Systems.

According to article 4 of the above-mentioned Decision, the Ministry of Security of Bosnia and Herzegovina needs to adapt its internal organization and systematization of working positions in order to establish the proper functioning of the Computer Emergency Response Team. All necessary opinions in line with the procedure when changing the internal organization and systematization of an institution were received in late 2017 and they are all positive, together with all documents which have been prepared.

The Ministry of Security of Bosnia and Herzegovina has made the required changes and amendments to its internal organization and systematization of working positions in order to establish the proper functioning of the Computer Emergency Response Team and delivered them to the Council of Ministers of Bosnia and Herzegovina for adoption. Currently, one is waiting for the Council of Ministers of Bosnia and Herzegovina to give its consent to the proposed rule book. After consent is received, the Ministry of Security of Bosnia and Herzegovina will start the technical and operational establishment of the Computer Emergency Response Team for the institutions of Bosnia and Herzegovina. The proposed change in internal organization includes an additional five positions to the new division in the Department for Information Technology and Telecommunication Systems.

The Ministry of Security of Bosnia and Herzegovina plans to strengthen the Computer Emergency Response Team operationally, institutionally and technically, aiming at the accomplishment of the strategic goals of that body (coordination and cooperation with the relevant bodies in Bosnia and Herzegovina, the elimination and decrease of consequences of security incidents caused by unauthorized access to information and communications technology (ICT) systems in the institutions of Bosnia and Herzegovina, the increase of reliability of ICT systems in the institutions of Bosnia and Herzegovina through constant dedication, work on the prevention and minimization of possibilities of occurrence of security incidents, assisting administrators in the implementation of security incidents, etc.), realizing activities in accordance with article 6 of the Decision and the establishment of a Computer Emergency Response Team network in Bosnia and Herzegovina.

Furthermore, upon the proposal of the Ministry of Security of Bosnia and Herzegovina, the Council of Ministers of Bosnia and Herzegovina, at its 107th session, held on 6 July 2017, adopted the analysis on the harmonization of legislation in the domain of cybersecurity in Bosnia and Herzegovina and obliged the Ministry of Security of Bosnia and Herzegovina to intensify activities on the drafting the strategy on cybersecurity in Bosnia and Herzegovina.

Accordingly, there are ongoing activities on the harmonization of views among entities and bodies concerning the model of the strategic document that would be synchronized with the European Union Network Information Security Directive and, on the other hand, fulfil the constitutional organization of Bosnia and Herzegovina.

Under the auspices of the Organization for Security and Cooperation in Europe (OSCE), an informal working group was formed. This group consists of representatives of competent/interested institutions in Bosnia and Herzegovina and it has drafted the "Guidelines for a strategic cybersecurity framework in Bosnia and Herzegovina".

Also, the Ministry of Security of Bosnia and Herzegovina participates in ongoing activities for the drafting of the new strategy for preventing and combating terrorism in Bosnia and Herzegovina, which should cover the use of the digital environment to conduct these activities.

The Ministry of Security of Bosnia and Herzegovina actively participates in the work of the Council of Europe Cybercrime Convention Committee.

Upon the proposal of the Ministry of Security of Bosnia and Herzegovina, the Council of Ministers of Bosnia and Herzegovina, at its eightieth session, held on 10 November 2016, adopted the Decision on the establishment of the interministerial working group for the implementation of the project for capacity-building in the area of cybercrime (iPROCEEDS) (published in the Official Gazette of Bosnia and Herzegovina, 14/17).

The European Union and the Council of Europe, in January 2016, signed an agreement on a regional project with the aim of capacity-building in the area of combating cybercrime for the South-Eastern European countries, iPROCEEDS, with an emphasis on the confiscation of proceeds from online crime or cybercrime. The project duration was 42 months. The project was financed by the European Union and the Council of Europe, while the implementation is carried out by the Council of Europe Office for Cybercrime in Bucharest. It has been proposed that the project team representing Bosnia and Herzegovina be composed of representatives of the Ministry of Justice that are competent for the given crime: prosecutor's office, police, financial intelligence department, etc. In accordance with the above-mentioned, the given working group has been formed.

Furthermore, the Ministry of Security of Bosnia and Herzegovina coordinates the project team members for iPROCEEDS-2 on targeting crime proceeds on the Internet and securing electronic evidence in South-Eastern Europe and Turkey, which started in January 2020. This project will build on the results achieved during the implementation of the iPROCEEDS project and concentrate on targeted support under the following project areas: (a) legislation regarding securing electronic evidence and access to data in full respect of fundamental rights and freedoms, including privacy and personal data protection; (b) alignment with European Union and Council of Europe personal data protection standards; (c) promotion of cybercrime and cybersecurity policies and strategies; (d) inter-agency and public-private cooperation for the investigation of cybercrime and proceeds from crime online; (e) public reporting systems on online fraud and other cybercrime offences; (f) judicial training on cybercrime and electronic evidence and related financial investigations and anti-money-laundering measures; and (g) international cooperation and information-sharing for the investigation of cybercrime and proceeds from crime online. The project duration is 42 months.

The Ministry of Security of Bosnia and Herzegovina successfully conducts the role of point of contact for the implementation of OSCE confidence-building measures. Some of the activities that have been accomplished in this period are the

successful reporting and delivery of information on the state of cybersecurity in Bosnia and Herzegovina, participation in the work of the interministerial working group assembled based on Permanent Council decision 1039, participating in seven communications checks and hosting a subregional training on cybersecurity and ICT security in May 2019, among others. Also, we have supported OSCE by providing our capacities and knowledge in the organization of several local conferences and workshops.

Also, Bosnia and Herzegovina has been included in the regional project, "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe". The project was financed by the Governments of Germany and the United States of America and it is realized by the OSCE Transnational Threats Department in cooperation with representatives of the countries from the region (Albania, Bosnia and Herzegovina, Montenegro, Kosovo,[1] Serbia and North Macedonia) and OSCE field missions. The main aim of the project is the education and training of experts working on cyber and cyberrelated organized crime cases. The project was ongoing in the period 2017–2019, and it contributed to the development of a comprehensive general strategic framework for solving questions of cybercrime and threats to cybersecurity, as well as strengthening the existing capacities for fighting against cybercrime as well as for responding to cybersecurity threats. The Ministry of Security of Bosnia and Herzegovina had a coordination role for Bosnia and Herzegovina in this project.

The Ministry of Defence of Bosnia and Herzegovina is conducting activities in order to have an efficient and sustainable cybersecurity system in its jurisdiction by 2023. So far, the Ministry adopted the Strategy for Cyber Security for the defence sector on 4 October 2017. A detailed implementation plan for this strategy was adopted on 27 December 2017. Security goals focus on the prevention of security incidents, the response to security incidents, the education and certification of staff working in the area of cybersecurity in the defence sector of Bosnia and Herzegovina and an increase in the awareness of end users in terms of the security of communication and information systems. Aiming at implementation of the above-mentioned points, the Ministry of Defence of Bosnia and Herzegovina has already drafted or adopted certain implementation documents.

Also, the Ministry of Defence of Bosnia and Herzegovina has started the process of establishing a computer emergency response team for the Ministry of Defence of Bosnia and Herzegovina.

The Ministry of Defence of Bosnia and Herzegovina has the obligation, within the North Atlantic Treaty Organization Partnership for Peace, to implement partner goal G7300 on cyberdefence, which requires: (a) the adoption of policies, procedures and other documents in order to have visible cyberdefence integration into the operations and processes of operational planning and to have international regulations in cyberspace, security measures for risk exchange and estimation of cyberthreats between national and international bodies in the field of cybersecurity implemented; (b) an established Computer Emergency Response Team; (c) the establishment of capabilities for ensuring the confidentiality, availability and authenticity of information and information systems of the Ministry of Defence of Bosnia and Herzegovina and the Armed Forces of Bosnia and Herzegovina; (d) the adoption of programmes for the education and training of experts in the field and end users, as well; (e) the adoption of education programmes through the organization of national cyberexercises and seminars, as well as the participation of representatives of staff of

[1] This designation is without prejudice to position on status.

the Ministry of Defence of Bosnia and Herzegovina and the Armed Forces of Bosnia and Herzegovina in international cyberexercises and seminars.

Upon the proposal of the Ministry of Transport and Communications of Bosnia and Herzegovina, and in cooperation with the Ministry of Security of Bosnia and Herzegovina, the Council of Ministers of Bosnia and Herzegovina, at its ninety-fifth session, held on 22 March 2017, adopted the policy on information security management for the institutions of Bosnia and Herzegovina, 2017–2022.

The Ministry of Transport and Communications of Bosnia and Herzegovina is currently working on the drafting and harmonization of a law on information security and the security of network and information systems in line with European Union Directive 2016/1148 on the security of network and information systems, together with the Ministry of Security of Bosnia and Herzegovina. The Ministry has also worked on a report on the maturity of capabilities for the estimation of cybersecurity capacities in Bosnia and Herzegovina, together with the Global Cyber Security Capacity Centre of Oxford University, the World Bank and the Global Centre for Cyber Security Development, among others.

Regarding future activities, the Ministry of Transport and Communications of Bosnia and Herzegovina plans to propose a law on electronic identification in confidence services for electronic transactions and to draft a strategy for the development of an information society in Bosnia and Herzegovina.

Entity level

Federation of Bosnia and Herzegovina

The Federal Police Administration has recognized the importance of cybersecurity and, consequently, established a cybercrime unit in 2015. This unit and the Centre for Forensic Analysis are covered by adequate staff, knowledge and equipment. The cybercrime unit has 10 experts, while the Centre for Forensic Analysis is a member of the European Network of Forensic Science Institutes. Also, this institution actively participates in the implementation of the project on preventing sexual exploitation and abuse of children in the digital environment in Bosnia and Herzegovina, together with the United Nations Children's Fund, Emmaus International and Save the Children. Furthermore, this institution played an important part in the realization of above-mentioned projects, such as iPROCEEDS and "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime in South-Eastern Europe", but it also plays a crucial role in the implementation of the new iPROCEEDS-2 project.

The Federation of Bosnia and Herzegovina adopted the Decision on the establishment of the Working Group for Computer Emergency Response for the Institutions of the Federation of Bosnia and Herzegovina in 2018, with the same goals and objectives to implement as in the two bodies previously described.

Republika Srpska

The Ministry of Interior of Republika Srpska has reported that a number of activities have been conducted in order to harmonize the legislation within this entity with European Union legislation. Therefore, it has adopted development directions for the period 2017–2021 and an action plan for the implementation of those directions for the period 2017–2019. Also, it has adopted a programme on information and communications technology development for the period 2017–2021, which contains a goal focused on the improvement and integration of the information-communications system. In line with this, the law on police and home affairs of Republika Srpska has been updated, thereby creating the mechanisms to implement European Union Regulation 910/2014 on electronic identification and trust services

for electronic transactions in the internal market and Directive 2016/1148 on the security of network and information systems.

Upon the proposal of the Ministry of Interior of Republika Srpska, the Law on Security of Critical Infrastructure (Official Gazette of Republika Srpska, 58/19) was adopted and thereby created the basis for the implementation of Directive 2008/114/EC and the European Union Network Information Security Directive. In this way, legislative capacities have been created, as has the definition of the critical infrastructure in this entity for the purpose of reacting to any incidents, including cyberrelated incidents.

Also, this institution participated in the following projects: the 2015 Instrument for Pre-accession Assistance project, “Enhance the quality and safety of information exchange among law enforcement agencies in Bosnia and Herzegovina”, “Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-enabled Crime”, iPROCEEDS and iPROCEEDS-2. This Ministry also prepares the infrastructure for safe data exchange with other institutions and legal subjects, and provides services based on security mechanisms defined in the European Union Directive Regulation on electronic identification and trust services for electronic transactions in the internal market. Also, documents related to the realization of current mechanisms in information security are being drafted.

The Ministry of Interior of Republika Srpska also has a dedicated unit for high-tech crime and, as do all other law enforcement agencies in Bosnia and Herzegovina, it works with the International Criminal Police Organization, the European Union Agency for Law Enforcement Cooperation, the European Union Agency for Criminal Justice Cooperation, the United Nations Office on Drugs and Crime, OSCE, the European Union Agency for Law Enforcement Training, the United States Embassy, International Criminal Investigative Training Assistance Program, the International Police Association , the United Nations Children’s Fund and many other embassies and international organizations. The areas of cooperation include education, training, knowledge and data exchange, among others.

When it comes to additional bodies for ensuring cybersecurity in Bosnia and Herzegovina, the entity Republika Srpska adopted, in 2011, the Law on Information Security (Official Gazette of Republika Srpska, 70/11), which defines the basic information security rules. In accordance with the Law, the department for information security, namely the Computer Emergency Response Team, in Republika Srpska has been established in the former Agency for Information Society of Republika Srpska (which is now the Ministry for Scientific and Technological Development, Higher Education and Information Society). This body has the task of coordinating prevention, protecting against computer security incidents and protecting the cyberinfrastructure of public bodies and legal and physical persons. In the past two years, this body has established the Security Operations Centre for the government of Republika Srpska with the aim of protecting the relevant infrastructure from the information security point of view. Training for the operators has also been conducted and three-shift work has started. This body works intensively on becoming accredited by or a member of relevant international organizations.

Canada

[Original: English, French]
[7 May 2020]

On cybersecurity, Canada:

- Is committed to promoting international stability, as well as a free, open and secure cyberspace

- Believes that international law applies to the use of information and communications technology by States and reinforces stability in cyberspace
- Encourages States to respect agreed norms of State behaviour in cyberspace, including the norms outlined 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, which was endorsed by the General Assembly
- Believes that practical confidence-building measure are a proven method to strengthen stability in cyberspace

At the national level, Canada is active in a number of ways:

- In June 2018, the Government, led by Public Safety Canada, released Canada's National Cyber Security Strategy. The Strategy aims to strengthen partnerships to secure vital cybersystems, both inside and outside the federal Government, and protect Canadians and Canadian businesses as they connect online. It also seeks to enhance the detection of, and ability to respond to, continually evolving cyberthreats. The Strategy is organized according to three high-level goals: (a) secure and resilient Canadian systems; (b) an innovative and adaptive cyberecosystem; and (c) leadership, governance and collaboration. Canada is implementing the Strategy's goals through the 2019 National Cyber Security Action Plan, which sets out specific initiatives over five years.
- In implementing the National Cyber Security Strategy, Canada created the Canadian Centre for Cyber Security, which consolidated the Government's cybersecurity operational units into one public-facing organization. As Canada's National Computer Emergency Response Team, the Cyber Centre is a unified source of expert advice, guidance, services and support for government, critical infrastructure owners and operators, the private sector and the Canadian public.
- The 2018 National Cyber Security Strategy also included funding for the new National Cybercrime Coordination Unit. While managed by the Royal Canadian Mounted Police, the Unit will serve all Canadian police agencies and will work with public and private sector partners. The Unit, to be fully operational by 2023, coordinates and deconflicts cybercrime investigations, targeting multiple jurisdictions in Canada and internationally.
- The Royal Canadian Mounted Police also received additional funding in 2018 to augment investigative intelligence operational capacity and strengthen specialized technical expertise to support action against both domestic and international cybercrime activities.

At the international level, Canada is active in a number of ways:

- Canada is engaging with the international community, like-minded States and allies in multiple international forums to strengthen the international cybersecurity environment. For example, Canada continues to promote the development of international law and respect for agreed norms of State behaviour in cyberspace, including the General Assembly-endorsed norms outlined in the 2015 Group of Governmental Experts report. Canada is also engaging actively at the ongoing Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and providing its views on ongoing Group of Governmental Experts discussions, as appropriate. Canada hopes that the Open-ended Working Group will promote the implementation of agreed norms and address the gender aspects of cybersecurity, among other issues.

- In United Nations multilateral forums, Canada has been working to advance norms and standards, and has been urging States to respect their human rights obligations. This includes addressing information and communications technology-facilitated violence against women and girls and ensuring their safety and personal integrity in both offline and online contexts. Canada has sought to advance these objectives in various ways, including by leading a resolution at the Human Rights Council on eliminating violence against women and girls in digital contexts.

- Guided by its 2017 defence policy, *Strong, Secure, Engaged*, Canada is working to deter and respond to malicious cyberactivity, including by leveraging its cybercapabilities in support of military operations. The Canadian Armed Forces active cybercapability is subject to the same rigour as other military capabilities, including applicable domestic and international laws and obligations and rules of engagement.

- At the June 2018 Charlevoix Summit, Group of Seven leaders announced the creation of the Rapid Response Mechanism. The Mechanism is mandated to coordinate Group of Seven efforts to identify and respond to diverse and evolving threats to our democracies, including disinformation, through information-sharing and analysis, and identifying opportunities for coordinated responses. The Mechanism is meant to address a broad spectrum of threats to democracy, for the benefit of Group of Seven members and the broader international community.

Some other ongoing international efforts include:

- Since 2015, Canada has committed over $4 million to support cybersecurity capacity-building projects. Canada has also funded the participation of female diplomats from the Americas in the Open-ended Working Group, as part of the Women in Cyber fellowship programme, which aims to promote the meaningful participation of women in United Nations cybernegotiations.

- Canada supports North Atlantic Treaty Organization efforts to strengthen the cyberdefence of the alliance and of individual allies.

- Canada has been working on implementing confidence-building measures in various forums, including the Organization for Security and Cooperation in Europe, the Organization of American States and the Regional Forum of the Association of Southeast Asian Nations.

- Canada is an active member of the Freedom Online Coalition, an international multilateral organization that promotes human rights online, where it chairs a multi-stakeholder task force on artificial intelligence and human rights.

Canada remains committed to advancing global efforts to ensure security and stability in cyberspace, for the benefit of all.

Colombia

[Original: Spanish]
[29 May 2020]

In accordance with General Assembly resolution 74/28, entitled “Advancing responsible State behaviour in cyberspace in the context of international security”, Colombia, 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, is

pleased to inform the Secretary-General of its views and assessments on the following questions:

- Efforts taken at the national level to strengthen information security and promote international cooperation.
- The content of the concepts mentioned in the reports of the Group of Governmental Experts.

Introduction

Colombia is generally in favour of a free, open and secure digital environment in which net neutrality is ensured, and thus believes that it is important to continue to give priority to capacity-building and cooperation based on international law and existing norms and agreements, as well as to the implementation of confidence-building measures in cyberspace.

Colombia has made significant efforts in the field of cybernetics by strengthening inter-agency coordination at the highest level in order to ensure a more secure cyberspace.

Pursuant to the public policy on digital security adopted in 2016, the national Government established the Digital Security Committee, in which relevant entities participate, and which coordinates efforts to address potential national cybersecurity crises. The Committee is led by a national coordinator, who is currently the Presidential Adviser for Economic Affairs and Digital Transformation. The Ministry of Information and Communications Technology serves as its technical secretariat.

These bodies coordinate efforts to examine and update policies and laws related to digital security, review the international agenda and ensure national defence and security in the digital environment, in order to guide activities aimed at mitigating and countering cyberattacks, protecting the country's critical infrastructure and strengthening human, technical, technological and physical capacities, as indicated below:

- **Computer Emergency Response Group of Colombia**. A body within the Ministry of Defence whose purpose is to coordinate the activities necessary to protect critical State infrastructure against cybersecurity emergencies which threaten or undermine national security and defence. It is responsible for responding to computer security incidents.
- **Joint Cyber Command of the national military forces.** A supervisory body responsible for directing, planning, coordinating, integrating, implementing and synchronizing joint cyberoperations. It is tasked with implementing cyberdefence measures and with conducting military cyberoperations at the strategic level in order to ensure national security and defence in cyberspace, including coordination concerning critical infrastructure.
- **Cybersecurity Capacities Centre of Colombia of the Cyber Police Centre**. A division within the Directorate for Criminal Investigation and the International Criminal Police Organization of the National Police which is responsible for developing criminal investigation strategies, programmes and projects to ensure digital security, cybersecurity and the protection of the national population's information and data circulating in cyberspace.
- **Computer security incident response team**. Colombia has governmental, financial, sectoral and private response teams. At the regional level, within the framework of the Organization of American States (OAS), Colombia is a member of the hemispheric network of computer security incident response

teams in the Americas, which is aimed at improving the dissemination of alerts in the region.

Colombia agrees that it is necessary to strengthen coordination and cooperation among States in order to consider threats and possible cooperative measures to address them. It is particularly important to enhance international cooperation, not only in the form of the transfer of knowledge, technologies and best practices, but also in the shape of joint and coordinated action.

It is also essential that countries that are less technologically advanced establish agreements to ensure that cyberspace does not become a stage for escalating conflict, in view 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 these countries, any harm to critical cyberinfrastructure can have an enormous impact, not only because of dependence on information and communications technologies (ICTs) 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.

Consequently, the lack of capacity should be taken into account as a risk factor, and international cooperation mechanisms are therefore needed to examine risks and build capacities.

In addition, the lack of risk categorization and of prevention and protection measures related to critical activities represents risks for States that are less advanced in the area of digital security. The lack of digital security governance frameworks which, in turn, hinders inter-agency and international coordination, also poses a risk.

In addition to new threats or threats which may arise in the future owing to the dizzying pace of technological development, the issues of responsible State behaviour in cyberspace and of information and telecommunications security must be addressed using a transnational approach in order to effectively counter threats. Joint efforts are required, both in ensuring the timely dissemination of information, including the responsible exchange of information on vulnerabilities, and in responding effectively to potential threats.

Colombia reiterates its full readiness to continue to enhance coordination and cooperation in considering current and potential threats, as well as possible measures, including cooperation, to address them.

Voluntary norms, rules and principles for the responsible behaviour of States

Colombia fully agrees with the concepts, considerations, interpretations and recommendations set forth in the reports of the groups of governmental experts, in particular that of 2015, which built on the work of its predecessors, and whose recommendations were welcomed that same year by the General Assembly as a guide for the use of ICTs by Member States.

Efforts in the immediate term should focus on the broad dissemination and implementation of those recommendations. Colombia does not believe that a binding instrument is required at present.

International cooperation is also important in order to strengthen national capacities to implement the recommendations.

Consistent with the purposes of the United Nations, including to maintain international peace and security, Colombia reiterates its readiness to cooperate in

developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

In that connection, on 23 September 2019, Colombia supported the statement prepared by the United States of America on advancing responsible State behaviour in cyberspace, which reflects a joint commitment by several countries to ensuring greater accountability and stability in cyberspace through cooperation aimed at more effectively responding to and deterring malicious, disruptive, destructive and destabilizing cyberactivities. The statement emphasizes that responsible State behaviour in cyberspace must be guided by international law, adherence to voluntary norms of responsible State behaviour in peacetime and the implementation of practical confidence-building measures.

Colombia also supports the Paris Call for Trust and Security in Cyberspace, an initiative of the Government of France launched on 12 November 2018, which promotes the development of common principles to enhance security in cyberspace, and which has received support from various countries, private companies and civil society organizations.

In addition, Colombia supports the Christchurch call to eliminate terrorist and violent extremist content online, an initiative of the Governments of France and New Zealand, launched in May 2019.

Colombia has public policies in place at the national level, which are contained in contained in documents of the National Council for Economic and Social Policy. In 2011, it formalized its efforts to recognize cybersecurity and cyberdefence as cornerstones of national defence. To that end, the national Government issued National Council for Economic and Social Policy document No. 3701, entitled “Policy guidelines for cybersecurity and cyberdefence,” whose overall objective was to strengthen State capacity to address threats to national security and defence in the cyberdomain (cybersecurity and cyberdefence), in order to create an environment and conditions where cyberspace is protected. Progress was made in three key areas: (a) establishment of bodies focused on addressing cybersecurity incidents, and issuance of guidelines to enhance State capacity to counter threats in cyberspace; (b) establishment of information security training mechanisms and expansion of the scope of relevant research; and (c) strengthening of cybersecurity laws.

In 2016, the Government issued National Council for Economic and Social Policy document No. 3854, entitled “National digital security policy”, which focused on four main objectives: (a) strengthening the institutional framework; (b) enhancing the capacities of the various stakeholders to identify, manage, address and mitigate risks to digital safety in their online socioeconomic activities; (c) promoting shared responsibility; and (d) incorporating a risk management approach into the online activities of the various stakeholders.

Since 2019, the Government has been designing a public policy on digital trust and security, whose objectives include evaluating and updating the digital security governance framework in order to improve it. This policy provides for the establishment of a national cybersecurity incident management system with the following aims: (a) coordinating institutional efforts to ensure the timely management of cybersecurity incidents; (b) serving as the official source of statistics on cybersecurity incidents reported in the country; (c) standardizing a mechanism for periodic reporting of incidents and vulnerabilities so that they can be identified, assessed and communicated to stakeholders; and (d) informing decision-making by the national Government. We are planning to implement the technology underlying the system. The information in the system will be available for consultation in real time by State security agencies.

International cooperation on security matters, and the use of innovation, science and technology to strengthen defence sector capacities, have been incorporated into the strategic transformation objectives of the policy guidelines for defence and security.

Colombia engages in diplomacy in the areas of cybersecurity and cyberdefence within the framework of cooperative security through strategic international partnerships. For example, it exchanges knowledge as a global partner of the North Atlantic Treaty Organization and, under the Individual Partnership Cooperation Programme, is enhancing the capacities of the national military forces and their coordinated efforts to address threats and protect cyberspace.

Colombia has also developed guidelines on the basis of international best practices and standards for the establishment and operation of computer security incident response teams for the private, public and mixed public-private sectors, in order to ensure the operational management of cybersecurity incidents which affect national interests; promote cooperation, collaboration and international assistance in digital security, cybersecurity and cyberdefence with members of computer security incident response teams in the Americas and in Europe; and exchange experiences and best practices.

For its part, the Joint Cyber Command participates in the Ibero-American Cyberdefence Forum in order to advance cooperation, share lessons learned, strengthen capacities to manage transnational risks and threats in cyberspace, and take part in national and international exercises.

Through the Cybersecurity Capacities Centre of Colombia, the Cyber Police Centre carries out analysis, issues prevention alerts, engages in activities associated with the management of cybersecurity incidents and initiates investigations into cybercrimes.

The Commission for the Regulation of Communications has the following objectives: (a) developing mechanisms to promote cooperation on digital security between communications service providers and the Computer Emergency Response Group of Colombia; (b) centralizing sectoral information on information security incidents within the entity responsible for managing such information; and (c) providing the Response Group with the information necessary to manage and raise awareness of incidents for the benefit of the various stakeholders.

To that end, the Commission for the Regulation of Communications issued decision No. 5569 of 2018, in which it stipulated that every telecommunications network and service provider must implement an information security management system and adjust its processes in order to ensure the integrity, confidentiality and availability of data.

It should be noted that the recommendations made by the Organization for Economic Cooperation and Development in the document *Digital Security Risk Management for Economic and Social Prosperity* have been taken into account in the digital security policy.

In that document, the Organization for Economic Cooperation and Development states that digital security risk management should begin with the definition of economic and social objectives or the design of specific activities so that, during the risk management phase, the level of risk associated with the activity may be assessed and any potential impact on economic and social objectives may be determined.

Subsequently, during the risk treatment phase, stakeholders should determine how strategies should be modified to increase the likelihood of success of the activity and preserve the established objectives, by deciding whether the risk should be taken,

reduced, transferred or avoided. To reduce the risk, they can select and apply security measures, or consider innovation and preparedness measures.

Accordingly, in case of ICT incidents, Colombia considers all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.

With regard to the characterization of incidents and their mandatory reporting to the competent authorities, the Commission for the Regulation of Communications, in defining categories of information security incidents in decision No. 5569 of 2018, also took into account the guidelines and best practices set forth in the 27000 series of standards developed by the International Organization for Standardization and the International Electrotechnical Commission (in particular the categories identified in standard No. 27035-1). Under that decision, when information security incidents occur, communications network and service providers are required to send an electronic report to the Computer Emergency Response Group of Colombia after containment, eradication and recovery.

In line with the recommendation that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, the State of Colombia prevents and responds to cybersecurity incidents of all classifications and types throughout the country through the Digital Security Committee, whose members include State cybersecurity entities such as the Computer Emergency Response Group of Colombia, the Joint Cyber Command, the Cyber Police Centre and the Government's computer security incident response team.

Colombia seeks to cooperate at the international level through information exchange, mutual assistance, the prosecution of the terrorist and criminal use of ICTs, and the implementation of other cooperative measures to address threats.

In that regard, the new National Council for Economic and Social Policy document on digital trust and security, which is being developed, provides for the establishment and implementation of a cyberinformation exchange system aimed at facilitating the dissemination of indicators of compromise among stakeholders which interact in the digital environment at the national and international levels. This system will be aligned with the single, central registry for digital security incidents.

The Attorney General's Office uses international cooperation channels in accordance with bilateral and multilateral agreements. However, a secure technological channel or web service needs to be established in order to enable it to directly consult and obtain information from Internet service providers, most of which are private, so that requests for mutual legal assistance can be sent, received, exchanged, considered, and responded to in a timely manner.

Under the current mechanisms, response times are slow, hindering criminal proceedings. When the response is received, the investigation is often at a stage at which it is unfeasible to use the outcome in the proceedings.

The National Intelligence Directorate has been coordinating with intelligence agencies in certain countries on developing a process for exchanging operational information in a timely manner, and for requesting additional information relating to specific incidents which require investigation or confirmation.

This coordination concerns additional information relating to incidents or trends identified in cyberspace for which the correlation of events or activity histories is required in order to monitor hostile actors that operate in cyberspace.

The Constitutional Court of Colombia has issued a number of judgments which relate to the recommendation that, in ensuring the secure use of ICTs, States should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion,

protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

For example, in Unifying Judgment No. SU-420 of 2019, the Court determined that, in Colombia, freedom of expression applies to the Internet in the same way as it does to other communications media, concluding that social networks cannot ensure a place for defamation; that, although it is not possible to make the publication of content subject to prior permission or authorization, the fact that freedom of expression has a certain priority status does not mean that it is without limits; and that, accordingly, anyone who exercises this right is subject to the consequences which arise from any impact on third parties.

For its part, the Commission for the Regulation of Communications issued decision No. 5111 of 2017, whereby it established the scheme for the protection of the rights of users of communications services, amended part II, chapter 1, of its decision No. 5050 of 2016 and set forth other provisions. Under the scheme for the protection of the rights of users of communications services, network and telecommunications service providers are required to use appropriate technological tools to prevent fraud within their networks and to verify periodically the effectiveness of these mechanisms. If a user submits a request, complaint, claim or appeal related to a case of alleged fraud, the provider must investigate it.

In order to identify the legal and regulatory reforms necessary to promote digital security and capacity-building, the new digital trust and security policy provides for the conduct of an assessment to determine which instruments require adjustments in areas such as: (a) ICT security; (b) protection and defence of privacy, freedom of expression and other human rights online; (c) responsible reporting of vulnerabilities; (d) data protection; (e) consumer protection; (f) risk and incident management; (g) incident response centres or other related entities; and (h) establishment of sectoral computer security incident response teams. This assessment will take into account the various stakeholders and will determine how the necessary adjustments will be made.

In line with the recommendation that States should take appropriate measures to protect their critical infrastructure from ICT threats, Colombia is seeking to develop, through coordination with the various relevant stakeholders, a critical infrastructure security and defence plan for the ICT sector, setting forth general guidelines for organizations in the sector. This document will be an initial step towards strengthening and coordinating efforts to protect such infrastructure.

Colombia engages in international cooperation and responds to requests from other States to mitigate malicious ICT activities. For example, on 16 March 2020 it acceded to the Convention on Cybercrime. It has also taken steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

With regard to the responsible reporting of ICT vulnerabilities and the sharing of associated information on available remedies for such vulnerabilities in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure, the new digital trust and security policy provides for the establishment of a procedure to promote responsible reporting of vulnerabilities in the information systems and technological infrastructure of State entities so that they can be remedied by the relevant entity.

In addition, the national Government, through National Council for Economic and Social Policy document No. 3854 of 2016, issued guidelines for the establishment of computer emergency response teams and cybersecurity incident response teams.

Voluntary confidence-building measures

Colombia is deeply committed to continuing to develop and adopt measures to enhance confidence and security in cyberspace. Relevant work has been done at the regional level through OAS.

In April 2017, Canada, Chile, Colombia, Mexico and the United States led the adoption of the resolution on the establishment of a working group on cooperation and confidence-building measures in cyberspace in the Inter-American Committee against Terrorism of OAS. In February 2018, Colombia was elected Chair of the working group. At the group's second meeting, which took place in Chile in April 2019, Chile succeeded Colombia as Chair.

The confidence-building measures adopted by OAS in the area of cybersecurity are as follows:

1. Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks and other documents that each member State considers relevant;

2. Identify a national point of contact at the policy level able to discuss the implications of hemispheric cyberthreats;

3. Designate points of contact, in the event that none exist, within ministries of foreign affairs, with the purpose of facilitating the work on international cooperation and dialogue in cybersecurity and cyberspace;

4. Develop and strengthen capacity-building through activities such as seminars, conferences, workshops on cyberdiplomacy for public and private sector officials;

5. Foster the inclusion of subjects related to cybersecurity and cyberspace into training courses for diplomats and officials of ministries of foreign affairs and other government agencies;

6. Foster cooperation and the exchange of best practices related to cyberdiplomacy, cybersecurity and cyberspace through the establishment of working groups, other dialogue mechanisms and the signing of agreements among States.

In particular, the confidence-building measures related to cyberdiplomacy represent an important contribution that is being made through OAS.

Through cyberdiplomacy, it is possible to identify ways to address cybersecurity challenges. This not only requires promoting the active participation of States in international debates on cybersecurity, an objective which, in turn, involves providing relevant training to diplomatic officials, but also requires ensuring the active participation of experts in multilateral forums.

Consideration should be given to promoting regular institutional dialogue with broad participation, and to expanding and supporting practices in cooperation among computer emergency response teams and cybersecurity incident response teams.

With respect to the proposed establishment of a comprehensive list of points of contact, points of contact should be designated at different levels, for example, one point of contact at the political and diplomatic level, and others at the technical level (policymakers, offices of attorneys general, computer emergency response teams, etc.).

It will be important to determine who will manage information and ensure that it is kept up to date. The development of a protocol for clear and open management of information, including databases, should be considered.

With regard to the identification of national points of contact at the technical and policy levels to address serious ICT incidents, the Ministry of Information and Communications Technology has clearly identified the individuals responsible for addressing each dimension of digital security. The relevant data may be shared with any bodies that require them.

The Ministry of Information and Communications Technology also has a directory with contact information for the chief information officers and chief information security officers of State entities and for the various stakeholders, who have been involved in discussions on digital security guidelines and in coordinated activities at each stage of incident management by the Government's computer security incident response team.

With regard to the development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, in order to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents, Colombia is actively participating in various international forums.

In particular, it has participated in debates held at the United Nations (in New York, Vienna and Geneva), and in regional mechanisms and events, primarily within the framework of OAS.

In the context of the Digital Agenda Group of the Pacific Alliance, and with the support of the OAS network of cybersecurity incident response teams in the Americas, Colombia is participating in the project for the exchange of information on cyberthreats among States members of the Pacific Alliance. In that connection, the technological platform for information exchange among the cybersecurity incident response teams of the member countries has been operational since 23 January 2020. The national node of Colombia is operated by the Computer Emergency Response Group of Colombia.

At the bilateral level, Colombia entered into a memorandum of understanding with Chile on cyberspace, cybersecurity, cyberdefence, cybercrime and cyberintelligence, which was signed on 21 March 2019 by the countries' ministers for foreign affairs. The participating entities for Colombia are the Presidential Advisory Office for Economic Affairs and Digital Transformation, the Ministry of Information and Communications Technology, the Ministry of Defence, the Cybersecurity Capacities Centre of Colombia of the National Police, the National Intelligence Directorate, the Attorney General's Office, the Ministry of Justice and the Ministry of Foreign Affairs.

An exchange of experiences in the area of digital security took place between government experts from Colombia and Peru in a virtual format on 15 April 2020. Information on national policies and strategies was exchanged, and a channel for communication regarding future support activities to address ICT-related security incidents was established.

Colombia also participates in cybersecurity innovation councils, an initiative of OAS and Cisco, which are forums for collaboration among key leaders in the public and private sectors, civil society and academia in promoting innovation, raising awareness and disseminating best practices related to cybersecurity in the region. These forums represent an important contribution to the implementation of confidence-building measures in cyberspace, and may support the implementation of more effective digital security policies at the national and international levels.

International requests related to cybersecurity matters are generally channelled through the Crime Prevention Coordination Office of the Ministry of Foreign Affairs.

With regard to the enhancement of cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations, it is important to note the work being done by various government authorities and entities on the preparation of a national incident management protocol, which is aimed at promoting early and coordinated efforts to address cybersecurity incidents that may threaten the economic and social order or national security. The implementation of this protocol is critical, as it focuses on identifying the incident, examining the facts, considering the threat and identifying the appropriate method of containment or correction.

Within the Attorney General's Office there are three groups responsible for addressing issues related to cybercrime, which provide expert support and assistance in investigations arising from requests for mutual legal assistance in which the malicious use of ICTs is observed.

These groups are: (a) the Office of the Prosecutor for Combating Organized Crime; (b) the Office of the Prosecutor for Citizen Security; and (c) the Directorate of the Technical Investigation Corps. In addition to providing assistance in investigations, these expert groups promote, within the Attorney General's Office, new trends and best practices related to cybercrime and digital evidence.

The Directorate of International Affairs of the Attorney General's Office is supported by the various specialized prosecutors and by the Office's cybercrime groups in conducting investigations related to cybercrime.

The United States Department of Justice has provided training on issues related to requests for mutual legal assistance. In the United States, requesting authorities are required to meet certain evidentiary benchmarks and standards in order to gain access to stored electronic communications. Specifically, they must provide articulable and chronological facts showing that there are reasonable grounds to believe that the electronic records are relevant and material to an ongoing investigation. They must also demonstrate that there are sound and reliable facts, not merely presumed facts, which indicate that an offence has been committed, and that the email or social network account contains information related to the offence under investigation.

Similarly, within the framework of international cooperation, the National Intelligence Directorate carries out two-way coordinated investigations and inquiries in response to direct requests from countries.

International cooperation and assistance in information and communications technology security and capacity-building

For Colombia, capacity-building is a key issue with regard to technology matters.

Digital security risk management is an area in which States, the private sector and academia can work together, and consideration should be given to mechanisms for cooperation and international assistance for that purpose.

It is important to involve different stakeholders in the analysis of the cybersecurity issue. Their assistance in both the identification and the adoption of preventive security measures and incident and emergency response measures is very valuable.

It is important that States begin by identifying the areas in which they need to strengthen their capacities. For that purpose, they can use as a basis the capability maturity models that have been developed internationally.

On that basis, they should design plans that include the development of operational, administrative, human and scientific capacities and physical and

technological infrastructure, and that are designed for the bodies and entities responsible for cybersecurity and key sectors. Likewise, and as part of the strengthening of capacities, it is important to regularly update the catalogue of national critical cyberinfrastructure and the related protection plans, as well as the mechanisms for coordination between them.

Since this is a matter that concerns us all, it is essential to work on the creation of educational content relating to digital security, so that it can be included in academic curricula at different levels of education and in non-formal courses.

In view of the establishment of procedures for mutual assistance in responding to incidents and in dealing with short-term network security problems, including procedures for expediting assistance, Colombia has a national model for incident response, which establishes the protocol for the management of incidents that occur throughout the country, whereby the cyber entities act in accordance with their powers and functions.

Specifically, the Government's computer security incident response team was established to strengthen the digital ecosystem in State entities, providing them with services free of charge. The service catalogue covers three types of services: proactive, reactive and security management. These include website availability monitoring, vulnerability analysis, monitoring of security events, support for incident management and response, and awareness-raising with regard to incident management.

The Government's computer security incident response team coordinates with the other State cyber entities (the Computer Emergency Response Group of Colombia, the Joint Cyber Command and the Cyber Police Centre) to manage incidents in State entities and, through the Digital Security Committee, is involved in devising strategies to address issues that affect the digital security of private citizens and the State.

In order to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders, the Attorney General's Office also coordinates with countries in the region on strategies for timely and streamlined information exchange in national investigations in which there is knowledge of possible attacks on or breaches of critical infrastructure.

The Ministry of Information and Communications Technology, through the Government's computer security incident response team, coordinates with the Computer Emergency Response Group and the Cyber Police Centre to validate information through various international sources that make it possible to expedite mitigation and investigation actions when warranted.

With regard to the development of sustainability strategies in capacity-building initiatives relating to ICT security, guidelines and recommendations for capacity-building were included in the various public policy instruments contained in National Council for Economic and Social Policy documents Nos. 3711 and 3854 of 2016. In addition, other administrative and legal measures to strengthen the response capacity are announced by the Ministry of Information and Communications Technology and the Ministry of Defence, among others.

In this regard, for example, cooperation agreements have been concluded between the Government of Colombia and OAS, through which the parties combine their technical cooperation efforts in order to support the updating of digital security guidelines and the strengthening of technical capacities and skills for cyberrisk management through initiatives in two basic areas: (a) policy development and dissemination and (b) capacity-building.

The Attorney General's Office, through the Directorate of International Affairs, has followed the guidelines and recommendations promulgated by various multilateral organizations for strengthening security in cyberspace, with the aim of ensuring proper management of cybercrime investigations and thus reducing impunity as far as possible.

With the intention of contributing to national cybercapabilities, the National Intelligence Directorate has decided to establish a computer security incident response team for the intelligence sector to serve as a coordinating mechanism for dealing with events and incidents in the sector and to foster the dissemination of technical information on events and incidents, as well as to carry out investigations of cyberincidents.

In Colombia, priority has also been given to raising awareness of ICT security and to capacity-building in national plans and budgets, with the aim of giving security due weight in development and aid planning. In that regard, in addition to what has already been stated with regard to public policies on digital security, awareness-raising programmes have been developed with the aim of educating and informing institutions and citizens about ICT security.

The Ministry of Information and Communications Technology has endeavoured to devise a programme focused on capacity-building and, through the establishment of cooperation agreements, has conducted courses and awarded diplomas and certificates in information security and information technology management, benefiting 1,134 public servants from government agencies at the national and local levels.

Notable among these is the "Let's talk about digital government" programme, through which more than 250 information technology officials and security officers from public entities participated in a panel on building capacity for the management of security and digital risks.

A cyberchallenge for public officials, held in the city of Pereira, was attended by 40 information technology leaders. They also participated in a cybersecurity challenge, in which they addressed challenges and situations that may arise online. This exercise was organized by OAS with the support of Trend Micro, a multinational cybersecurity firm.

With regard to the "More digital security, better region" workshops, more than 1,400 officials, including information technology leaders and security officers from public entities, attended 25 meetings held in 24 cities in Colombia.

With the support of OAS, training in the region has been enhanced. For example, the course entitled "The Hague Process: international security operations and cyberspace", funded by the Kingdom of the Netherlands, has been held on several occasions. In 2019, the above-mentioned course was held in Colombia; training was provided to Colombian officials, and delegates from Latin America and the Caribbean with responsibility for cybersecurity matters also participated. The course curriculum includes topics such as sovereignty, jurisdiction, the principle of due diligence, the use of force, international human rights law, the law of the sea, peaceful agreements and other related topics, all in an academic context relating to cyberoperations.

With regard to capacity-building in forensic techniques and in cooperation measures to address the use of ICTs for terrorist or criminal purposes, the Government of Colombia hosted a regional workshop for Latin America on obtaining electronic evidence from private communications service providers as part of the prevention of terrorism and organized crime in cross-border investigations, organized by OAS, the Counter-Terrorism Committee Executive Directorate, the United Nations Office on Drugs and Crime, the International Association of Prosecutors, the National

Coordination Mechanism for Digital Security and the Ministry of Information and Communications Technology of Colombia. The workshop was attended by delegates from 13 Latin American countries (officials from the criminal investigation police and other government agencies), who received training on matters relating to obtaining cross-border digital evidence; legislative updates in the United States, Canada and the European Union; emergency disclosure requests; and the preparation of requests for mutual legal assistance, among other issues, with a view to strengthening international cooperation in the prevention of terrorism and organized crime.

During the past three years, the Attorney General's Office has approved the secondment of criminal investigation officers from the computer crime and computer forensics groups to attend important seminars and training sessions organized by OAS and the Latin American and Caribbean Internet Addresses Registry, among others, and to work with prosecutors who are familiar with and lead investigations relating to technology (as a means or an end in the commission of a crime).

In addition, with the support of private entities and local universities, various training courses have been held on combating cybercrime and improving techniques such as protocols and training in hardware and software for digital evidence analysis in order to correlate cases and detect patterns.

The National Intelligence Directorate, in coordination with the intelligence sector's computer security incident response team, plans to build capacities for penetration testing and vulnerability analysis, forensic analysis and recovery of digital information, analysis of malware and cyberartefacts, analysis of apps, an open-source laboratory and the study of cyberphenomena.

In response to the recommendation to develop regional approaches to capacity-building, bearing in mind specific issues of a cultural, geographical, political, economic or social nature, in order to promote an approach adapted to each specific case, the Ministry of Information and Communications Technology, through the security and privacy group of the Digital Government Directorate, has been implementing an information security and privacy model that brings together instruments that enable State entities at the national and local levels to deal with cyberthreats, creating a security culture that makes it possible to build situational awareness in dealing with the cyberthreats that affect organizations at the transnational level.

In addition, the authorities responsible for crime policy have been designing a national plan that covers matters relating to different forms of crime.

The National Intelligence Directorate is working on building the capacity of the national intelligence community with regard to the secure exchange of information. In that regard, a project is being developed to provide training and capacity-building for Caribbean countries in protection and the management of good practices, in coordination with the Presidential Agency for Cooperation.

In the interests of building ICT security capacity, as already noted, Colombia has participated in bilateral and multilateral cooperation initiatives with a view to improving the environment for the provision of effective mutual assistance in response to ICT incidents.

The Ministry of Information and Communications Technology has also been developing strategies for cooperation with security companies and cyber entities at the international level, to share threat intelligence at the strategic, tactical and operational levels.

The application of international law to the use of information and communications technologies

Colombia considers that international law, in particular the Charter of the United Nations and including international human rights law and international humanitarian law, applies to the "virtual" as well as to the "physical" world.

It agrees with the statement of the then Secretary-General in the foreword to the 2015 report of the Group of Governmental Experts: "Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations."

Colombia therefore considers that the general concepts of international law may be applicable in cyberspace, with the adjustments required by the nature of virtual operations.

Considering the various possible interpretations of issues associated with international law in cyberspace does not preclude the development of guides or manuals on the application of public international law in cyberspace.

In that regard, the practice relating to the Convention on Cybercrime, which has guidance notes to guide the implementation of its provisions and to bring them into line with developments in technology, could be very beneficial. This is considered a good practice that could be emulated.

Considering that the General Assembly recommended and welcomed the set of international rules, norms and principles of responsible behaviour of States enshrined in the reports of the groups of governmental experts, for Colombia the immediate task must be to step up the implementation of those rules, norms and principles. Colombia does not believe that a binding instrument is required at present.

It should also be emphasized that Colombia abides by commitments and established safeguards.

Concepts

The conceptual development that was considered necessary for a deeper understanding of concepts relating to international peace and security in the use of ICTs at the legal, technical and political levels should, given the specific nature and the novelty of their application, continue to be discussed in the context of multilateral scenarios.

These discussions are essential in order to adjust the international legal framework to the challenges of cyberspace and to be able to reach consensus on how international law is applied in this virtual space. In that regard, Colombia agrees with the conclusions of the Group of Governmental Experts set out in its 2015 report and is ready to pursue more detailed discussions with other delegations at the United Nations.

This is the only way to ensure the appropriate use of ICTs, which are essential to meet the challenges that the international community is currently facing, and to prevent them from being used in a way that is contrary to the purposes and principles of the Charter of the United Nations, including the full upholding of international peace and security.

The disruptive use of new technologies to provide services is driving a new type of relationship in the information society, which is based on the secure processing of information and the special protection of personal data and thus encourages the

promotion of the benefits of technological advances and their contribution to social and economic development.

Therefore, it is essential to strengthen the leadership of Governments in order to build a new vision in accordance with best international practices for addressing digital security risks, taking into account principles that support responsible behaviour by States, facilitate their participation in discussion forums on international digital security and encourage them to behave in a transparent and predictable manner towards their peers, thus reducing the risks of misinterpretation, escalation and conflict in digital security matters.

Lastly, the implementation of strategies and measures for the responsible use of the digital environment contributes to peacebuilding through the establishment of conditions conducive to digital coexistence based on respect, including support for freedom of expression and the appropriate use of language on the web, with a view to maximizing the benefits of ICTs and supporting adjustment to a digital future.

Denmark

[Original: English]
[29 May 2020]

Like the rest of the world, Denmark is increasingly connected through the Internet. Digital solutions are part of everyday life and help drive economic growth. As one of the most digitalized countries in the world, it is vital for Denmark to advance a global, open, stable, peaceful and secure cyberspace in which human rights and fundamental freedoms, as well as the rule of law, fully apply.

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

Denmark has taken several steps to strengthen its information security and promote international cooperation in cyberspace.

The Defence Agreement for the period 2018–2023 allocates DKr 1.4 billion to strengthened cybersecurity and cyberdefence, thereby strengthening our resilience. The Danish Cyber and Information Security Strategy 2018–2021 took further steps to increase cybersecurity. Through 25 initiatives and 6 targeted strategies addressing what are so far defined as critical sectors (energy, finance, transport, health-care, telecommunications and maritime), Denmark has enhanced the technological resilience of its digital infrastructure, improved citizens', businesses' and authorities' knowledge and skills, and strengthened coordination and cooperation regarding cybersecurity. In addition, the European Directive on the security of network and information systems is fully transposed in Danish law.

As part of the Danish Cyber and Information Security Strategy 2018–2021, dedicated cybersecurity and information security units have been established in the six critical sectors mentioned above. Furthermore, the national strategy established a forum for the dedicated sectoral units and the Centre for Cyber Security, focusing on sharing their experience in working with information security and cybersecurity. The Agency for Digitization and the Danish Security and Intelligence Service also participate in the forum.

In order to have sufficiently skilled personnel to detect and handle cyberattacks against Denmark, in particular concerning critical infrastructure, the Centre for Cyber Security has furthermore developed and executed its own intensive Cyber Academy. The Cyber Academy had 15 graduates in 2019 who are now employed in the Centre's situation centre. Beyond the Academy, the Centre for Cyber Security also supports

education and research in cybersecurity. For example, in 2019, the Centre for Cyber Security collaborated with the Copenhagen School of Design and Technology, Aalborg University, the University of Southern Denmark, Copenhagen Business School, and the Technical University of Denmark to conduct the first-ever Cyber Security Summer School.

In 2019, a public-private Cyber Security Council (Cybersikkerhedsråd) was established to qualify the work of the national authorities and the private sector, strengthen digital democracy and improve the knowledge of the threats and opportunities brought about by digitization and new technologies.

With the Danish Cyber and Information Security Strategy 2018–2021, Denmark has also strengthened its international cyberengagement by posting cyberattachés in Brussels; appointing an international cybercoordinator in the Ministry of Foreign Affairs; appointing a cybersecurity adviser to the Office of Denmark's Tech Ambassador in Silicon Valley; and joining the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence in Tallinn. This has allowed Denmark to step up its engagement in multinational cyberforums, such as the United Nations, the European Union, the North Atlantic Treaty Organization, and the Organization for Security and Cooperation in Europe. Denmark is also an active member of the Network Information Security Cooperation Group and the computer security incident response team network and is a member of the board of the European Union Agency for Cybersecurity. Through its engagement in these forums, Denmark has consistently promoted a global, open, stable, peaceful and secure cyberspace.

Moreover, Denmark played an active role in the development of the European Union 5G toolbox. The toolbox seeks to identify a coordinated European approach to 5G based on a common set of measures, aimed at mitigating the main cybersecurity risks of 5G networks.

Denmark stresses that, as the international community has made clear, cyberspace is firmly rooted in existing international law, as the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security have attested in their 2013 and 2015 consensus reports. Existing international law, including the Charter of the United Nations in its entirety, international humanitarian law and international human rights law, applies to States' behaviour in cyberspace. Denmark furthermore stresses the importance of the 11 voluntary non-binding norms for responsible State behaviour articulated in the 2015 Group of Governmental Experts reports, as a complement to binding international law.

Despite our joint efforts, the ability and willingness of State and non-State actors to conduct malicious cyberactivities are still increasing. That should be of global concern. Malicious activities in cyberspace may constitute wrongful acts under international law, as well as being destabilizing and risking escalation. Denmark remains determined to prevent, deter and respond to malicious activities and seek to enhance international cooperation to this effect. Denmark joins the European Union in calling on the international community to strengthen international cooperation in favour of a global, open, stable, peaceful and secure cyberspace where human rights, fundamental freedoms and the rule of law fully apply.

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

Existing and emerging threats

As mentioned, Denmark recognizes that cyberspace holds tremendous opportunities for increasing welfare, boosting sustainable economic growth and

improving our citizens' quality of life. Nonetheless, our dependence on digital solutions also creates certain challenges.

Denmark is concerned by the rise of malicious activities in cyberspace by State and non-State actors, as well as the use of cyberspace to infringe on intellectual property. Such actions threaten economic growth and the stability of the international community.

Never before has the need for an open, secure, stable, accessible and peaceful cyberspace been more evident than during the coronavirus disease (COVID-19) pandemic. Information and communications technologies (ICTs) enable the communication, collaboration and knowledge-sharing that the world needs in order to manage the pandemic.

Nonetheless, during the current COVID-19 crisis, we have witnessed that malicious actors will take advantage of any opportunity – even a global pandemic. This includes interfering with critical infrastructure, including hospitals essential in combating the pandemic. This is unacceptable and must be strongly condemned by all States. Moreover, States must exercise due diligence and take swift and firm action against malicious ICT activity originating from their territories.

How international law applies to the use of information and communications technologies

Denmark strongly supports a multilateral system based on the rules-based international order to deal with the existing and potential threats stemming from the malicious use of ICTs.

The international community has made it clear that cyberspace is firmly rooted in existing international law, as the Groups of Governmental Experts also attest in their 2013 and 2015 consensus reports. Denmark emphasizes that existing international law, including the Charter of the United Nations in its entirety, international humanitarian law and international human rights law, applies to States' behaviour in cyberspace.

Sovereignty, non-intervention and the prohibition of the use of force are fundamental principles of international law, and States' violation thereof will constitute an internationally wrongful act, for which States may conduct countermeasures and seek reparation under the rules of State responsibility. There is still room for strengthening the common understanding and interpretation of these fundamental principles, and Denmark supports the work of 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 – and other international and regional initiatives – in pursuing this outcome.

Importantly, the principle of sovereignty should not be used by States to limit or violate international human rights law within its own borders. Human rights law is applicable online, as well as offline, and entails both a negative and a positive obligation for States to respectively refrain from acts that violate human rights and a duty to ensure that people can exercise their rights and freedoms.

As described in the "Danish military manual", cyberspace operations do not differ from the use of conventional military capacities in relation to applicable international law. The issue is also reflected in the national *Joint Doctrine for Military Cyberspace Operations* of 2019, in which military leaders are guided to include considerations on compliance with international law when conducting cyberspace operations. Thus, international humanitarian law, including the principles of precaution, humanity, military necessity, proportionality and distinction, applies to State conduct in cyberspace and is wholly protective, by setting clear boundaries for

its legality, in times of armed conflict. Denmark would like to join the European Union in underscoring that international law is not an enabler of conflict, but a way of protecting civilians and limiting disproportionate effects.

Existing international law – complemented by the 11 voluntary non-binding norms for responsible State behaviour articulated in the 2015 Group of Governmental Experts report – provides States with a framework for responsible behaviour in cyberspace. Denmark calls on all States to adhere to this framework and implement its recommendations.

As there is already an international legal framework regarding cyberissues, Denmark does not call for, nor see the necessity of, new international legal instruments for cyberissues. However, there is room for strengthening the common understanding of how it applies. Denmark hopes that the work and recommendations of the current Group of Governmental Experts and the Open-ended Working Group will contribute to clarifications and thus facilitate much-needed State compliance, ultimately promoting greater predictability and reducing the risk of escalation.

Norms, rules and principles for the responsible behaviour of States

Denmark joins the European Union and its fellow member States in encouraging all States to build on and advance the work repeatedly endorsed by the General Assembly, notably in resolution 70/237, and on the further implementation of these agreed norms and confidence-building measures, which play an essential role in conflict prevention.

As a complement to binding international law, the norms, rules and principles of responsible State behaviour articulated through successive Group of Governmental Experts reports in 2010, 2013 and 2015 hold immense value. Denmark will continue to be guided by international law, as well as through adherence to these voluntary norms, rules and principles. Further implementation of these norms should be pursued through increased cooperation and transparency around best practices.

France

[Original: French]
[29 May 2020]

France welcomes the opportunity to respond to General Assembly resolution 74/28, on advancing responsible State behaviour in cyberspace in the context of international security, and wishes to provide the information below.

1. General assessment of cybersecurity issues

France wishes first to reiterate that it does not use the term “information security”, preferring the terms “information system security” or “cybersecurity”. France does not consider information as such to be a potential source of vulnerability. The term “cybersecurity” is more accurate, as it refers to the ability of an information system to be resilient in the face of events that originate in cyberspace and may threaten the availability, integrity or confidentiality of data stored, processed or transmitted, and related services provided or made accessible by such systems.

France believes that the digital space must remain a space of freedom, exchange and growth, contributing to prosperity and progress in our societies. 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 malicious practices. The specificities of the digital space (including relative anonymity, the low costs of, and ease of access

to, malicious tools, the existence of vulnerabilities and the proliferation of certain tools) have allowed a number of actors to carry out espionage, illegal trafficking, destabilization and sabotage. While some low-intensity threats are not a matter of national security but rather a form of crime, the use of such tools against State information systems, critical infrastructure or 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. France believes that States must retain their monopoly on legitimate violence, both in cyberspace and elsewhere. However, the spread of digital technology as a new tool and sphere of conflict gives the private sector, in particular a number of system actors, a critical role and unprecedented responsibility in safeguarding international peace and security.

2. Efforts of France in the field of cybersecurity at the national and international levels, and views of France on the substance of the concepts mentioned in the reports of the Group of Governmental Experts

France has for several years been pursuing a policy and engaging in active diplomacy to preserve, develop and promote an open, secure, stable, accessible and peaceful cyberspace, and address threats to international stability and security.

The work of the first five Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, in which France participated, enabled progress in the definition of common principles and in the collective understanding of cyberspace, particularly in the areas of international cooperation, standards and the application of international law.

Action taken by France in relation to international cooperation, capacity-building, and the promotion and development of confidence-building measures

France promotes international cooperation on cybersecurity at the bilateral, European and international levels.

In order to enhance the cyberresilience of the European Union, France is helping to develop a voluntary cooperation framework for the prevention and resolution of incidents. The framework is based, in particular, on the development of common operational norms and procedures for cooperation among partners; those standards and procedures are tested through pan-European exercises. France has also participated in the creation of a “cybertoolbox” that provides a European framework for a joint diplomatic response to cyberattacks and is based on prevention, cooperation, stabilization and response measures, in particular restrictive measures, related to cyberincidents. France is also participating in the development of the CyCLONe network for the organization of operational cooperation among European national cybersecurity agencies in the event of cybercrises, and in joint exercises to prepare for cybercrises as a complement to cooperation among those agencies’ computer emergency response teams.

Within the North Atlantic Treaty Organization, at the initiative of France, the allies adopted, at the Warsaw Summit in June 2016, a commitment to cyberdefence, the “Cyber Defence Pledge”, in which every member State undertook to devote an appropriate share of its resources to strengthening its cyberdefence capabilities, thereby improving the alliance’s overall security.

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

OSCE in the area. In particular, France, alongside the other participating States, is piloting the implementation of confidence-building measure 15, on securing critical infrastructure.

France also believes that many of the challenges related to cybersecurity should be addressed through a multi-stakeholder approach, in order to take into account the role and specific responsibilities of non-State actors. In the Paris Call for Trust and Security in Cyberspace, issued in 2018, France emphasized the need for a strengthened multi-stakeholder approach. France believes that civil society, academia, the private sector and the technical community possess expertise and resources that are useful for developing aspects of relevant cybersecurity policies. The Paris Call,[2] submitted by the President of the Republic 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. The world's largest multi-stakeholder cybersecurity initiative, the Paris Call, is now supported by 78 States and more than 1,000 non-State entities. It is intended 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 of States on legitimate violence, and recognition of the specific responsibilities of private actors.

France has also supported the development, by the Global Commission on the Stability of Cyberspace, of proposals for standards and policies to strengthen international security and stability and to guide responsible State behaviour in cyberspace. The report containing the conclusions of the Commission was presented at the second Paris Peace Forum.

France is working to ensure that the Group of 20 addresses the fundamental issues of competition in the digital economy and new methods of regulation and governance of digital security, in line with the Paris Call.

France has also been involved from within the Organization for Economic Cooperation and Development (OECD). It currently chairs the OECD Working Party on Security and Privacy in the Digital Economy and wishes to work on such matters as the responsibility of private actors, the securing of products and services, and the responsible disclosure of vulnerabilities.

In the area of capacity-building, owing to the high level of connectivity between networks and societies, France believes that cybersecurity for all will be ensured only once each State has sufficient capacity to secure its own information systems. It is therefore strengthening the cybersecurity capacities of its partners, bilaterally or multilaterally. Such efforts to improve cooperation are beneficial to all parties: they allow us to remain up to date by engaging with and learning from our peers, and they foster the mutual enrichment of knowledge and expertise and the development of trust among the stakeholders involved. In recent years, France has also deployed international technical experts in cybersecurity within the internal security forces of partner countries. For example, France is working with Senegal to continue the activities of the national school for cybersecurity in Dakar, an institution that has a regional scope and was 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.

[2] Available at https://pariscall.international/en.

Definition of standards of responsible behaviour: a major achievement

France has established a set of mechanisms, through its national doctrine, governance arrangements and laws, to apply the norms of behaviour recommended in the reports of the Group of Governmental Experts, in particular the 2015 report (A/70/174). The information provided below is intended, without being exhaustive, to illustrate the ways in which France has sought to implement the norms.

> Norm (a): Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of information and communications technologies (ICTs) and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

France has taken a set of measures in response to this norm, in particular by consolidating a national cybersecurity strategy focused on defence, prevention, resilience and cooperation. In our strategic review of cyberdefence, issued in February 2018,[3] a doctrine for crisis management is established and our objectives are clarified. The French model, in which a distinction is made between institutions that are responsible for offensive capabilities and those that conduct defensive missions, is confirmed, and the diplomatic objective of developing confidence and stability in cyberspace is strongly affirmed.

France is also establishing bilateral strategic dialogues with various partners on cybersecurity issues. It is also active in many forums for regional and international cooperation and coordination, as mentioned above.

France has also recognized that it has the capacity to conduct defensive and offensive military operations in cyberspace in order to guarantee its national sovereignty, in strict compliance with national and international law. In order to ensure transparency and consistency, it made its doctrines accessible to as many people as possible in 2019 by publishing several documents on, among other things, military doctrine related to offensive cyberwarfare, and a white paper on international law applied to military operations in cyberspace. This desire to clarify and share the country's vision should make it possible to limit misunderstandings and uncertainties, and thus help to consolidate confidence and transparency in cyberspace. France encourages all other States to do the same.

> Norm (b): In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

France has established the following crisis management procedures and national structures and policies in the event of a technology-related incident:

– An interministerial crisis cell, deployed in the event of a major crisis;

– A cybercrisis coordination centre that meets every month and comprises technical or operational layers and a high-level, interministerial, strategic layer whose members analyse cyberincidents in a broader context, evaluate their consequences and may consider attribution. For France, the attribution of an attack and the decision to make that attribution public are sovereign prerogatives.

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

France has developed means of assessing incidents, including through a severity scale to help decision makers to conduct analyses and take action. In determining the severity of an incident, France takes into account, among other things, its consequences for the following:

– The interests and sovereignty of the nation, and democracy

– Domestic and civil security

– People and the environment

– The economy

Other criteria, such as intent, dangerousness, attribution, volume and recurrence, may be taken into consideration.

Norm (c): States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

In order to ensure that its territory is not used to carry out malicious acts, France has:

– Required operators of vital importance, namely, operators of national critical infrastructure (see Act No. 2013-1168) and operators of essential services (see Act No. 2018-133), to strengthen the security of their information and communications systems;

– Criminalized, in article 323-1 of the Criminal Code, unauthorized intrusions into third parties' information security systems;

– Strengthened, through Act No. 2018-607, the capacity of the National Cybersecurity Agency to detect cyberincidents affecting operators of critical infrastructure;

– Encouraged the responsible disclosure of vulnerabilities through Act No. 2016-1321, under which individuals who inform the National Cybersecurity Agency of a vulnerability in a digital product or service are protected from legal action.

Norm (d): States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

In addition to the information provided above regarding cooperation, France has developed a range of measures to improve cooperation with its partners to prevent the criminal and terrorist use of information technologies, in particular by acceding to the Convention on Cybercrime (Budapest Convention) and supporting the Christchurch Call to eliminate terrorist and violent extremist content online.

At the technical level, the National Cybersecurity Agency continues to establish partnerships with its counterparts in many countries in order to encourage the sharing of critical data, such as information on vulnerabilities or faults in products and services. In addition, the government computer emergency response team, part of the National Cybersecurity Agency, is active in several multilateral networks (the Forum of Incident Response and Security Teams, the European Task Force on Computer Security Incident Response Teams, the European Government Computer Emergency Response Team and the Computer Security Incident Response Team Network of the European Union) through which it maintains contacts with computer emergency response teams worldwide.

Norm (e): States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and

enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

France attaches the utmost importance to the principles that human rights must be respected and promoted on the Internet and that individuals must enjoy the same rights online as offline. Since 1978, the National Commission on Information Technology and Freedoms has been the authority responsible for ensuring respect for human rights and fundamental freedoms, in particular the rights to privacy and freedom of expression, in the country.

France has also been involved in the adoption of European regulations that take into account requirements related to competitiveness and the potential of digital technology, while continuing to protect Member States' citizens and businesses (including the right to privacy and personal data protection, the protection of critical infrastructure and the fight against online terrorist content). That desire was clear in 2016 during the adoption of Regulation (EU) No. 2016/679 of the European Parliament and of the Council 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) No. 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, and in the support of France for the enhancement of the competences of the European Union Agency for Cybersecurity. Lastly, France is working to ensure that the European Union, through its industrial policy, supports advanced research and development capacities in order to foster the deployment of digital security technologies and services that are reliable and independently assessed. France also actively participated in the drafting of the European Union human rights guidelines on freedom of expression online and offline, adopted by the Council on 12 May 2014.

In the Council of Europe, France supports action to protect human rights on the Internet. For example, it supported the adoption, in April 2014, of the "Guide to human rights for Internet users", which was drafted by the Committee of Ministers of the Council and in which particular emphasis is placed on freedom of expression, access to information, freedom of association, the right to privacy, the protection of personal data and protection against cybercrimes; those rights and freedoms apply equally online and offline.

At the United Nations, France has supported the adoption of all Human Rights Council resolutions on the promotion of the protection and enjoyment of human rights on the Internet, and General Assembly resolution 68/167, on the right to privacy in the digital age.

At the second Paris Peace Forum, held in November 2018, the President of France, Emmanuel Macron, and 11 other Heads of State and Government also announced the launch of an intergovernmental initiative on information and democracy, building on the work already done on the subject by the non-governmental organization Reporters Without Borders. That initiative is now under the auspices of the Alliance for Multilateralism, launched by France and Germany.

Norm (f): A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

In the spirit of this norm, and as mentioned above, France has criminalized, in article 323-1 of the Criminal Code, unauthorized intrusions into the automated data processing systems of third parties.

France has also clearly established, in the public elements of its doctrine, including its 2019 white paper on international law applied to operations in cyberspace, that international humanitarian law applies fully to cyberoperations conducted in the context of and in connection with armed conflict, as will be discussed in greater detail below in relation to international law.

> Norm (g): States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

France has, as stated above, developed a regulatory framework to protect critical infrastructure by requiring operators of vital importance to strengthen the security of the critical information systems that they operate, known as information systems of vital importance (Act No. 2013-1168 of 18 December 2013), and by strengthening the competences and capacity to detect incidents of the National Cybersecurity Agency. Operators of vital importance must also strengthen their security measures and use detection systems approved by the Agency. France encourages public-private cooperation to develop critical infrastructure protection and define an effective and appropriate framework.

> Norm (h): States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

To comply with this norm, France has, for example, developed a network of trust-based cooperation through technical partnerships of the National Cybersecurity Agency, a network that, among other things, enables contact among computer emergency response teams through permanent contact points.

In order to organize crisis management, France has also set up a permanent interministerial mechanism for threat analysis, preparation and coordination, in the form of a cybercrisis coordination centre. In particular, the centre allows information to be exchanged smoothly among the various services to improve national coordination and respond to these needs.

France has also set up a round-the-clock network of points of contact under the Convention on Cybercrime to allow data freezing.

At OSCE, France has been involved in putting into operation the list of contact points established pursuant to confidence-building measure 8 of Permanent Council Decision No. 1106, and has supported various efforts to ensure that each State establishes appropriate channels of exchange and information in accordance with confidence-building measure 13 of Permanent Council Decision No. 1202.

> Norm (i): States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

France has encouraged the development of norms and standards for the industry, notably through the Paris Call. It has also promoted the launch of international work on the subject in various forums, mainly through the Digital Economy Task Force of the Group of 20 and at OECD.

France has also promoted the use of third-party certification principles, under the authority of the National Cybersecurity Agency, to ensure that the market provides the highest level of security. This process is being piloted at the Agency by the National Certification Centre. France has also promoted the establishment of such certificates at the European Union level.

In order to strengthen efforts to counter the proliferation of malicious tools and techniques, France has also supported the inclusion of intrusion software in the list of dual-use goods of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

> Norm (j): States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

As stated above, France has taken various steps to allow the responsible disclosure of computer vulnerabilities and has developed cooperation at the technical level through the National Cybersecurity Agency, which regularly exchanges information on vulnerabilities and available solutions with its counterparts and partners.

> Norm (k): States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Act No. 88-19 of 5 January 1988 on computer fraud, known as the Godfrain Act, was the first French law to punish computer crime and hacking. It criminalizes the act of fraudulently accessing or remaining in all or part of an automated data processing system.

The French governance model, under which offensive capabilities are distinguished from defensive capabilities and missions, ensures that that principle is respected. The missions of the government computer emergency response team include the coordination and investigation of responses to cyberincidents, not only for the Government but also for operators of critical infrastructure and essential services as defined in law, by helping those operators to establish the necessary level of protection, detect vulnerabilities in networks and systems, organize the response to incidents, with the help of partners if necessary, and participate in a trusted network of computer security incident response teams.

Application of international law, including the Charter of the United Nations, to cyberspace: another principle recognized by the Group of Governmental Experts

France believes that the emergence of a collective cybersecurity framework can be based only on compliance with the rules of international law. It therefore does not believe that a new legally binding international instrument dedicated to the challenges of cybersecurity needs to be established at this stage. Existing international law applies to cyberspace, as it does to other spheres, and must be respected.

As the Group of Governmental Experts concluded in its 2013 report, the principles and rules of international law apply to the behaviour 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.

The principle of sovereignty applies to cyberspace. France therefore reaffirms that it exerts its sovereignty over information systems, individuals and cyberactivities in its territory or under its jurisdiction, in accordance with its obligations under international law. The unauthorized penetration of French systems and the resulting effects in French territory through the use of offensive electronic means by a State entity or by non-State actors acting on the instructions or under the 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 depends on the seriousness of the attack's effects. A cyberoperation can therefore 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 depends not on the electronic means used but rather on the effects of the cyberoperation. If the effects are similar to those of conventional arms, a cyberoperation can be understood as a use of force. In the view of France, if the scope or effects of a major cyberattack perpetrated by a State, or by non-State actors acting under the control or on the instructions of a State, reach a sufficient threshold (such as substantial loss of life, significant material damage, or deficiency of critical infrastructure with significant consequences), that attack 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, in accordance with the principles of necessity and proportionality. 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 also recognizes that international humanitarian law fully applies to cyberoperations conducted in the context of and in relation to armed conflicts. Offensive cyberoperations are currently carried out in combination with conventional military operations.

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. In accordance with this principle, a distinction must be made between combatants, or members of organized armed groups, and civilians. The civilian population in general and individual civilians must not be targeted unless and for such time as they participate directly in hostilities. In an armed conflict, any cybercombatant who is a member of the armed forces of a party to the conflict, any member of an organized armed group engaged in cyberattacks against another party, and any civilian directly participating in hostilities through electronic means may be the target of a conventional attack or a cyberattack;

– The principle of proportionality and the precautionary principle. 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, in addition to whether those effects are direct (such as damage to the targeted system or interruption of service) or indirect (such as effects on the infrastructure controlled by the system under attack, and 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. In accordance with this principle, the use of cyberweapons that cannot be controlled in time and space is also prohibited.

This information is provided in the report on international law applied to operations in cyberspace, published by the Ministry of the Armed Forces on 9 September 2019, as well as in the public elements of French military doctrine on offensive cyberwarfare, published in the same year.

France considers that 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 here 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", to the online domain.[4] Accordingly, States should not knowingly allow their territory to be used for acts that are committed by electronic means and proscribed by international law, and must take all measures that can reasonably be expected of them to ensure that their territory is not used by non-State actors to commit such acts. France has identified the regulation of private actors' capability to respond to incidents as an important area of work, which could help to ensure that the principle of due diligence is respected by limiting actions that adversely affect third parties.[5] A better understanding of how the principle applies to challenges in the area would strengthen cooperation among States with a view to protecting certain critical infrastructure and eliminating major cyberattacks made through third countries.

Georgia

[Original: English]
[29 May 2020]

The Government of Georgia, while promoting safe, resilient, secure and reliable eGovernment solutions and developing the information society at large, closely considers every opportunity to address the recommendations of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security on advancing responsible State behaviour in cyberspace. Georgia aspires to actively contribute to the principles and guidelines provided by the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and to develop dedicated national mechanisms for that purpose.

This document summarizes important updates on cybersecurity and information security development in Georgia and efforts taken at the national level to strengthen information security and promote international cooperation.

Georgia continues to be committed to developing its cybersecurity posture and making its cybersecurity profile comparatively advanced in the international arena. Georgia's geopolitical conditions clearly raise the stakes for its cybersecurity

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

[5] Such regulation, whose underlying principle should inform the work of the Group of Governmental Experts, should be based on a risk analysis related to the measures that can be taken by private actors on their own account in response to an incident.

development efforts. On 28 October 2019, a large-scale cyberattack was launched against the websites, servers and other operating systems of the Administration of the President of Georgia, the courts, various municipal assemblies, State bodies, private sector organizations and media outlets. The cyberattack targeted Georgia's national security and was intended to harm Georgian citizens and government structures by disrupting and paralysing the functioning of various organizations. The investigation conducted by the Georgian authorities, together with information gathered through cooperation with our partners, concluded that this cyberattack was planned and executed by the Main Division of the General Staff of the Armed Forces of the Russian Federation. The above-mentioned incident reconfirms the importance of the Georgian Government's efforts to strengthen cybersecurity at the national level and again demonstrates the need for enhancing the international partnership on cybersecurity.

Georgia directs all its resources to becoming a stronger, secure and safe country in cyberspace. In particular, the Georgian Government strives to empower every target group of the information society to possess the required level of knowledge and experience to challenge cyberthreats. Georgia's governance model provides the capability for both public and private organizations, collectively and independently, as well, to ensure the country's cybersecurity and relevant sustainability by jointly sharing resources. In addition, Georgia, as a trusted partner in cybersecurity, enjoys international acclaim and support from its international partners.

The Government of Georgia is actively striving to provide an open, safe and secure cyberspace. Cybersecurity is a strategic direction of the national security policy of the Georgian Government and making it more developed and resilient is under high political attention. The Government sees its prerogative to establish an enabling environment for the information society, the digital economy and eGovernance in the country; the Government assumes responsibility for forming relevant strategic, institutional-organizational and legal-regulatory frameworks that will support the safe and secure functionality of citizens as well as the public and private sectors in an electronic environment, taking into account that they are safely using online space.

Strengthening bilateral, regional and international cooperation in the field of cybersecurity has been high on the political agenda for the Government of Georgia. Georgia serves as a good example of partnership at the regional and international levels, and in multilateral formats (European Union, North Atlantic Treaty Organization (NATO), Organization for Security and Cooperation in Europe (OSCE), United Nations, Eastern Partnership, Council of Europe, European Union Agency for Law Enforcement Cooperation, International Criminal Police Organization, European Union Agency for Law Enforcement Training, European Union Agency for Cybersecurity). Georgia actively participates in international projects and meetings relating to cybersecurity.

In past years, the following cooperation and partnership initiatives have taken place:

- Steps aimed at strengthening cybersecurity which have been taken by Georgia in the past decade are positive, and implemented reforms and ongoing processes are positively assessed at an international level. Georgia ranks high and is in a leading position in terms of cybersecurity development among the Eastern Partnership, which is why regional countries are involved in multiple activities for capacity-building and the sharing of information and best practices, in which Georgia plays the role of a regional cybersecurity hub.

- Georgia-NATO cooperation in the field of cybersecurity is in the development phase. Georgia is in an active phase of collaboration with NATO member States

and participates both individually and collectively in various projects administered under the patronage of NATO. This also includes Georgia's participation in strategic or technical learning initiatives. NATO (headquarters and Liaison Office), assists Georgian cyberauthorities in performing systematic and ongoing awareness-raising and training activities throughout Georgia directed at different target groups. Georgia regularly presents its cybersecurity achievements and initiatives to the NATO-Georgia Commission and closely guides itself using the NATO Cyber Defence Pledge.

- Georgia and the European Union. Through the five-year programme, "EU4 Security, Accountability and the Fight against Crime in Georgia", Georgia receives assistance from the European Union in the fields of cybercrime, cyber and hybrid threats handling, border management, civil protection and supervision of the security sector. Georgia strengthened its cooperation within the framework of the European Union Common Security and Defence Policy platform, which echoes the internationally defined strategic goals of the organization and, in total, by developing Georgia's defence capabilities, supports consolidating its national security.

- Georgia and OSCE. Georgia sees great value in building a trusted network between partner countries, enabled by confidence-building measures in the field of cybersecurity. Georgian points of contact actively participate in the OSCE cybersecurity platform and its initiatives.

- The Governments of Georgia and the United Kingdom signed the Memorandum of Understanding on Cyber Security Cooperation. Its aim is to enhance mutual work, share best practices and better align approaches on different topics of cybersecurity.

- Georgia and Eastern Partnership countries. The Data Exchange Agency continues cooperation with Eastern Partnership countries within the scope of the "EU4 Digital: Improving Cyber Resilience in the Eastern Partnership Countries" programme. The CyberEast project helps Georgia and other Eastern Partnership countries to increase the capacities of cyberresilience, criminal justice and electronic evidence of the Eastern Partnership countries, to better address cybercrime. The focus is on improving legal and policy frameworks; reinforcing the capacities of judicial and law enforcement authorities and inter-agency cooperation; and introducing efficient international cooperation mechanisms to increase trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement.

- Georgia continues strengthening regional cooperation with neighbouring countries under the umbrella of the Organization for Democracy and Economic Development. In 2019, Georgian representatives took part in meetings at the premises of the Organization for Democracy and Economic Development in Kiev.

- The Computer Emergency Response Team, a subsidiary unit of the Data Exchange Agency of the Ministry of Justice of Georgia, has signed a considerable number of memorandums of cooperation to share knowledge and experience with the respective organizations of European and Eastern Partnership countries (i.e., Lithuania, Romania, Moldova, Ukraine and Belarus). Georgia is actively participating in international cyberexercises and study programmes, in which the country constantly takes leading places in terms of observed results.

As a matter of practice, Georgia, with its immense national knowledge in the field, considers international best and most relevant expertise as valuable guidance and

opportunities for cooperation in the development of its strategic, legal, institutional and capacity-building pillars, as well as for the cyberculture transformation process.

With active cooperation between sectoral agencies[6] in the field of cybersecurity, the third draft of the national cybersecurity strategy and its action plan were elaborated in Georgia in 2019.[7] The Office of the National Security Council played a coordinating role in this process. At the same time, relevant stakeholders from the private sector, academia and civil society were also involved in the respective endeavours. As Georgia strives to make its national framework compatible with the respective Euro-Atlantic mechanisms, the strategic development process is heavily advised by foreign experts and like-minded national consultants. Of special significance in the context of drafting the national cybersecurity strategy and its action plan was the assistance rendered by the United Kingdom to relevant Georgian cybersecurity actors. The draft national cybersecurity strategy and its action plan will be approved by the Government of Georgia in the course of 2020. The respective documents will undergo the scrutiny of the permanent inter-agency commission created in January 2020 at the National Security Council and entrusted with the function of coordinating the elaboration of the national-level conceptual documents in the field of security. Subsequently, the draft documents will be submitted by the National Security Council to the Government of Georgia for approval.

Georgia continues to strengthen the enforcement of legal and regulatory frameworks for the cyberdomain. Comprehensive information and communications technology legislative and regulatory frameworks addressing cybersecurity have been implemented, and legislation protecting the rights of individuals and organizations in the digital environment has been adopted in Georgia. Laws address the protection of the critical information infrastructure, the liability of Internet service providers, incident reporting obligations and the security of e-transactions. As a next step, Georgia has ambitious plans to make its cybersecurity legal framework compatible with the European Union Directive on the security of network and information systems. Namely, responsible agencies, in the course of 2019, have already initiated the cooperation process with the European Union and, by the end of this year, the Twinning Fiche will be developed, with the aim of helping Georgia with the harmonization process. As a result of the twinning project, Georgia will update its Information Security Law, which, among other important aspects, will clearly define a cybersecurity governance framework, authorities for the Directive, and roles and responsibilities in cybersecurity at the strategic, operational and tactical levels.

Georgia has also started another ambitious process of designing and adopting a European Union-compatible model for critical information infrastructure protection. In the course of 2019, several workshops were conducted in order to discuss a proper system for identification and cooperation with critical infrastructures in the cyberfield. Georgia created a relevant methodology and questionnaires for critical information infrastructures. The process involved discussions with privately owned critical sector representatives from different sectors and business fields.

Currently, information security policy and cybersecurity requirements are in the process of being implemented in all those organizations defined as critical information infrastructures. The responsible State agencies assist these entities in the implementation of information security policies and cybersecurity essentials, providing recommendations, expertise and trainings, as well as through more comprehensive activities, such as information security audits, penetration testing and other information and cybersecurity services. Various projects for the implementation

[6] Data Exchange Agency (Ministry of Justice), Cybersecurity Bureau (Ministry of Defence), Operative-technical Agency (State Security Service).

[7] Foreseen for the three-year period 2020–2023.

of an information security management system have been launched in the agencies that are part of the critical information system. These entities are supported in the adoption of information security policies, asset management tasks and policy reviews. At the same time, the Government sets standards and procedures for information security through legislation and by-laws (based on the ISO 27000 family of standards) and delivers training courses on information security for government and private sector representatives. The next goal is to develop and adopt legal provisions on critical information infrastructure protection in harmonization with the European Union Directive on the security of network and information systems, guaranteeing that expanded legal provisions regarding the security of networks and information systems are applicable to critical information infrastructure protections.

The Government of Georgia successfully uses the public-private multi-stakeholder platforms as a tool for creating trust among all stakeholders and sharing information and knowledge, realizing new initiatives and enabling private sector engagement in the policy and strategy development process. The Data Exchange Agency, leading the public-private cooperation process, conducted numerous workshops and meetings in the course of 2019 with the financial, energy and telecommunications sectors in order to join preparatory consultations for the critical infrastructure identification process. Private stakeholders are part of all the major consultation processes about horizontal projects in strategy, policy, legal, regulatory and capacity-building initiatives.

Georgia performs systematic and ongoing awareness-raising and training activities for building up cyberprofessionalism and proficiency, directed to different target groups. Through the engagement of Georgia's State organizations, wide-scale awareness-raising campaigns aimed at increasing the population's knowledge level on cyberhygiene have been carried out; also, at present, learning-retraining programmes for various target groups in the field of cybersecurity are being actively administered. Year after year, the Georgian cybersecurity capacity maturity level is improved as a result different initiatives and educational programmes, the Government of Georgia has been and is very active in its attempts to raise the qualifications of cybersecurity professionals employed in the public sector. As a result, their professional proficiency is high, and many of them are in possession of internationally recognized, highly reputable certificates (SANS Institute, Information System Audit and Control Association, International Organization for Standardization).

Finally, Georgia will continue its active participation in the international dialogue on Internet governance and other international initiatives relating to collective cybersecurity.

Honduras

[Original: Spanish]
[17 April 2020]

Report on measures taken with regard to cyberspace in the context of international security

The National Police of Honduras is taking various internal steps in the context of the International Organization for Standardization (ISO) 27001 (international information security standard) and with a view to creating a working culture consistent with the digital government initiative promoted by the Office of the President of the Republic. These steps are focused on the responsible use of Internet resources in accordance with its information security manual, which contains a clear statement of the policy established to protect the different operational activities of our officers and reduce the vulnerability gap whereby our systems could fall victim to an attack or malicious act.

Some of the measures adopted by the National Police with regard to cyberspace are set out below.

1. Development of the information security policy

The information security policy establishes standards and guidelines to ensure appropriate use of technological tools designed to protect the information technology and physical resources of the police, as a key input for the fulfilment of its constitutional mission, and to guarantee continuous improvement, managing and protecting the mission through the effective application of best practices and controls and guaranteeing the confidentiality, availability and integrity of information in general.

2. Training sessions

The National Police of Honduras, through the Police Telematics Directorate, holds cyberspace awareness sessions for operational and administrative personnel on an ongoing basis. It also participates in special activities, providing training on issues such as cyberbullying, social engineering, fake news, cybercrime and cybersecurity.

3. Implementation of a local network

Our intranet page, “Poliweb”, is used to keep our staff informed about the latest trends in cybercrime, publish important newsletters on cybersecurity developments in our environment and disseminate policies derived from the information security manual for the preservation of computer security.

This internal connectivity allows all internal operations of the National Police to be carried out through our local network or intranet, thus minimizing the risk of our users accessing unknown sites and saving Internet resources and bandwidth.

4. Incident management and investigation

The information security team carries out continuous monitoring of the institutional data network, identifying vulnerabilities in and threats to equipment that may be caused by our users, either through inappropriate Internet surfing or through attempts to circumvent our restrictions. At the same time, steps are being taken to investigate and manage computer incidents in the institutional network. The Information Administration Section and the Incident Management Section of the Information Security Department analyse known vulnerabilities that could put institutional systems and information at risk. These vulnerabilities are appropriately managed and remedied through the following formal procedure:

- Addition to information asset inventories of data relating to the software provider, version, current deployment status and the officer responsible for the software.
- Biannual conduct of vulnerability analysis.
- Maintenance of up-to-date information on new vulnerabilities.
- Establishment of a timeline for applying fixes and remedies for known vulnerabilities.
- Testing of fixes or patches for vulnerability remediation before deployment in production environments.

5. Audits

Compliance with the policies issued for the correct use of computer equipment and police Internet connections is verified through the annual audit plan.

Some of the restrictions are as follows:

- Prohibition of the installation of virtual private networks (VPNs) on computers.
- Prohibition of the use of various incognito browsers, such as Tor, I2P, DuckDuckGo and Whonix.
- Prohibition of the use of social networks (with exceptions for special directorates).
- Prohibition of the use of high-consumption streaming sites such as digital television and video playback sites.
- Prohibition of the storage of personal documents and installation of non-work-related software.

The information systems, as well as the servers, network devices and other technological services, keep audit records (logs) that include, whenever possible:

- The user identification.
- The date and time of the transaction.
- The IP address and name of the device from which the transaction was made.
- The transaction type.
- The transaction identification.
- The data consulted, modified or deleted.
- Failed connection attempts.
- Changes in the system configuration.
- Change or revocation of privileges.
- Files accessed.
- Alarms originating from control systems.
- Deactivation of protection mechanisms.

6. Antivirus software

Antivirus software is kept active as another layer of protection against malware; it provides us with anti-phishing capabilities, protection against zero-day attacks, anti-ransomware capabilities and ongoing updates of security patches.

7. Firewall administration

Network segmentation and authorization are carried out by means of “firewall” perimeter security software, which blocks attempted intrusions into our network and counts logins by our users, identifying website views and logins to the different institutional systems.

8. Encrypted communications

With regard to response to national security emergencies and the internal coordination of the National Police, we have a state-of-the-art radio communication system with security encryption to safeguard the integrity of our communications.

All the adopted measures are improving the protection of institutional information and contributing to efforts to prevent a cyberattack, bearing in mind that we do not have protection measures for our systems. At present there is no totally secure system but, by implementing some of these measures, we are reducing the vulnerability gap and ensuring the governance of cyberspace with regard to the identification and blocking of cyberattacks.

Hungary

[Original: English]
[15 May 2020]

General appreciation of the issues related to cyberspace in the context of international security

In December 2019, the General Assembly adopted a resolution on advancing responsible State behaviour in cyberspace in the context of international security. In the resolution, the Assembly invites Member States to continue to inform the Secretary-General of their views and assessments on the efforts taken at a national level to strengthen information security and promote international cooperation in this field and the content of the concepts mentioned in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Hungary would welcome the continuation of the process to discuss voluntary norms, rules and principles for responsible State behaviour, confidence-building measures and international law on a regular basis under the United Nations First Committee and the establishment of further Groups of Governmental Experts.

In 2018, Hungary supported General Assembly resolutions 73/266 and 73/27, respectively, which established another Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and an Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security as important next steps in addressing the threats posed by the use of information and communications technologies (ICTs).

For the first time, Hungary is also part of these negotiations, although we followed the work of the previous Groups of Governmental Experts with great interest, including during the adoption of our first National Cyber Security Strategy in 2013. Since its establishment, Hungary was represented at the first and second formal meetings of the Open-ended Working Group by its Permanent Representative to the Organization for Security and Cooperation in Europe (OSCE) (also Chair of the OSCE Informal Working Group on Cyber Security) and by the Coordinator for Cyber Issues of the Ministry of Foreign Affairs and Trade, respectively. Hungary also actively participates in the consultations concerning the draft report of the Chair of the Open-ended Working Group. In general, Hungary aligns itself with the position of the European Union.

Hungary strongly supports an effective multilateral system, underpinned by a rules-based international order, which delivers results in tackling global challenges in cyberspace. Our participation in and support for different intergovernmental and multi-stakeholder initiatives is a good example of this. Hungary reiterates the applicability of existing international law to State conduct in cyberspace, as recognized in the Group of Governmental Experts consensus reports from 2010, 2013 and 2015. However, non-compliance with international law obligations by State and non-State actors still constitutes a major threat to international peace and security and

to our national sovereignty, both in the physical world and in cyberspace. Therefore, we need to be able to deter and prevent both conventional and unconventional attacks.

Support for the Agenda for Disarmament

Hungary shares the concerns expressed by the Secretary-General over the increasing malicious use of ICTs and, therefore, supports the promotion of a peaceful ICT environment as a key priority laid down in the Agenda for Disarmament announced by the Secretary-General in May 2018. As a recognition of the high level of our engagement, Hungary has been identified by the United Nations Office for Disarmament Affairs as a supporter of action 31 of the Agenda, aimed at fostering accountability and adherence to emerging norms in cyberspace.

Hungary supports the good offices of the Secretary-General to prevent the escalation of cyberincidents and the operationalization of voluntary cybernorms, as well as further collaboration aimed at closing the cyberknowledge gap among Member States.

Cybersecurity as a matter of national security

In April 2020, the Government adopted Hungary's new National Security Strategy (attached to Government Decision 1163/2020 (IV. 21.)), based upon which our existing National Cybersecurity Strategy needs to be subject to a review. The new National Security Strategy provides an overview of the changes in the security threat landscape in the period since 2012. One of its primary objectives is to identify, to address and to respond to the security challenges posed by the rapid development of information and communications technologies.

It is widely expected that the number and sophistication of cyberattacks will keep growing. Therefore, the Government of Hungary, in cooperation with other stakeholders, will do everything in its power to strengthen its capacities in order to guard against malicious cyberattacks targeting our critical information infrastructure and to further increase public awareness of cyberhygiene.

Addressing the challenges caused by the spread of misinformation and disinformation both online and offline is a key priority, especially today, as we continue our fight against the coronavirus disease (COVID-19) pandemic. In a national emergency, fake information can be particularly damaging.

The development of offensive and defensive cybercapabilities must be consistent with a State's obligations under international law. Otherwise, the use of offensive ICT capabilities can contribute to the militarization of the digital space.

In our view, cybercapabilities capable of threatening national security and stability are considered to be weapons, the use of which can reach the threshold of an armed attack to which States can also react with kinetic response as a means of self-defence. Considering the challenges of attribution in the ICT environment, public authorities, in the case of an ICT incident, should act with due diligence and consider all relevant information, including the larger context of the event and the nature and extent of the consequences.

International cooperation and other multi-stakeholder initiatives

As a member of the European Union, Hungary is actively involved in the development of the European Union's own cyberdiplomacy toolbox in order for the European Union to able to coordinate its response to malicious cyberactivities against its institutions and its member States originating from outside of the European Union. Emphasizing the importance of international cooperation, we support an enhanced dialogue with our strategic partners, allies and other international organizations.

No single country or organization may be successful in tackling contemporary security threats alone. This makes partnerships, in particular European Union-North Atlantic Treaty Organization (NATO) cooperation more important today than ever before. There is no alternative but to continue and further deepen this cooperation in the forthcoming years. Countering hybrid threats (including cybersecurity threats) is certainly one of the main areas where the two organizations should focus their efforts.

It is expected that conflict in cyberspace will further intensify in the years to come and the capacity gap between technologically advanced and developing countries will further expand. In July 2016, the allies reaffirmed the defensive NATO mandate and recognized cyberspace as an operational domain which NATO must defend. In July 2018, the allies once again declared the readiness of NATO to continue to adapt to the evolving cyberthreat landscape, which is affected by both State and non-State actors, including State-sponsored actors. NATO member States agreed to integrate sovereign cybereffects, provided voluntarily by allies, in the framework of strong political oversight. Reaffirming the alliance's defensive mandate, NATO declared it was determined to employ a full range of capabilities, including cybercapabilities, to deter, defend against and counter the full spectrum of cyberthreats. NATO is committed to further developing its partnership with industry and academia from all allies to keep pace with technological advances through innovation.

The commitment of Hungary to cybersecurity is not new. The first and still the only international agreement on countering cybercrime, called the Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention, was agreed in Budapest in 2001 and, ever since, has served as a guideline to develop comprehensive national legislation against cybercrime and as a framework for international cooperation. The treaty was ratified by Act LXXIX of 2004. In addition to being a party to the Budapest Convention, Hungary is actively promoting the accession of third countries to it.

As a national contribution, since 2017, the Permanent Representative of Hungary has been acting as the Chairperson of the OSCE Informal Working Group established by Permanent Council decision 1039 on the development of confidence-building measures to reduce the risks of conflict stemming from the use of ICTs. Hungary supports the efforts aimed at closer cooperation between United Nations processes and other relevant regional organizations, such as OSCE. Regionally, we underline the importance of the implementation of the set of confidence-building measures adopted by OSCE. We are also in favour of elaborating on the globalization of regional confidence-building measures in the context of the Open-ended Working Group. However, our focus should be to operationalize each and every regional confidence-building measure at the same level of effectiveness.

Hungary is one of the few countries with staff dedicated to cyberdiplomacy. The Coordinator for Cyber Issues of the Ministry of Foreign Affairs and Trade is responsible for international outreach activities on cyberspace issues both in bilateral and multilateral relations, including the United Nations, the European Union, OSCE and other relevant multi-stakeholder initiatives, such as the Global Forum on Cyber Expertise. Cyberdiplomacy is a relatively new field of our international cooperation that our Government can benefit from while addressing malicious cyberactivities.

Hungary contributes to capacity-building efforts in third countries. As part of these efforts, cybersecurity also plays an integral role in Hungary's international development cooperation policy, especially vis-á-vis African partner countries. To this end, Hungary has been providing development assistance to Uganda in the field of information technology security with the aim of helping Uganda to face twenty-first century challenges. The area of cybersecurity is a key element of cooperation

laid down in Hungary's recently adopted Africa Strategy and its International Development Cooperation Strategy for the period 2020–2025.

In addition to being part of different intergovernmental negotiations, the Hungarian Government is a supporter of multi-stakeholder initiatives, such as the Paris Call for Trust and Security in Cyberspace, answering the call for more in-depth cooperation on the development of norms, rules and principles of State behaviour in cyberspace. Our Government was joined by dozens of Hungarian private sectors organizations in these efforts. Hungary is also a supporter of the Christchurch Call to eliminate terrorist and violent extremist content online, which have adverse impacts on human rights and on our collective security.

Hungary shares the view that that non-governmental organizations (civil society, academia, the private sector and the ICT community) have a range of technical expertise and/or the necessary resources to contribute to the development of a safe and sustainable cyberspace in their own respective roles and responsibilities. States have the leading role in promoting this coordination and collaboration.

Indonesia

[Original: English]
[31 May 2020]

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

Indonesia has more than 170 million Internet users, accounting for 65 per cent of its total population. Information and communications technologies (ICTs) have provided opportunities for Indonesia that are vital to the attainment of Sustainable Development Goals. On the other hand, challenges in cyberspace are also on the rise. In 2019, Indonesia experienced more than 220 million cyberattacks, hampering the beneficial use of cyberspace.

Indonesia is pursuing multiple measures actively to both maximize digital potential and tackle cyberthreats through the strengthening of legal and policy aspects of institutional infrastructure, capacity-building and international cooperation.

National efforts

In 2017, the National Cyber and Crypto Agency was established as Indonesia's centralized body on cybersecurity affairs. The national Computer Emergency Response Team is set up under the Agency for rapid response on cyberincidents, directed at government or private infrastructures. A computer security incident response team has also been established in each central and district government agency in 34 provinces of Indonesia, to tackle and recover from cyberincidents.

In strengthening the national legal and policy framework, Indonesia promulgated the Law on Information and Electronic Transactions as well as the National eCommerce Roadmap for 2017–2019, which includes efforts to secure electronic and digital transactions. Indonesia's Cyber Defence Guidelines were adopted through Ministry of Defence Regulation No. 82 of 2014. Indonesia's national standardization system has also adopted international standards for ICT security, namely ISO/IEC27001 and ISO 15408.

Indonesia's cybersecurity law has been set as a priority bill of 2020, and the legislative process is currently ongoing. Indonesia is also currently drafting the national cybersecurity strategy 2020–2024, which covers five pillars: cyberresilience, the strengthening of the legal framework, cybertechnology capability, the supporting of digital economic growth, and national and international cooperation.

Indonesia is also committed to continuing to strengthen domestic cooperation, particularly with State-owned enterprises, the private sector and industry to support the creation of an inclusive cybersecurity culture. Since 2018, the Government of Indonesia initiated the Cyber Security Literacy Campaign to promote secure Internet access, the campaign against hoaxes and cyberbullying, social media ethics, responsible usership and guidance to parents for children's Internet safety.

International efforts

Through its multiple undertakings, Indonesia continues to advance mutual cooperation, best practices and capacities to help enable an effective edifice on cybersecurity that could ultimately be adopted universally.

In terms of global multilateral engagement, Indonesia is actively engaged in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, including in its capacity as the Coordinator of the Working Group on Disarmament of the Movement of Non-Aligned Countries. Indonesia is also currently among the 25 members the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Regionally, Indonesia takes part in confidence-building measures in the Association of Southeast Asian Nations (ASEAN) framework, among others, by supporting the establishment of points of contact in ASEAN sectoral bodies dealing with cyberissues under its political-security and economic community pillars, as well as through information exchange, regular cybersecurity collaboration and member States' dialogues. ASEAN also strengthens its cooperation on cybersecurity issues by establishing a cross-pillar coordination committee. Through the ASEAN Regional Forum, the discussion on confidence-building measures in the context of cybersecurity has expanded beyond ASEAN to also involve other countries and partners.

Further, Indonesia maintains bilateral dialogues and cooperation with various States and partners. Indonesia will continue to meaningfully advance efforts in strengthening responsible State behaviour as well as the promotion of an open, secure, stable, accessible and peaceful ICT environment.

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

The misuse of cyberspace by both State and non-State actors, including proxies, poses risks to international peace and security as well as the stability of national political, economic and social domains. A great shift to ICT is also currently taking place internationally in coping with the multidimensional implications of the coronavirus disease (COVID-19) pandemic. Malicious cyberactors might attempt to exploit, in particular, the ICT systems and the spread of information in cyberspace.

Mutual understanding, cooperation, collaboration, confidence-building measures, assistance and capacity-building are essential to strengthening security and stability in cyberspace. Bilateral, regional and global efforts, in this respect, must all be supported and seen as complementary, not competing.

Indonesia supports the continued discussion and implementation of non-binding norms in accordance with the Group of Governmental Experts report of 2015. Indonesia reiterates the vital role played by the United Nations and regional organizations in promoting the discussion and implementation of 11 norms, confidence-building measures and capacities on cybersecurity, especially in narrowing and closing the digital gap between countries.

Indonesia is of the view that voluntary and non-binding norms serve as an important framework for responsible State behaviour. While the gap on ungoverned cyberspace issues needs to be addressed, Indonesia encourages the creation of further State and customary practices.

Indonesia is open to discussing the application of existing international law in cyberspace, including the possibility of *lex specialis*. Indonesia stresses that the use of cyberspace should be carried out in accordance with international legal principles, especially those related to full respect for sovereignty, non-intervention, peaceful settlement of disputes, human rights and the Charter of the United Nations.

Indonesia supports a declaration by all States in the General Assembly to refrain from the militarization of cyberspace, which undermines international peace and security and is contrary to States' rights and obligations under international law.

Indonesia emphasizes the widening of understanding and the deepening of engagement, in particular for those countries and regions that have not partaken adequately in cybersecurity discourse and measures.

Ireland

[Original: English]
[30 May 2020]

Ireland welcomes this opportunity to respond to the request by the Secretary-General pursuant to paragraph 2 of resolution 74/28 on advancing responsible State behaviour in cyberspace in the context of international security. Ireland also supports the submission from the European Union.

Information and communications technologies (ICTs) have benefited our societies and States, facilitating communication, education, innovation and economic activity, and promoting prosperity. But in an increasingly interconnected world, the abuse of these powerful technologies can also have a very adverse impact, and the rise in malicious cyberactivity, including during the current pandemic, is of major concern to Ireland. This activity affects citizens, and their trust and confidence in institutions. Its effects are also felt at the level of societies and States, where it can cause or escalate conflict.

The United Nations remains the pre-eminent forum to address the challenges related to the misuse of ICTs and malicious cyberactivity, which have an impact on all three pillars of the United Nations agenda: peace and security, human rights and sustainable development. As an economy with an important ICT sector, and as a country with a deeply held commitment to the United Nations, Ireland will continue to support the United Nations in promoting and advancing responsible State behaviour in cyberspace. Ireland will also continue to engage proactively and collaboratively with partners at the United Nations and internationally to support an open, free, safe and secure cyberspace, to promote freedom of expression, association and assembly online, to reduce the risk of conflict and to promote peace, and to ensure that the social and economic benefits of cyberspace are accessible to all, including in support of the Sustainable Development Goals. We believe that progress in tackling the challenges faced can only be sustained through multilateral and multi-stakeholder engagement, which we are committed to nationally through initiatives, including the Cyber Ireland cluster that was established in 2019 with government funding and which brings together multiple stakeholders from industry, academia and government to discuss and promote cooperation and awareness-raising on cyberrelated education and career opportunities, and to promote innovation in Ireland's cybersecurity sector. We also extend this commitment to our international approach and, in this regard, welcome initiatives at the United Nations and in other forums to promote broader

cooperation and dialogue, including through the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Ireland also supports the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.

Ireland's approach to cyberissues remains grounded in our commitment to the applicability and centrality of international law, including the Charter of the United Nations, international humanitarian law, and international human rights law. Ireland also welcomes the consensus reached by the General Assembly in 2015 that all States should be guided in their use of ICTs by the 2015 Group of Governmental Experts report, which delineated 11 voluntary and non-binding norms of responsible State behaviour. We consider that these norms, combined with international law, complemented by capacity-building measures to build cyberresilience and to facilitate greater access to ICTs, and confidence-building measures aimed at reducing the risk of armed conflict, provide a strong framework to advance positive State behaviour in cyberspace. ICT capacity-building initiatives can also help address the continuing global digital divide, transforming the lives of people and communities and promoting prosperity, contributing to and facilitating the implementation of the Sustainable Development Goals, including in areas of gender.

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

Ireland's National Cyber Security Strategy 2019–2024

In an interconnected cyberspace, all States must ensure that they build resilience against cyberrelated risks, both domestically and globally. Ireland's National Cyber Security Strategy 2019–2024[8] sets out key actions and objectives in this regard. The Strategy supports the United Nations goal of promoting responsible State behaviour in cyberspace and sustaining international peace and security by protecting Ireland, its people and its critical national infrastructure from cybersecurity threats. It also underpins Ireland's international engagement to support a free, open, peaceful and secure cyberspace. Ireland's cybersecurity policy is implemented by the National Cybersecurity Centre, which contributes to the United Nations cyberagenda by promoting dialogue on cyberissues and collaborating with partner agencies and other stakeholders internationally, promoting trust and security in cyberspace.

The key objectives of Ireland's Cyber Security Strategy include:

- To continue to improve Ireland's ability to detect, respond to and manage cybersecurity incidents
- To identify and protect critical national infrastructure by increasing resilience to cyberattacks
- To improve the resilience and security of public sector information technology systems to better protect services that citizens rely upon, and their data
- To invest in educational initiatives to prepare the workforce for advanced information technology and cybersecurity careers
- To raise awareness of the responsibilities of businesses around securing their networks, devices and information and to drive research and development in cybersecurity in Ireland, including by facilitating investment in new technology

[8] Available at www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.

- To continue to engage with international partners and international organizations to ensure that cyberspace remains open, secure, unitary and free and able to facilitate economic and social development and to support sustainable capacity-building
- To increase the general level of skills and awareness among private individuals around basic cyberhygiene practices and to support them in this through information and training

White Paper on Defence

Ireland's *White Paper on Defence* (published in 2015[9] and updated in 2019[10]) notes the dangers posed by malicious cyberactivity domestically and internationally, including to critical infrastructure and key services, and also recognizes how cyberissues can be misused to undermine core values, including human dignity, freedom and democracy. The *White Paper on Defence* and the National Cyber Security Strategy continue to inform Ireland's engagement on ICTs and cyberissues.

Bilateral, regional and multilateral approaches

Ireland continues to promote dialogue on ICT and cyberissues in its engagement with other States at the bilateral level and in regional and multilateral forums.

Ireland welcomes the work of the Organization for Security and Cooperation in Europe (OSCE) and other regional organizations around the world in promoting trust- and confidence-building measures.

Ireland supports State and non-State initiatives that promote trust, security and peace in cyberspace, including the Paris Call for Trust and Security in Cyberspace. Ireland also supports the Christchurch Call to eliminate terrorist and violent extremist content online. Ireland is a member of the Freedom Online Coalition of 31 States who work together to advance Internet freedom.

Ireland has also submitted a letter of intent seeking to join the Cooperative Cyber Defence Centre of Excellence in Tallinn, to contribute to collaboratively tackling cybersecurity challenges with like-minded partners. Ireland will join the Centre as a Contributing Participant (as a non-NATO member).

Promoting international cooperation at the European Union

Ireland continues to play a full and proactive role in the European Union on cyberissues and works closely with its European Union partners to promote a globally open, free, stable and secure cyberspace which contributes to conflict prevention, including through cyberdiplomacy initiatives and the European Union cyberdiplomacy toolbox. In the development of its cyberresilience capabilities, Ireland also participates in a number of European Defence Agency initiatives.

Promoting international cooperation at the United Nations

At United Nations level, Ireland supports the work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (see also below), and has actively contributed to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Ireland's Ambassador to the United Nations also spoke at the Arria-formula meeting of the Security Council on cyberstability, conflict prevention and capacity-

[9] Available at https://assets.gov.ie/21963/f1e7723dd1764a4281692f3f7cb96966.pdf.
[10] Available at www.gov.ie/en/publication/a519cf-white-paper-on-defence-update-2019/.

building, held on 22 May 2020, underlining Ireland's commitment to work with the United Nations on the broad range of activity in this area, including by using ICTs and cyberspace to deliver the Sustainable Development Goals, with particular reference to the Goal on gender.

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

General principles

Ireland supports a technology-neutral and multilateral approach to promoting global cybersecurity, underpinned by a rules-based international order. Ireland considers that discussions at recent meetings of the Open-ended Working Group have been enriched by the engagement and contributions of stakeholders (including civil society, academia, and technical and industry representatives). These stakeholders will play an increasingly critical role in advising States on future developments in the ICT domain and in directly maintaining a safe and stable cyberspace. Ireland believes that enhanced participation by stakeholders in future meetings and other discussions on cyberissues is valuable and necessary and should be formalized.

Existing and emerging threats

Ireland's National Cyber Security Strategy acknowledges the growing and positive impact of ICTs on economic and social development, but also highlights the rise of cybercrime, of the theft of intellectual property and the spread of disinformation, as well as of the use of offensive cybercapabilities by States. The coronavirus disease (COVID-19) pandemic has demonstrated our reliance on ICTs to work and communicate flexibly and securely and to sustain economic activity. However, the pandemic has also highlighted the activities of malicious actors who exploit vulnerabilities, both technical and human, to commit cybercrime, or to spread disinformation, sowing confusion, distrust and division. Ireland notes with particular concern recent cyberattacks against health, medical and related services. Such attacks against health care and other essential services endanger lives. With its European Union partners, Ireland has condemned them and called upon every State to exercise due diligence and take appropriate action against actors conducting such activities from its territory, consistent with international law and the 2010, 2013 and 2015 consensus reports of the Group of Governmental Experts.

International law

Ireland believes strongly in the applicability and centrality of international law, including the Charter of the United Nations, international humanitarian law and international human rights law, to cyberspace. Human rights and fundamental freedoms must be respected online as well as offline. Given the existing international legal framework, Ireland has outlined its reservations, including at recent meetings of the Open-ended Working Group, around calls for the drafting of a new legal instrument. However, Ireland welcomes ongoing dialogue to promote greater shared understanding on the application of existing international law to the use of ICTs by States.

Norms, rules and principles for the responsible behaviour of States

Ireland supports the voluntary and non-binding norms, rules and principles for responsible State behaviour in the 2015 Group of Governmental Experts report and welcomes the agreement by consensus by the General Assembly that all States should be guided in their use of ICTs by the report. These norms promote stability and security in the global ICT environment and can contribute to maintaining

international peace. Ireland's National Cyber Security Strategy and Irish policy reflect these norms, rules and principles, including in relation to sustainable capacity-building. Ireland has called, at the United Nations, for the further elaboration of guidance on how these existing norms, endorsed by consensus by all Member States, could be practically implemented and operationalized.

Confidence-building measures

Ireland proactively contributes to and promotes discussions on ICTs and cybersecurity issues at bilateral, regional and multilateral meetings and forums, including in the context of global peace and security, sustainable development and human rights. Ireland recognizes the extensive work undertaken by regional organizations and State and non-State stakeholder initiatives, including the Paris Call, in promoting trust and confidence, and broadly supports proposals to establish mechanisms to share best practices on confidence-building measures to support future initiatives.

Capacity-building measures

Ireland's National Cyber Security Strategy includes a commitment to further sustainable capacity-building measures. Ireland also values a multilateral and multi-stakeholder approach to building the resilience of all States against malicious cyberactivity and to reducing vulnerabilities, protecting critical infrastructure and extending the full benefits of access to ICTs to all States. Ireland also believes that it is critical that all States and key stakeholders have the ability to take part in global discussions on cyberissues. In this regard, Ireland was pleased to sponsor the informal intersessional meeting of the Open-ended Working Group from 2 to 4 December 2019, which brought States together with stakeholders, including representatives of non-governmental organizations and civil society, technical experts, researchers and academics, and the private sector. Ireland also strongly supports efforts to tackle the gender digital divide. Ireland would welcome stronger linkages between future United Nations capacity-building discussions and initiatives and the Sustainable Development Goals and the women and peace and security agenda.

Italy

[Original: English]
[29 May 2020]

Introduction

Italy aligns itself with the positions expressed by the European Union in its contribution to the report and would like to provide the Secretary-General with the following national information.

For the purposes of the present report, Italy will not consider the expression "information security", which is not in use in the Italian legal system. Other expressions, such as "cybersecurity" or "networks and information systems security", are employed and therefore preferable. Freedom of expression – online as well as offline – is recognized by Italian fundamental law and by article 19 of the International Covenant on Civil and Political Rights, ratified by Italy in 1978.

According to the Italian Prime Ministerial Decree of 17 February 2017, which contains guidelines for national cyberspace protection and information and communications technology security, the term "cybersecurity" refers to cyberspace protection ensured through adequate physical, logical and procedural security measures with the aim of preventing and countering events, whether intentional or accidental, involving undue acquisition and transfer of data, modification or

illegitimate destruction of data, or undue control, damage, destruction or blockage of the regular functioning of networks and information systems or their components.

Likewise, the expression “networks and information systems security” refers to the ability of a network or information system to resist, at a certain level of confidentiality, any action targeting the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed and of related services available or accessible through that network or information system, as defined in Legislative Decree 65/2018 transposing the European Union Directive on security of network and information systems.

Efforts taken at the national level to strengthen cybersecurity: the institutional and normative framework

In December 2013, Italy adopted the National Strategic Framework for cyberspace security, which takes note of the increasing and evolving threats posed by the use of information and communications technology (ICT) and aims at enhancing Italy’s cybercapabilities and resilience. The following national action plans, the latest issued in March 2017 and adopted in line with the above-mentioned Prime Ministerial Decree of 17 February 2017, identify a number of actions, items and priorities to implement the Strategic Framework.

The Prime Ministerial Decree defines the national cybersecurity architecture and its governance, establishing within the Security Intelligence Department, a Cyber Security Management Board, which is responsible for preventing and preparing for a national cybercrisis, as well as for coordinating the response and recovery activities to be carried out by public and private sectors in compliance with the Prime Minister’s decisions.

The Cyber Security Management Board consists of a Secretariat and of a joint board chaired by the Deputy Director General for Cyber of the Security Intelligence Department and composed of representatives of the intelligence community (the Security Intelligence Department, the External Intelligence and Security Agency and the Internal Information and Security Agency), the Prime Minister’s Military Advisor, the Ministries of Foreign Affairs and International Cooperation, Internal Affairs, Justice, Defence, Economy and Finance, and Economic Development, the Department of Civil Protection and the Agency for Digital Italy. A representative of the Security Intelligence Department’s Central Office for Secrecy joins the Board whenever an event compromising classified information systems is under discussion.

In the case of a national cybercrisis, the Board may also include representatives from the Ministry of Health, the Ministry of Infrastructure and Transport, and the Fire Department. The Prime Minister, on the basis of the information provided by the NSC, can declare a situation of cybercrisis whenever a cyberevent, on account of its scale, intensity or nature, cannot be dealt with by the single office concerned but requires a joint and coordinated approach, which is ensured by the Cyber Security Management Board.

Additional pieces of legislation followed the Prime Ministerial Decree, namely:

- Legislative Decree 65/2018, which transposes the European Union Directive on the security of network and information systems and appoints the Security Intelligence Department as the single point of contact for network and information systems
- National Cyber Security Perimeter (Law 133/2019), which entered into force in November 2019, applies to national public and private entities performing essential functions or providing essential services for the implementation of activities deemed vital for Italian national interests. Public and private entities

are included in the “perimeter” according to the principle of “progressive priority for national security”. The law covers those networks, IT systems and services owned or operated by the above-mentioned entities, which could affect national security. The law entails the following:

– Incident notification, in order to ensure an immediate information flow towards the relevant structures responsible for prevention, preparation and management of cyberevents, namely the Cybersecurity Management Board and the Computer Security Incident Response Team which are both part of the Security Intelligence Department

– Security measures covering organizational issues, processes, and procedures, including ICT procurement

– Technological screening of ICT products and services that fall into specific categories and are related to assets/entities included in the perimeter. According to the law, any operator wishing to purchase those items shall inform the National Centre for Evaluation and Certification which, in turn, may perform preliminary assessments, impose conditions and require hardware or software testing. In the latter case, the related calls for tender and contracts shall include a clause suspending cancellation policies, related to the requirements to be met or to the positive results of the tests prescribed by the National Centre for Evaluation and Certification

– Inspection and sanctioning activities for public and private actors to be carried out respectively by the Presidency of the Council of Ministers and the Minister of Economic Development.

Should a severe and imminent risk for national security related to networks, information technology systems and services occur, the Prime Minister may instruct that one or more devices or products installed on networks or systems or related to services delivery be partially or totally shut down/suspended. The decision is subject to prior deliberation of the Interministerial Committee for the Security of the Republic and is valid for the time strictly necessary to eliminate or mitigate the threat, according to the principle of proportionality.

• Decree Law 22/2019 converted into Law 41/2019 (article 1), which complements the “Golden Power” Decree Law 21/2012 converted into Law 56/2012 “on special powers on shareholding in defence and national security sectors, as well as for strategically relevant activities in the energy, transport and communications sectors”, includes broadband electronic communication services based on 5G technologies among the activities strategically relevant for national defence and security. According to the latest provisions, contracts or agreements on the acquisition of goods or services for planning, execution, maintenance and management of networks related to broadband electronic communication services based on 5G technologies, or the acquisition of “high-intensity technology components” useful for the above-mentioned execution or management are subject to notification to the “Golden Power” Board established within the Presidency of the Council of Ministers whenever they involve non-European Union entities. The rationale behind this is to allow the exercise of veto power or to impose specific prescriptions and conditions, which can be modified or combined with additional measures, including the replacement of products and equipment, if the National Centre for Evaluation and Certification detects the presence of vulnerabilities which can compromise the integrity and security of networks and their data.

Cyberdefence

The 2015 White Paper for International Security and Defence recognizes the need to protect and defend the cyberdomain, including through the establishment of "specific defensive operational capabilities… in order to preserve the solidity of political, economic and social structures". According to the Ministry of Defence Multi-Year Planning Document for the years 2019–2021, cyberspace must be protected and defended from attacks on network or computer services and critical infrastructure. In recent years, the Ministry of Defence has undergone a number of reforms to reinforce its protection as well its resilience and posture.

Inter alia, the Italian Ministry of Defence in 2017 established the Joint Cyber Operations Command, a military command responsible for planning, conducting and carrying out cyberoperations, with the aim to detect and neutralize threats and attacks on the Ministry of Defence networks, systems and services within the country as well as in theatres of operations outside the Italian borders.

The Joint Cyber Operations Command has been recently integrated into the newly established Cyber Component Command), with the aim to develop a more direct chain of command and ensure more efficiency and coordination among all relevant cybersecurity departments in place within the defence sectors (Air Force, Army and Navy). The Cyber Component Command supports the Italian Joint Operations Headquarters), and it is tasked with conducting defensive operations to protect the Italian Ministry of Defence and its military apparatus from cyberincidents and attacks.

In addition, the Cyber Component Command is:

- Responsible for the cybersecurity and cyberdefence of the Ministry of Defence's networks, which it ensures through the Computer Emergency Response Team, which is in charge of monitoring cyberactivity and preventing and managing incidents and emergencies affecting the defence sector;
- Currently carrying out a study to define the legal framework in operational theatres, in full compliance with international law and international humanitarian law. Such a study will aim to define minimum standards and rules of engagement to support the operations through activities carried out in cyberspace. The need for a legal framework comes inter alia from the numerous national and international activities and exercises carried out in the last years, including within the framework of the North Atlantic Treaty Organization (NATO).

A Cyber Lab has been established within the Joint Cyber Command with the aim of developing tools to investigate cybervulnerabilities and organize training activities.

Other activities include preliminary testing to establish a cyberrange for technical cybertraining at the Italian Armed Forces Schools of Telecommunications) and collaboration with many Italian universities in the field of cybersecurity.

Efforts taken to promote international cooperation in the cybersecurity field, including with regard to the reports of the Group of Governmental Experts

According to article 10 of the Italian Constitution, "the Italian legal system conforms to the generally recognised rules of international law".

Italy is therefore committed to promoting the application of existing international law in cyberspace, including the Charter of the United Nations in its entirety, also in accordance with the European Union position as per the above-

mentioned contribution; adherence to the rules, norms and principles of responsible State behaviour established by the 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and previous groups; the development of confidence-building measures and capacity-building programmes; and Internet governance based on a multi-stakeholder approach.

Italy supports the Paris Call for Trust and Security in Cyberspace regarding the implementation of cooperative measures to reduce risks to the stability of cyberspace and to build confidence, capacity and trust. Italy is also one of the signatories of the Christchurch Call to eliminate terrorist and violent extremism content online.

The promotion of capacity-building activities with third countries is part of our national cybersecurity strategy and is carried out in compliance with the "Council conclusions on EU External Capacity Building Guidelines", adopted by the General Affairs Council of the European Union at its 3629th meeting held on 26 June 2018. Capacity-building activities with third countries mainly focus on sharing information and best practices, especially with regard to computer security incident response, and education and training.

Participating in international forums and supporting the adherence to norms of responsible State behaviour in cyberspace are also an essential part of the Italian national cybersecurity strategy. International cooperation in the cybersecurity field, including with regard to the reports of the Group of Governmental Experts, is also discussed, where relevant, in our bilateral and multilateral dialogues and/or consultations. The main multilateral forums in which Italy actively contributes to enhance cooperation in cyberspace are the United Nations, the European Union, NATO, the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe and the Group of Seven.

With regard to the latter, on 10 and 11 April 2017 Italy hosted the Group of Seven Ministerial Meeting on Foreign Affairs that adopted the "G7 Declaration on responsible States behaviour in cyberspace". The Declaration calls upon all States to be guided in their use of ICT by the cumulative reports of the United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security.

During the Italian Chairmanship of the OSCE in 2018, Italy actively supported the actual implementation of the OSCE confidence-building measures in the field of information and communication security by participating States, inter alia by organising a scenario-based discussion on their use in the case of an international cyberincident, on the margins of the 2018 OSCE-wide Conference on Cyber/ICT Security, held in Rome on 27 and 28 September 2018. In 2019, Italy, during its Chairmanship of the OSCE Asian Contact Group, organized the twentieth Asian OSCE Conference, on "How to achieve comprehensive security in the digital era: the perspectives of the OSCE and its Asian Partners", held in Tokyo on 2 and 3 September 2019. Italy also supported a number of OSCE projects on capacity-building in the field of cyber/ICT, such as the "Sub-regional Training on the role of Information and Communication Technologies (ICTs) in the context of regional and international security" held in Athens on 7 and 8 February 2019.

Italy actively participates in the activities of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and supports the work carried out by the current Group of Governmental Experts and by previous groups. Italy also recalls that General Assembly resolution 70/237 welcomes the conclusions of previous groups of governmental experts in their 2013 and 2015 reports and calls upon Member States

to be guided by the 2015 report in their use of information and communications technologies.

The recent establishment of a department dealing with cybersecurity and cyberpolicies within the Italian Ministry of Foreign Affairs and International Cooperation aims at further strengthening and promoting our diplomatic action and international cooperation in this field.

Japan

[Original: English]
[31 May 2020]

Japan welcomes the opportunity to respond to General Assembly resolution 74/28 on advancing responsible State behaviour in cyberspace in the context of international security.

1. 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. The Government has also adopted a policy of realizing a human-centred society that achieves both economic development and the resolution of social issues through a high level of integration of cyberspace with real space. Under these circumstances, 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 providing 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. Especially, the outbreak of coronavirus disease (COVID-19) seems to be accelerating the trend of mankind's increased reliance on information and communications technology (ICT) while accentuating the risks and the problems caused by malicious use of ICT. There is growing concern over reports of cyberattacks and malicious cyberactivities which take advantage of the crisis, including ransomware striking medical institutions and authorities, as well as distributed denial of service attacks against medical research facilities. 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 has 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, and mindful of the desired state of affairs in 2020 and beyond, Japan will spare no effort regarding cybersecurity measures by clarifying its 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 cyber-related issues. The Government will also share expertise with foreign countries, promote specific cooperation and collaboration, and take action whenever necessary. Furthermore, the Government will actively participate in international discussions to address cybersecurity-related issues which have surfaced under the outbreak of COVID-19.

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 and strategies and systems for responding, 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 the same basic principles on cybersecurity.

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 cyber drills. Furthermore, the Government will respond appropriately in the case of incidents through appropriate international collaboration.

In the light of the diplomatic aspects of cyber-related 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 for Japan's national security. Japan takes the position 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 (INTERPOL).

Japan will work to build confidence among States in order to prevent the occurrence of cyberattacks. Due to the anonymity and secrecy of cyberattacks, there are risks that they could unintentionally increase tensions among States. 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 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 Asian Nations (ASEAN) Regional Forum inter-sessional 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, capacity-building 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 the first Asian country to have ratified 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.

2. 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 of malicious cyber acts

To flexibly incorporate the rapid development of ICT into our lives, and to prevent the damage stemming from malicious cyber acts, 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 cyber acts 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 cooperation for relevant confidence-building measures and capacity-building

To further enhance each nation's efforts 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 desire to eliminate security holes in cyberspace and prevent profit-making from malicious cyber acts. In this context, the Group members should consistently encourage all States to steadily implement the voluntary, non-binding norms of responsible State behaviour, including confidence-building measures, and

cooperate in supporting national capacity-building efforts in order to implement the above-mentioned norms and recommendations, including through the process of the next Group of Governmental Experts and the Open-ended Working Group.

Mexico

[Original: Spanish]
[29 May 2020]

Information technologies and new developments in telecommunications have expanded the range of possibilities for sustainable development and for the achievement of a world based on rights, equity and inclusion. The entire international community has an obligation to ensure the peaceful use of those technologies for the common good.

The discussions at the United Nations on stability in cyberspace, cybersecurity and cyberspace governance, in particular the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security on advancing responsible State behaviour in cyberspace, lay the foundation for progress towards an open, free, stable and secure cyberspace.

In line with those precedents, the Government of Mexico is submitting the present report with the understanding that the resolutions adopted by the General Assembly are valuable and that only a multilateral approach can ensure, in the long term, the legitimate and peaceful uses of cyberspace, resilience in the digital environment, the potential of information technologies as enablers of sustainable development, and the protection of human rights in cyberspace.

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

The Government of Mexico has established the following national coordination mechanisms and response bodies focusing on information security:

(a) Specialized Committee on Information Security

An inter-agency collegial body responsible for developing information security policies applicable to national security institutions and for ensuring their proper implementation. Federal bodies in Mexico focusing on national security, public security, telecommunications, the financial sector and foreign policy are represented on this committee. Examples of initiatives that have been taken by the committee include the design and updating of the national cybersecurity strategy, computer security incident response exercises and awareness-raising activities related to information security.

(b) National Cybersecurity Incident Response Centre

This body, which is under the responsibility of the newly established National Guard of Mexico, is responsible for monitoring the integrity of the country’s strategic technological infrastructure. The Centre has units which specialize in the prevention and investigation of illicit conduct through the use of computers, monitors networks to identify criminal conduct and carries out activities aimed at reducing and mitigating risks of cybersecurity threats and attacks. It also implements scientific and technological development programs related to cybersecurity.

(c) Sensitive Information Security Incident Response Group

A coordination mechanism designed to respond effectively to information security incidents in the financial sector. The Attorney General's Office, the national financial authorities and financial trade unions in Mexico participate in the mechanism, whose purpose is to respond effectively to incidents which directly affect the financial sector.

At the national level, Mexico has taken the following initiatives to strengthen information security in recent years:

The Government of Mexico, through the Ministry of Security and Civil Protection, hosts an annual National Cybersecurity Week. The purpose of this event is to encourage dialogue on promoting cybersecurity, and to foster partnership among relevant sectors in order to ensure a secure and resilient digital environment. The event is also aimed at raising awareness about information technologies and digital security through conferences, panel discussions, training, workshops, webinars and recreational activities.

Since 2018, the Government of Mexico, in collaboration with the Organization of American States (OAS) and Trend Micro, has hosted an annual event known as Cyberwomen Challenge. This event is aimed at promoting gender equality in activities related to protection against and response to cybersecurity threats, and at strengthening the capacities of relevant institutions.

In 2019, the Ministry of Communications and Transport held cybersecurity working group meetings, with the participation of more than 5,000 people from the Ministry's digital inclusion centres, which are located throughout the country. These meetings focused on identifying risky behaviour in the use of telecommunications and broadcasting services. The information gathered from the meetings served as input for a 2019 report on the cybersecurity habits of users in Mexico.

On the basis of the findings contained in that report, a simulator was developed with the support of OAS and the Government of the United Kingdom. A simulator is a tool which enables users to experience simulated cybersecurity threats in an interactive environment, in order to evaluate their ability to respond to such threats and provide advice on the best protection methods.

In order to help advance international cooperation and the responsible behaviour of States in cyberspace, Mexico participates in the following multilateral and regional forums, mechanisms and initiatives:

(a) First Committee of the United Nations General Assembly

Mexico participates in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, which was established pursuant to General Assembly resolution 73/27.

In addition, a governmental expert from Mexico participates in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, which was established pursuant to General Assembly resolution 73/266.

Mexico has sought to ensure that both bodies operate in a complementary manner, and recognizes that both continue to build on the work of previous groups of governmental experts and on their reports, which were adopted by consensus by the General Assembly.

(b) Group of Friends on Digital Technologies

Mexico attaches great importance to designing and collaborating on activities related to digital technologies, in particular those which support the implementation of the Sustainable Development Goals and targets by promoting the positive use of information and telecommunications technologies. Accordingly, since November 2019 Mexico, together with Finland and Singapore, has served as Co-Chair of the Group of Friends on Digital Technologies, which is aimed at fostering inclusive dialogue with all stakeholders in order to consider the links between digital technologies and sustainable development, and to discuss relevant cross-cutting forms of international cooperation.

(c) High-level Panel on Digital Cooperation of the United Nations Secretary-General

Pursuant to the recommendations of the High-level Panel on Digital Cooperation, Mexico, together with the United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), led a group discussion aimed at identifying specific steps to implement recommendations 1(c) and 1(d), on digital inclusion and related metrics.

(d) International Telecommunication Union

Mexico participates in initiatives related to information security and cybersecurity coordinated by the International Telecommunication Union, such as the Global Cybersecurity Agenda and the Global Cybersecurity Index.

Mexico considers the Global Cybersecurity Agenda to be an important initiative which contributes to the development of a safer and more resilient digital environment, and which is intrinsically valuable in that it provides for the participation of all stakeholders, including States, the private sector, civil society and academia.

(e) Organization of American States

Mexico actively participates in the cybersecurity programme of the OAS Inter-American Committee against Terrorism, which promotes policy development, capacity development, research and outreach in the region.

The National Cybersecurity Incident Response Centre participates in the network of computer security incident response teams of the Americas within the framework of the cybersecurity programme of the OAS Inter-American Committee against Terrorism.

Mexico also participates in the working group on cooperation and confidence-building measures in cyberspace of the OAS Inter-American Committee against Terrorism. As a result of the work of this group, which was established in 2018, the following confidence-building measures were adopted:

- Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks and other documents that each member State considers relevant.
- Identify a national point of contact at the policy level able to discuss the implications of hemispheric cyberthreats.
- Designate points of contact, in the event that none exist, within ministries of foreign affairs, with the purpose of facilitating the work on international cooperation and dialogue in cybersecurity and cyberspace.
- Develop and strengthen capacity-building through activities such as seminars, conferences, workshops on cyberdiplomacy for public and private sector officials.

- Foster the inclusion of subjects related to cybersecurity and cyberspace into training courses for diplomats and officials of ministries of foreign affairs and other government agencies.
- Foster cooperation and the exchange of best practices related to cyberdiplomacy, cybersecurity and cyberspace through the establishment of working groups, other dialogue mechanisms and the signing of agreements among States.

(f) Global Forum on Cyber Expertise

Since 2015, Mexico has participated in this forum, which is dedicated to building cybersecurity capacities. The areas that are of interest to Mexico are the prevention of cyberattacks, data protection, the prevention of cybercrime (including child pornography and similar offences), e-government initiatives and digital strategies, the protection of critical infrastructure, the peaceful uses of information and communications technologies and the Internet, and the applicability of international law to cyberspace.

(g) Forum of Incident Response and Security Teams

The National Cybersecurity Incident Response Centre is a member of the Forum of Incident Response and Security Teams, a global forum which brings together and promotes collaboration among cybersecurity incident response teams from around the world. This makes it possible to develop and strengthen research which, together with the cybersecurity policies of other nations, can be used to identify and locate probable perpetrators of cyberattacks.

2. Content of the concepts mentioned in the reports of the Group of Governmental Experts

In accordance with the statements contained in the previous reports of the Group of Governmental Experts, Mexico believes that international law is applicable to cyberspace. To uphold that principle, the Government of Mexico has taken initiatives at the national level to support its position that applicable international law refers to the Charter of the United Nations, international human rights law, international humanitarian law, applicable norms of customary international law and the related jurisprudence.

In line with the previous reports of the Group of Governmental Experts, Mexico recognizes the potential role and contributions of regional bodies, in particular in the implementation of confidence-building measures. The Government of Mexico has thus encouraged its national bodies to consider implementing the confidence-building measures set forth in the reports of the Group of Governmental Experts and further developed in the work of OAS.

Mexico attaches great importance to the concept of capacity-building emphasized in the reports of the Group of Governmental Experts, as that concept refers not only to the development of national capacities in the area of information security, but also to the need to draw on all forms of international cooperation that have been proven to contribute to international peace and security. Capacity-building ensures that States and all other stakeholders are better equipped to address cybersecurity threats, and fosters a common understanding of issues related to cybersecurity.

During the reporting period, the Government of Mexico has also sought to promote synergies among groups, forums, bodies and initiatives of the United Nations system which focus on issues related to information technologies, telecommunications, cybersecurity, cyberspace governance, digital cooperation and

technological change, in order to improve coherence, avoid duplication of effort and make better use of resources for cooperation.

Singapore

[Original: English]
[27 April 2020]

Singapore is strongly committed to the establishment of an international rules-based order in cyberspace that will serve as a basis for trust and confidence among Member States, and facilitate economic and social progress. To reap the full benefits of digital technologies, the international community must develop a secure, trusted and open cyberspace that is underpinned by applicable international law, well-defined norms of responsible State behaviour, robust confidence-building measures and coordinated capacity-building. It is important that discussions on such laws, rules and norms continue to take place at the United Nations, which is the only universal, inclusive, multilateral forum where all States have an equal voice.

Singapore is a participant in both the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Singapore reiterates that it sees the two platforms as complementary, and will continue to contribute constructively to both processes. For both processes to succeed, their work must be conducted in a spirit of constructive cooperation, consensus, mutual respect, and mutual trust. As a co-Chair of the Group of Friends on e-Governance and Cybersecurity with Estonia, Singapore is committed to engaging all countries to support the work of both processes. Singapore believes that the informal intersessional consultative meeting of the Open-ended Working Group, chaired by the Chief Executive of the Cyber Security Agency of Singapore, David Koh, was useful in facilitating an interactive exchange between Member States, the private sector, civil society, academia and the technical community on a range of substantive issues.

Singapore believes that States need to promote awareness of the existing voluntary, non-binding norms of responsible State behaviour and support their implementation. Singapore supports further elaboration of such norms where needed. For example, supranational critical information infrastructure could be considered a special category of such critical infrastructure, whose protection is the shared responsibility of all Member States, and can be included in the existing set of norms. [11]

Regional organizations can play an important role. The Association of Southeast Asian Nations (ASEAN) reaffirmed the need for a rules-based international order in cyberspace in the first ASEAN leaders' statement on cybersecurity cooperation issued in April 2018. In September 2018, the third ASEAN Ministerial Conference on Cybersecurity decided to subscribe in principle to the 11 norms in the 2015 report of the Governmental Group of Experts, as well as to focus on regional capacity-building in implementing these norms. In October 2019, the fourth ASEAN Ministerial Conference on Cybersecurity decided to establish a working-level committee to consider the development of a long-term regional action plan to ensure effective and practical implementation of the norms including in the areas of cooperation among computer emergency response teams, protection of critical information infrastructure and mutual assistance in cybersecurity.

[11] Supranational critical information infrastructures are those owned by private companies and operating across national borders, but not under any single State's jurisdiction.

Capacity-building is essential to ensure that States develop the ability to successfully implement rules and norms of responsible State behaviour. As part of this effort, Singapore established a S$10 million ASEAN Cyber Capacity Programme in 2016 to support capacity-building in ASEAN on cyberpolicy, strategy, and technical issues. To date, 170 officials from ASEAN member States have been trained under the Programme. As an extension of the ASEAN Cyber Capacity Programme, Singapore launched the S$30 million ASEAN-Singapore Cybersecurity Centre of Excellence in October 2019 to further support cybersecurity policy-making, strategy development, and technical and operational capacity in ASEAN countries, as well as to engage more closely with international partners.

Singapore also co-organised a workshop under the United Nations-Singapore cyber programme to build awareness of cybernorms and policy planning on cyber scenarios in ASEAN member States. In addition, Singapore partnered with the Office for Disarmament Affairs to develop a flagship online training course open to all States Members of the United Nations. The course aims to promote greater understanding of the use of information and communications technologies (ICTs) and their implications for international security. Singapore has also rolled out several training courses on cybersecurity under the Singapore Cooperation Programme. We remain committed to sharing our experience and expertise with States Members of the United Nations, especially small and developing countries.

At the national level, Singapore has continued to strengthen 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*. The Cyber Security Agency of Singapore has developed the Operational Technology Cybersecurity Masterplan as part of Singapore's continuous efforts to enhance the security and resilience of its critical information infrastructure sectors in delivering essential services. The Masterplan serves to improve the cross-sector response to mitigating cyber threats in the operational technology environment and to strengthening partnerships with industry and stakeholders. The Operational Technology Cybersecurity Masterplan outlines key initiatives covering the areas of people, processes and technology to enhance the capacities of our critical information infrastructure owners and organizations that use operational technology systems.

(b) *Creating a safer cyberspace*. As part of efforts to better secure its cyberspace and raise cyber hygiene levels, Singapore will be introducing the Cybersecurity Labelling Scheme in 2020 for network-connected smart devices. The Cybersecurity Labelling Scheme will be launched as a voluntary scheme to allow time for the market and developers to understand how the scheme benefits them. The cybersecurity labels will provide an indication of the level of security embedded in the products. Consumers can choose products with better security ratings using the information on the cybersecurity label. The Cybersecurity Labelling Scheme is aimed at incentivizing manufacturers to develop and provide products with recognized and improved cybersecurity features.

(c) *Developing a vibrant cybersecurity ecosystem*, Singapore recognizes that strengthening cybersecurity involves building up the cyber ecosystem and encouraging innovation within the industry. There is also a growing need to develop a pool of talented individuals who can assume cybersecurity leadership roles in organizations. Since its inception in 2015, the Cyber Security Agency has worked with government agencies, associations, industry partners and institutions of higher learning in Singapore to expand and develop the cybersecurity workforce. The Cyber Security Agency is spearheading a new national SG Cyber Talent initiative to attract

and nurture talented cybersecurity enthusiasts from a young age and to help cybersecurity professionals deepen their skills. SG Cyber Talent aims to reach out to at least 20,000 individuals over three years.

Turkey

[Original: English]
[22 May 2020]

Efforts made at the national level to strengthen information security and promote international cooperation

Information and communications technologies (ICTs) have become an essential part of society and the economy. These technologies are used in a broad network that includes the public and private sectors, critical infrastructure and individuals, and have become widespread in Turkey and 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.

Turkey focuses on taking measures necessary to improve national cybersecurity. The Ministry of Transport and Infrastructure is the body responsible for making policies and developing strategies and action plans on national cybersecurity in Turkey. In this context, the national cybersecurity strategy and action plan was created by involving all the relevant stakeholders in study groups under the coordination of the Ministry of Transport and Infrastructure. The national cybersecurity strategy, the 2013–2014 action plan and the 2016–2019 national cybersecurity strategy and action plan were published and implemented. Turkey has been developing its next national cybersecurity strategy and action plan, which is planned to cover the years 2020–2023, and it will be published soon.

The main strategic objectives of the next national cybersecurity strategy and action plan of Turkey are:

- Protection of critical infrastructures and increasing resilience
- Capacity development
- Security of new technologies (Internet of things, 5G, cloud computing etc.)
- Combating cybercrime
- Developing and fostering national technologies
- Organic cybersecurity network
- Improving international cooperation.

Furthermore, the National Cyber Emergency Response Team of Turkey, which is part of the Information and Communication Technologies Authority, has coordinated the cyberincident response in Turkey since 2013. In addition to cyberthreat detection and cyberincident response including before, during and after the incidents, the National Cyber Emergency Response Team is responsible for the implementation of preventive measures against cyberthreats and ensures cyber deterrence. Its main focus areas in cybersecurity are; cyber capacity-building, technological measures, threat intelligence collection and sharing, and critical infrastructure protection.

In the context of improving national cybersecurity, 14 sectoral cyber emergency response teams for critical sectors or infrastructures (such as energy, health, banking

and finance, water management, electronic communications and critical public services) and 1,299 institutional cyber emergency response teams have also been established since 2013. They all operate 24 hours a day, seven days a week, under the coordination of the national team in order to mitigate cyber risks and to fight against cyberthreats.

The National Cyber Emergency Response Team organizes and supports training courses, summer camps and competitions on cybersecurity that are open for several communities. In addition, it provides training courses for cyber emergency response teams in areas such as malware analysis, log analysis and others. More than 4,500 people have been trained in different areas of cybersecurity by the National Cyber Emergency Response Team in the last three years.

Studies in technological measures include early detection, alarms and warning activities. For this purpose Turkey has developed detection and prevention systems. These systems play a huge role in increasing the level of national cybersecurity in Turkey.

Several Turkish organizations, institutions, universities, non-governmental organizations and the private sector also organize seminars, conferences and training courses nationwide on cybersecurity, protection of critical infrastructures and other related topics.

Furthermore, a Safe Internet Day is organized annually for awareness activities on the conscious and safe use of the Internet. An Internet helpline and a safe web website, where families can find advice for efficient use of the Internet, have been launched (https://www.guvenlinet.org.tr/).

In line with the dissemination of ICT usage among individuals, personal information or data have become an attractive target for cyberattackers. The privacy and protection of personal data is also among the major security concerns. In this regard, Law No. 6698 on the protection of personal data came into effect in 2016 to protect privacy.

Turkey has taken important roles in many organizations, either by being a founder member, or by contributing to cooperation efforts on cybersecurity and information security issues. In this context, Turkey attaches importance to information-sharing with different countries and organizations in a large range of areas. The National Cyber Emergency Response Team of Turkey is a member of the Forum of Incident Response and Security Teams, Trusted Introducers, the International Telecommunication Union (ITU), the North Atlantic Treaty Organization (NATO) Multi National Malware Information Sharing Platform and the CyberSecurity Alliance for Mutual Progress. Turkey has also taken part in the NATO Cooperative Cyber Defence Centre of Excellence as a sponsoring nation since November 2015. In addition, there is ongoing bilateral and multilateral cooperation on cybersecurity such as memorandums of understanding with many countries. Furthermore, Turkey is an active participant and contributor to the studies of international organizations such as NATO, the United Nations, the Organization for Security and Cooperation in Europe, the Organization for Economic Cooperation and Development, the Group of 20, the Cooperation Council of Turkic-speaking States and the RACVIAC–Centre for Security Cooperation.

Cybersecurity exercises are another important activity for cooperation and preparedness. This kind of exercise performed at the national and international levels contributes to strengthening cyberspace and the testing of measures to be taken against potential cyberthreats. Since 2011, four national and two international cybersecurity exercises have been organized by the Ministry of Transport and Infrastructure. Most recently, Cyber Shield 2019, which is an international

cybersecurity exercise, was co-organized by the Ministry of Transport and Infrastructure and the Information and Communication Technologies Authority on 19 December 2019 in Ankara, Turkey. Cyber Shield 2019 was supported by ITU and the Cyber Security Alliance for Mutual Progress. Furthermore, Turkey participates in and contributes to international cybersecurity exercises such as NATO Locked Shields, NATO Cyber Coalition and the NATO Crisis Management Exercise.

Turkey has also ratified the Convention on Cybercrime, which 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.

International peace and security in cyberspace requires further studies based on enhanced international cooperation. It may clearly be seen that international law and the norms and rules stated in the reports of the Group of Governmental Experts and in related studies contribute to a safer cyberspace.

Additionally, improving collaboration and supporting information-sharing mechanisms are vital for fighting against cyberthreats and need to be given due priority.

Furthermore, the need for guidance about the security of new generation technologies (Internet of things, 5G, cloud computing, etc.) is another point to be taken into consideration. Guides or baseline security recommendations for new generation technologies, which are prepared with cooperation among Member States, will help to increase the readiness levels for the new cyberthreats that accompany them. In addition, as well as the other capacity-building and guidance studies, international cybersecurity exercises remain essential for increasing preparedness levels and building cyberincident response capacities across the world.

Ukraine

[Original: English]
[29 May 2020]

Since the beginning of the hybrid aggression of the Russian Federation against Ukraine, new threats and challenges have emerged, among which the use of cyberinfluence mechanisms to the detriment of Ukraine's State security has taken a significant place.

Ukraine remains unwavering in its commitment to international law on the use of information and communications technology (ICT), as well as its full support for the conclusions and recommendations contained in the reports of the Group of Governmental Experts. First of all, it refers to the preservation of sovereign equality of States, non-use of force or threat of use of force against the territorial integrity of States, non-interference in the internal affairs of other States and respect for human rights and fundamental freedoms.

In order to organize effective action to counter threats in cyberspace and legal regulation of behaviour in cyberspace, while outlining the development of the system of action to counter such threats at the State level, a number of regulations were adopted, the main ones being the Cybersecurity Strategy of Ukraine approved by the National Security and Defence Council; The decision on the cybersecurity strategy of Ukraine (enacted by Decree No. 96 of the President of Ukraine of 15 March 2016) and the Law on the basic principles of maintaining the cybersecurity of Ukraine of 5 May 2017.

A separate mechanism for countering cyberthreats was the use of the provisions of the Law of Ukraine on sanctions of 14 August 2014, which made it possible to

organize a rapid response to identified threats by applying restrictive measures against a number of legal entities and individuals involved in measures designed to harm Ukraine's national security.

Today, cyberprotection of State electronic information resources and critical infrastructure in Ukraine is carried out in accordance with the Law on the basic principles of maintaining the cybersecurity of Ukraine. The definitions of the authority, tasks and functions of the subjects of cybersecurity enshrined in this Law serve to establish a holistic system of cybersecurity.

In this regard, the basic principle in the development of public policy in the field of cybersecurity and cyberdefence is the development of a regulatory framework consistent with international approaches and standards. To implement this task, in particular, the following measures have been taken:

- The Resolution of the Government of Ukraine on approval of the general requirements for the cyberprotection of critical infrastructure was adopted; the approaches to cybersecurity defined by this resolution consider the requirements of international standards in the field of information security and implement the European Union directives, which makes the State an equal participant in the global security space
- Draft resolutions of the Government of Ukraine have been developed:
  - On approval of the procedure for reviewing the status of cyberprotection of critical information infrastructure, State information resources and information, the requirement for protection of which is established by law
  - On approval of the procedure for the designation of critical infrastructure facilities
  - On approval of the procedure for compiling a list of critical information infrastructure facilities, inclusion of critical information infrastructure facilities in the State register of critical information infrastructure facilities, and its formation and operation, taking into account the requirements of Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union
  - On approval of the protocol on joint actions of cybersecurity entities and owners (managers) of critical information infrastructure facilities during detection, prevention and cessation of cyberattacks and cyberincidents, as well as in eliminating their consequences.

In order to enhance the system of technical and cryptographic protection of information, the road map for reforming the field of information protection was introduced by adapting the legislation of Ukraine to the requirements of the legislation of the European Union; a draft law of Ukraine on information security and communication and information systems has been developed to implement this Roadmap.

One of the key elements for the effective development of the national cybersecurity system is the review of the condition of cybersecurity. The results of the review will be the basis for the development of a new national cybersecurity strategy or adjustment of the existing strategy, for improving the regulatory framework of cybersecurity entities, financing measures for cyberprotection of State information resources and critical infrastructure, improving the human resources training system in cybersecurity, the development of new approaches to the formation of public-private cooperation in this area, the strengthening of information exchange

between the subjects of cybersecurity and their interaction in addressing security issues.

Also, in order to strengthen information security and promote international cooperation in this area, the State Special Communications Service has made provision for:

- The functioning of the Computer Emergency Response Team of Ukraine, which is accredited by the Forum of Cyber Incident Response Teams and interacts with other teams from 96 States
- State control over the condition of protection in cyberspace and technical protection of State information resources and information, the requirement for the protection of which is established by law
- Participation in the meetings of national points of contact using the Communications Network of the Organization for Security and Cooperation in Europe (OSCE)
- Raising public awareness and conducting practical seminars on cybersecurity for the subjects of the national cybersecurity system
- Interaction with law enforcement agencies and timely information about cyberattacks
- Coordination, organization and carrying out of an audit of the communication and technological systems of critical infrastructure facilities, with the audit of information security in accordance with the State Standard of Ukraine ISO/IEC 27001: 2015.

Given the current challenges and threats, legal mechanisms are being established in the field of cyberdefence in Ukraine with a view to:

- Enhancing the security of network and information systems, the main purpose of which should be the effective protection of information and data, ensuring the stability of networks and systems and continuity of their functions, as well as the effectiveness of detection, response and minimization of recovery after cyberincidents
- Implementation of a risk management system
- Creating conditions for the provision of resources, including human resources in the field of cybersecurity
- Strengthening the operational and cyber resilience of critical infrastructure facilities
- Establishing a system for the preservation of State information resources and ensuring the protection of technological information, which is critical for the functioning of critical infrastructure facilities
- Participation in the Common Criteria Committee by acceding to the relevant agreement (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security), which will ensure the inclusion of products certified in Ukraine in the register recognized by the European Union countries and other leading countries in the field
- Ensuring strict compliance with the requirements of the legislation in the field of protection of State information resources, cryptographic and technical protection of information, including the protection of personal data, by the heads of bodies managing critical information infrastructure facilities

- Use of opportunities for public-private partnerships and stakeholders' interaction to solve the issues of cyberdefence and cybersecurity
- Raising the level of culture of behaviour on the Internet
- Active participation in relevant initiatives of the international community and joining the relevant structures of leading international organizations.

From 2015 to 2020, the National Security and Defence Council of Ukraine adopted annual decisions on the application of personal special economic and other restrictive measures (sanctions), which were implemented by the relevant decrees of the President of Ukraine.

In addition to the above, the Security Service of Ukraine, as one of the main entities responsible for cybersecurity, in accordance with its competence as defined by law, is taking measures to improve the domestic regulatory framework on cyberspace. In particular, work is carried out on a regular basis to determine the regulations necessary for the implementation of the Law on the basic principles of maintaining the cybersecurity of Ukraine.

Measures are being taken to apply the provisions of the Law on the basic principles of maintaining the cybersecurity of Ukraine to the regulatory framework governing the activities of the Security Service of Ukraine.

However, despite those measures, the issue of improving the regulatory framework in the field of information and cybersecurity is still relevant today.

In particular, a number of legislative initiatives relating to the Security Service, which were under consideration by the Verkhovna Rada committees of the previous convocation, have not yet been considered by Ukrainian parliamentarians (strengthening criminal liability for cybercrime, division of investigative powers between the Security Service and the National Police, and establishing liability for non-compliance).

The provisions of the Convention on Cybercrime have not been fully implemented.

The Council of Europe Convention on Cybercrime of 23 November 2001 was ratified by the Verkhovna Rada of Ukraine in September 2005. The provisions of the Convention cover criminal liability for offences against the confidentiality, integrity and availability of computer data and systems, namely: illegal access; illegal interception; data interference; system interference; and misuse of devices. That is, those provisions of the Convention cover crimes against the sustainable operation of critical infrastructure.

However, a number of provisions of the Convention on Cybercrime are not currently implemented in national legislation, which restricts the activities of law enforcement agencies to detect and prevent cybercrime. In particular, the provisions of the Convention on Cybercrime that need to be implemented concern the expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, the procedure for a production order, search and seizure of stored computer data, and real-time collection of traffic data (articles 16–20). There is also a need for amendments to the Criminal Procedure Code of Ukraine to introduce a separate category of evidence, namely digital evidence in criminal proceedings.

Currently, the representatives of the Security Service of Ukraine in the working group of the Verkhovna Rada Committee on Law Enforcement are working on the draft law of Ukraine on amendments to certain legislative acts on implementation of the Convention on Cybercrime in order to standardize the provisions of the Convention in Ukrainian legislation, improve the provisions of the Criminal

Procedure Code of Ukraine and establish an effective legal mechanism to combat cybercrime, including:

- Granting the heads of the operational unit, the investigator and the prosecutor the authority to give mandatory instructions to the owners of computer data (telecommunications operators and providers, other legal entities and individuals) for the expedited preservation of computer data required to solve the crime, for up to 90 days
- Establishing requirements for the disclosure by telecommunications operators and providers, at the request of law enforcement agencies, of the information necessary to identify service providers and the route by which the information was transmitted
- Introduction of an effective mechanism for the use of evidence in electronic (digital) form in criminal proceedings
- Amendments to the Criminal Procedure Code of Ukraine and the Law on telecommunications and the draft law on electronic communications in order to ensure the establishment of a legal mechanism to temporarily restrict access to information or computer data posted on a certain (identified) information resource (service) and determine the procedure for its implementation.

On 4 February 2020 the Verkhovna Rada of Ukraine withdrew the draft law on electronic communications (Reg. No. 2264), on which the Security Service of Ukraine had submitted comments and proposals through the Verkhovna Rada Committee on Digital Transformation at the end of 2019.

On 5 February 2020 a draft law with the same title (on electronic communications) and an almost identical author team was registered in the Verkhovna Rada of Ukraine for No. 3014. According to a preliminary analysis, the new draft legal act also does not contain provisions that would facilitate the full implementation of the provisions of the Convention on Cybercrime.

To address current issues in the field of cybersecurity in 2020, the Security Service of Ukraine supported the introduction of a legislative initiative for consideration of a number of bills by the Verkhovna Rada of the ninth convocation. Adoption of the bills will create a legal basis for the Security Service in accordance with the Law on the basic principles of maintaining the cybersecurity of Ukraine.

In particular, there is a legislative distinction between the investigators of the National Police and the security authorities for the investigation of crimes committed with the use of computers, systems and computer networks and telecommunications networks, State information resources and critical information infrastructure, as well as strengthening the penalties for committing these crimes.

The execution of tasks relating to the prevention, detection, cessation and disclosure of crimes against peace and the security of mankind committed in cyberspace, and the implementation of counterintelligence and investigative measures aimed at combating cyberterrorism and cyberespionage necessitate amendments to the Law on counterintelligence to supplement the functions and powers of bodies, subdivisions and employees of the Security Service of Ukraine.

In addition, the principles and guidelines for building the State system of critical infrastructure protection have not been established at the legislative level, the critical infrastructure of the State has not been defined at the level of bylaws (the List of Critical Infrastructure Objects and the List of Critical Information Infrastructure Objects have not yet been established).

In 2019, the Government approved the General Requirements for Cyber Protection of Critical Infrastructure Facilities (Resolution No. 518 of the Cabinet of Ministers of Ukraine of 19 June 2019). This legal act is invalid in the absence of the State List of Critical Infrastructure and the List of Critical Information Infrastructure, the existence of which is provided for by the Law on the basic principles of maintaining the cybersecurity of Ukraine.

The uncertainty regarding the critical infrastructure of the State complicates the implementation of cybersecurity and cybersecurity tasks assigned to the Security Service of Ukraine and other cybersecurity actors.

The need to ensure the development and adoption of the Law on critical infrastructure and its protection, as well as to accelerate the adoption of acts of the Cabinet of Ministers of Ukraine aimed at implementing the provisions of the Law on the basic principles of maintaining the cybersecurity of Ukraine was emphasized by the Verkhovna Rada Committee on Digital Transformation at a meeting on national cybersecurity and cyberdefence of Ukraine, including in the field of critical infrastructure, which took place on 23 December 2019.

The issue of the practical application of the Law on the basic principles of maintaining the cybersecurity of Ukraine and adoption of the regulations necessary for its implementation was considered separately at a meeting of the Verkhovna Rada Committee on Digital Transformation, which took place on 19 February 2020.

The problem of the absence of regulations to reduce the critical dependence of domestic institutions, organizations and enterprises on software of foreign origin, which may contain intentionally implemented vulnerabilities and undocumented functions, remains relevant.

According to the specialists of the Security Service of Ukraine, this requires the development of a national import substitution programme in the field of informatization, a set of measures to support domestic software producers, and the creation of:

- A register of verified software suppliers for critical information infrastructure facilities, and preparation of the procedure for their inclusion or exclusion from the specified register
- A register of proprietary software recommended for use at critical information infrastructure facilities
- A national repository of free software and strengthened implementation of State programmes for the transfer to public authorities and administration of its use.

Also, in order to establish a legislative procedure for an immediate and effective response to existing and potential threats to the national interests and security of Ukraine in the field of information and communications technology, appropriate amendments are required to the Law on sanctions: the introduction of restrictions on the use by critical infrastructure of all forms of ownership of software (including antivirus) and telecommunication equipment that was developed or manufactured by economic entities of the aggressor country.

An additional factor with a negative impact is the gap in domestic legislation in terms of the lack of a legally defined mechanism for blocking a user’s access to Internet resources and removing messages that contain information that was obtained illegally.

It should also be noted that the Security Service of Ukraine carries out measures of international cooperation in the field of strengthening information and

cybersecurity. The main priorities and areas, according to the cybersecurity strategy of Ukraine, are:

- Development of international cooperation in the field of cybersecurity
- Support for international initiatives in the field of cybersecurity that meet the national interests of Ukraine
- Deepening of Ukraine's cooperation with the European Union and the North Atlantic Treaty Organization (NATO) to strengthen Ukraine's cybersecurity capabilities
- Participation in confidence-building measures in cyberspace under the auspices of the OSCE.

In particular, the Security Service of Ukraine, within its areas of competence, participates in the activities of CyberEast, a joint project of the European Union and the Council of Europe for the Eastern Partnership Programme countries, which aims to implement legislative and policy decisions to implement the provisions of the Budapest Convention on Cybercrime. The CyberEast project is implemented by the European Union Directorate-General for Neighborhood and Enlargement Negotiations in conjunction with the Council of Europe Cybercrime Programme Office.

Emphasizing the importance of informing international partners about Ukraine's latest achievements in the field of cybersecurity, as well as the implementation of certain confidence-building measures in accordance with OSCE Permanent Council decisions Nos. 1039, 1106 and 1202 in the field of ICT use and ICT, representatives of the Security Service of Ukraine usually take part in the meetings of the OSCE ICT Informal Working Group. In addition, the Security Service of Ukraine has identified a contact point in the framework of confidence-building measure No. 8 set out in Decision 1202, which at the professional level performs activities as part of planned and unscheduled communication checks.

The Security Service of Ukraine also participates in an OSCE project, the main purpose of which is to conduct a detailed analysis of the national governance structure in the field of cybersecurity, as well as the implementation of Ukraine's confidence-building measures in the field of ICT and cybersecurity, as stipulated by Decision 1202.

In addition, in accordance with the tasks assigned to the Security Service of Ukraine, with the support of the Ukraine-NATO Trust Fund for Cyber Security, the necessary equipment was obtained and the Situation Centre for Cyber Security of the Security Service of Ukraine was established, aimed at:

Prevention, detection, suppression and detection of crimes against the peace and security of mankind committed in cyberspace

- Counterintelligence and investigative measures aimed at combating cyberterrorism and cyberespionage
- Verification of the readiness of critical infrastructure facilities for possible cyberattacks and cyberincidents
- Counteracting cybercrime, the consequences of which may threaten the vital interests of the state
- Investigation of cyberincidents and cyberattacks on State electronic information resources and critical information infrastructure
- Ensuring the response to cyberincidents in the field of State security.

The Security Service of Ukraine has also initiated cooperation on the exchange of information on cyberthreats, cyberattacks and cyberincidents using the Malware

Information Sharing Platform and Threat Sharing–Ukrainian Advantage, which is a public platform for cooperation between the Security Service of Ukraine and critical infrastructure facilities, other enterprises, institutions and organizations, regardless of ownership, and also individuals in matters of improving the security for users of information, telecommunications and information and telecommunications systems that they are authorized to provide protection for under the relevant agreements or other legal grounds.

United Arab Emirates

[Original: Arabic]
[31 May 2020]

National report on efforts by the United Arab Emirates to enhance information security and promote international cybersecurity cooperation

Introduction

The United Arab Emirates attaches great importance to cybersecurity. Warding off attacks using information and communications technology (ICT) that pose a serious threat to infrastructure, government services and individuals is key to maintaining the country's national security. The United Arab Emirates has therefore endeavoured to create an integrated system to ensure the security of vital sectors, enhance user confidence and stimulate innovation.

Efforts taken at the national level to strengthen cybersecurity

The country has launched a national cybersecurity strategy, the aim of which is to create a safe and flexible digital environment enabling individuals to achieve their ambitions and companies to grow. The goals of the strategy encompass five main areas:

1. To implement a comprehensive legal and regulatory framework to address cybercrime, protect current and emerging technologies and enable small and medium-sized enterprises to protect themselves against cyberthreats;

2. To develop an integrated awareness-raising and capacity-building programme in the area of cybersecurity, with a view to encouraging safe practices in the use of technology and developing the skills of cybersecurity personnel to effectively respond to attacks and secure systems and services;

3. To develop an effective national plan to enable a rapid and coordinated nationwide response to cybersecurity incidents;

4. To protect the digital infrastructure of vital sectors;

5. To strengthen local and global cybersecurity partnerships.

In 2006, the United Arab Emirates passed the Information Technology Crimes Act, which contains numerous provisions that protect private material published and circulated on ICT-based media and punishing the misuse of such media.

The United Arab Emirates has also launched numerous programmes and initiatives over the years to enhance cybersecurity, including the establishment of the national Computer Emergency Response Team (aeCERT). The team provides a range of services to government agencies, such as round-the-clock monitoring and inspection of infrastructure in order to identify and respond directly to any unusual activity or attacks; effective cybersecurity incident response; and security assessment of websites and mobile phone applications in order to address vulnerabilities that can be exploited or result in the leaking of information. The team also provides

government agencies and individuals, across a variety of platforms that include its website, social media and a mailing list, with regular security advisories and reports on major cyberattacks.

To ensure that best cybersecurity practices are applied throughout the country's vital sectors, an information security assurance system has been established to set benchmark requirements for raising the minimum protection level of information security assets and support systems.

Aside from policies and technical systems, there was a need to intensify the professional development of personnel in order to increase their awareness of how to use ICT constructively and safely and to make them the first line of defence against the dangers of cyberattack for both their country and their families. With that in mind, the national cybersecurity awareness and capacity-building programme was launched to foster a culture of cybersecurity in society and excellence in national cybersecurity competencies. Under the CyberPro initiative, cybersecurity professionals attend month-long training courses. A virtual academy offering courses in the same field has also been established. Public information campaigns and events are held periodically for different segments of society.

The cartoon character Salim, created with child online protection in mind, has made great headway in communicating to children, in a light-hearted and simple way, the principles of safe use of technology. In addition to a digital safety curriculum established in cooperation with the Ministry of Education and the launch of a Salim website, thousands of interactive workshops have been organized to educate children through story-telling in which they are the protagonists. Those initiatives have also led to the participation of children in awareness-raising through the Cybersecurity Ambassadors initiative, whereby they are given the tools to spread the word among their peers and encourage a safe, sound approach to the subject.

Efforts to strengthen international cybersecurity cooperation

The United Arab Emirates is well aware that achieving an optimal level of cybersecurity and capacity to respond to attacks and risks requires international cooperation and a serious attitude. It therefore strives to take an active part in all international cybersecurity forums, some of which are mentioned below.

The United Arab Emirates is a member of the International Telecommunication Union (ITU) and works with other member States to find solutions and identify best cybersecurity practices through the relevant study commissions and working groups. It is pleased that some of its own specialists occupy key positions in the Union, such as the head of the ITU Council Working Group on Child Online Protection, underlining the country's commitment to supporting global efforts on those important matters.

The United Arab Emirates is represented by aeCERT on the Board of the Organization of Islamic Cooperation Computer Emergency Response Team (OIC-CERT), in which it promotes cybersecurity awareness by developing programmes, manuals and other essential materials on security risks to institutions and individuals. The aeCERT team also takes an active part in the Arab Regional Cybersecurity Centre and the Gulf Cooperation Council (GCC) Committee of National Computer Emergency Response Centres.

In addition to working with international forums and organizations, the United Arab Emirates is keen to strengthen bilateral cybersecurity cooperation with friendly countries by signing memorandums of understanding and agreements to regulate the exchange of information and expertise between countries and cooperation in response to cyberattacks.

Views regarding the content of the concepts mentioned in the reports of the Group of Governmental Experts

The United Arab Emirates wishes to thank the Group of Governmental Experts for its reports on developments in the field of information and telecommunications in the context of international security. It agrees with the Group's findings on the importance of States striving to prevent harmful ICT practices, cooperate in responding to cyberattacks, support dialogue built on transparency and joint action, support the global development of digital infrastructure and consult on the development of cybersecurity legislation, strategies and systems.

III. Replies received from intergovernmental Organizations

European Union

[Original: English]
[20 May 2020]

Cyberspace, and in particular the global, open Internet, has become one of the backbones of our societies. It offers a platform that drives connectivity and economic growth. The European Union and its member States support a global, open, stable, peaceful and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply, with a view to societal well-being, economic growth, prosperity and the integrity of free and democratic societies.

As the Internet becomes more embedded in our lives, a number of the same issues we face in the physical world arise in cyberspace. In the international context, some States appear to have embraced a vision for cyberspace that involves a high degree of government control, raising concerns over infringements of human rights and fundamental freedoms. There has also been a worrying increase in malicious cyberactivities by State and non-State actors. The European Union and its member States have regularly expressed concern about such malicious activities, which undermine the rules-based international order and increase the risks of conflict.

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

The European Union and its member States strongly support the aforementioned vision of an open, free, stable and secure cyberspace, through advancing and implementing an inclusive and multifaceted strategic framework for conflict prevention and stability in cyberspace, including through bilateral, regional and multi-stakeholder engagement. As part of this strategic framework, the European Union works to strengthen global resilience, advance and promote a common understanding of the rules-based international order in cyberspace, and develop and implement practical cooperative measures, including regional confidence-building measures between States. Strengthening global cyber resilience is a crucial element in maintaining international peace and stability, by reducing the risk of conflict and as a means to address the challenges associated with the digitalization of our economies and societies. Global cyber resilience reduces the ability of potential perpetrators to misuse information and communications technology (ICT) for malicious purposes and strengthens the ability of States to effectively respond to and recover from cyber incidents.

The cybersecurity strategy "An Open, Safe and Secure Cyberspace",[12] as well as other subsequent policy documents cited below, represent the European Union's comprehensive vision on how best to prevent and respond to cyber disruptions and cyberattacks. They are aimed at promoting European Union values and ensuring that the conditions are in place for the digital economy to grow. Certain specific actions are aimed at enhancing the cyber resilience of information systems, reducing cybercrime and strengthening European Union international cybersecurity policy and cyber defence.

In February 2015, the Council of the European Union stressed in its Council Conclusions on Cyber Diplomacy[13] the importance of further developing and implementing a common and comprehensive European Union approach to cyber diplomacy that promotes human rights and fundamental European Union values, ensures free expression, promotes gender quality, advances economic growth, combats cybercrime, mitigates cybersecurity threats, prevents conflicts and provides stability in international relations. The European Union also calls for a strengthened multi-stakeholder model of Internet governance and for enhanced capacity-building efforts in third countries. In addition, the European Union recognizes the importance of engagement with key partners and international organizations. The European Union also stresses the application of existing international law in the field of international security and the relevance of norms of behaviour, as well as the importance of Internet governance as an integral part of the common and comprehensive European Union approach for cyber diplomacy.

Based on a review of the 2013 Cybersecurity Strategy, the European Union further strengthened its cybersecurity structures and capabilities in a coordinated manner, with the full cooperation of the member States and the different European Union structures concerned, while respecting their competencies and responsibilities. In 2017, the joint communication entitled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[14] sets out the scale of the challenge and the range of measures envisioned at the European Union level, to ensure that the European Union is better prepared to face the ever-increasing cybersecurity challenges.

Concerns about ever-increasing cybersecurity challenges gave an impetus to the development of a framework for a joint European Union diplomatic response to malicious cyberactivities, the cyber diplomacy toolbox.[15] The increasing ability and willingness of State and non-State actors to pursue their objectives through malicious cyberactivities should be of global concern. Such activities may constitute wrongful acts under international law and could lead to destabilising and cascading effects with enhanced risks of conflict. The European Union and its member States are committed to the settlement of international disputes in cyberspace by peaceful means. To this end, the framework for a joint European Union diplomatic response is part of the European Union's approach to cyber diplomacy, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. The framework encourages cooperation, facilitates mitigation of immediate and long-term threats, and influences the behaviour of malicious actors in the long term. It also provides due coordination with the European Union's crisis

[12] See joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace".

[13] 6122/15 Council Conclusions on Cyber Diplomacy.

[14] See joint communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

[15] 10474/17. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

management mechanisms, including the Blueprint for Coordinated Response to Large Scale Cybersecurity Incidents and Crises. The European Union and its member States call on the international community to strengthen international cooperation in favour of a global, open, stable, peaceful and secure cyberspace where human rights, fundamental freedoms and the rule of law fully apply. They are determined to continue their efforts to prevent, discourage, deter and respond to malicious activities, and they seek to enhance international cooperation to this effect.

The European Union's international cyberspace policy promotes respect for European Union core values, defines norms for responsible behaviour and advocates the application of existing international laws in cyberspace, while assisting countries outside the European Union with cybersecurity capacity-building and promoting international cooperation on cyber issues.

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

Existing and emerging threats

The European Union and its member States recognize that cyberspace offers significant opportunities for economic growth, as well as sustainable and inclusive development. Nonetheless, recent developments in cyberspace present continuously evolving challenges.

The European Union and its member States are concerned by the rise in malicious behaviour in cyberspace, including the abuse of information and communications technology (ICT) for malicious purposes, by both State and non-State actors, as well as the increase in cyber-enabled theft of intellectual property. Such behaviour undermines and threatens economic growth, as well as the integrity, security and stability of the global community, and can lead to destabilising and cascading effects with enhanced risks of conflict.

More recently, as the coronavirus disease (COVID-19) pandemic continues, the European Union and its member States have observed cyberthreats and malicious cyberactivities targeting essential operators in member States and their international partners, including in the health care sector. The European Union and its member States condemn this malicious behaviour in cyberspace and underline their continued support to increasing global cyber resilience.

Any attempt to hamper the ability of critical infrastructures is unacceptable and can put people's lives at risk. All actors should refrain from conducting irresponsible and destabilizing activities in cyberspace. The European Union and its member States call upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law and the 2010, 2013 and 2015 consensus reports of the United Nations Groups of Governmental Experts. The European Union and its member States emphasize again that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs and should also respond to appropriate requests by another State to mitigate malicious cyberactivities emanating from their territory.

In addition, as recognized in previous reports of the Group of Governmental Experts, given the unique character of ICs, the European Union's approach to addressing cyber issues in the context of international security must remain technology-neutral. This is consistent with the concept and with the acknowledgement by the United Nations that existing international law applies to new areas, including the use of emerging technologies.

The European Union and its member States can only support the development and use of technologies, systems or services enabled by ICTs that fully respect

applicable international law and norms, particularly the Charter of the United Nations, as well as international humanitarian law and its derived principles and human rights.

How international law applies to the use of information and communication technologies

The European Union and its member States strongly support an effective multilateral system, underpinned by a rules-based international order, which delivers results in tackling present and future global challenges in cyberspace.

A truly universal cybersecurity framework can only be based on existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law. In addition, the European Union and its member States reiterate the applicability of existing international law to State conduct in cyberspace, as recognized by the reports of the Governmental Group of Experts in 2010, 2013 and 2015, as well as the principles established in paragraphs 28 (a) to 28 (f) of the 2015 report.

International law, including international humanitarian law, which incorporates the principles of precaution, humanity, military necessity, proportionality and distinction, applies to State conduct in cyberspace and is wholly protective, by setting clear boundaries for its legality, also in times of conflict. The European Union underlines its conviction that international law is not an enabler of conduct; rather, international law delineates the rules governing military operations to limit their effects, and in particular to protect civilian populations.

Furthermore, human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online and offline. The European Union and its member States welcome that these principles have also been affirmed by the Human Rights Council[16] and the General Assembly.

For these reasons, the European Union and its member States do not call for and do not see the necessity for the creation of new international legal instruments for cyber issues at this stage, as there is already an international legal framework.

The European Union and its member States reaffirm their support for continued dialogue and cooperation to advance a shared understanding on the application of existing international law to the use of ICT by States, as well as their support to efforts to bring legal clarity on how existing international law applies, as it will contribute to maintaining peace, preventing conflict and ensuring global stability.

We continue to support ongoing efforts to promote the application of existing international law to cyberspace, including on exchanging information and best practices on the application of existing international law in cyberspace. We are committed to continuing to report on national positions on how international law applies to the use of ICT by States, as it promotes transparency and advances global understanding on national approaches, which is fundamental to maintaining long-term peace and stability and reduces the risk of conflict through acts in cyberspace. Further focus should be placed on raising awareness on the applicability of existing international law as a mean to promote stability and to prevent conflict in cyberspace.

Norms, rules and principles for the responsible behaviour of States

The European Union and its member States encourage all States to build on and advance the work repeatedly endorsed by the General Assembly, notably in its

[16] A/HRC/RES/20/8.

resolution 70/237, and on further implementation of these agreed norms and confidence-building measures, which play an essential role in conflict prevention.

The European Union and its member States will be guided in their use of ICT by existing international law, as well as through adherence to voluntary norms, rules and principles of responsible State behaviour and their implementation in cyberspace, as articulated in successive reports of the Group of Governmental Experts in 2010, 2013 and 2015. We believe that a practical way forward should encourage increased cooperation and transparency to share best practices, including on how the existing norms of the Group of Governmental Experts are applied, through related initiatives and frameworks, such as regional organizations and institutions, to facilitate awareness-raising and to effectively implement agreed norms of responsible State behaviour.

Confidence-building measures

Building effective mechanisms of State cooperation and interaction in cyberspace are critical components in conflict prevention. Regional forums have proven to be a relevant platform to create space for dialogue and cooperation among actors with shared concerns but common interests in order to address effectively challenges from a regional perspective.

Developing and implementing cyber confidence-building measures, including cooperation and transparency measures, in the Organization for Security and Cooperation in Europe (OSCE), the Regional Forum of the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS) and other regional settings will increase the predictability of State behaviour and reduce the risk of misinterpretation, escalation and conflict that may stem from ICT incidents, thereby contributing to long-term stability in cyberspace.

International cooperation and assistance regarding security and capacity-building of information and communications technologies

In order to prevent conflicts and reduce tensions stemming from the misuse of ICTs, the European Union and its member States aim to strengthen resilience globally, with particular emphasis on developing countries, as a means of addressing the challenges associated with the digitalization of economies and societies, as wells as reducing the ability of potential perpetrators to misuse ICTs for malicious purpose. Resilience strengthens the ability of States to effectively respond to and recover from cyberthreats.

The European Union and its member States support a range of tailored programmes and initiatives to assist countries with developing their skills and capacities to address cyber incidents, as well as initiatives to facilitate the exchange of best practices, whether through direct engagement, bilateral contacts or engagement through regional and multilateral institutions.

The European Union and its member States recognize that the promotion of adequate protective capacities and more secure digital products, processes and services will contribute to a more secure and trustworthy cyberspace. We recognize the responsibility of all relevant actors to engage in capacity development in this regard and further call for stronger cooperation with key international partners and organizations to support capacity-building in third countries.