United Nations A/76/187

General Assembly

Distr.: General
19 July 2021
English
Original: English/Spanish

Seventy-sixth session
Item 96 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Advancing responsible State behaviour in cyberspace in the context of international security

Report of the Secretary-General

Contents

* A/76/150.

I. Introduction

1. On 7 December 2020, the General Assembly adopted resolution 75/32 entitled "Advancing responsible State behaviour in cyberspace in the context of international security" under the agenda item "Developments in the field of information and telecommunications in the context of international security".

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

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

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

3. Pursuant to that request, on 18 February 2021, a note verbale was sent to all Member States inviting them to provide information on the subject. In order to facilitate the submission of the views of Member States on the issues outlined above, the deadline for submission was 31 May 2021.

4. The replies received at the time of reporting are contained in sections II and III below. Additional replies received after 31 May 2021 will be posted on the website of the Office for Disarmament Affairs[1] in the original language received. No addenda will be issued.

II. Replies received from Governments

Australia

[Original: English]
[31 May 2021]

Australia welcomes the opportunity, in response to the invitation in General Assembly resolution 75/32, 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 resolutions 74/28 in 2020, 70/237 in 2016, 68/243 in 2014 and 65/41 in 2011 on developments in the field of information and telecommunications in the context of international security.

International Cyber and Critical Technology Engagement Strategy

On 21 April 2021, Minister for Foreign Affairs Marise Payne launched Australia's International Cyber and Critical Technology Engagement Strategy, which sets out Australia's interests and objectives in cyberspace and critical technology. Australia's overarching goal is a safe, secure and prosperous Australia, Indo Pacific and world enabled by cyberspace and critical technology (www.internationalcybertech.gov.au/).

The Strategy sets out Australia's interests in pursuit of this goal across the spectrum of cyber and critical technology issues. This includes our core principles and values of human rights, rule of law, fairness, open competition, security, transparency, respect and integrity.

[1] http://www.un.org/disarmament/ict-security.

The Strategy identifies three main pillars, namely, values, security and prosperity, to guide Australia's international cyber and critical technology engagement:

(a) *Values*. Australia will always pursue a values-based approach to cyberspace and critical technology and oppose efforts to use technologies to undermine these values;

(b) *Security*. Australia will always support international peace and stability and secure, trusted and resilient technology;

(c) *Prosperity*. Australia will always advocate for cyberspace and technology to foster sustainable economic growth and development to enhance prosperity.

On 6 August 2020, Australia also released its *Cyber Security Strategy 2020* to achieve a more secure online world for Australians, their businesses and the essential services upon which Australia depends (www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf).

Framework of responsible State behaviour in cyberspace

As States increasingly exert power and influence in cyberspace, Australia considers it important that there be clear rules in place. Cumulatively, the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 2010 (A/65/201), 2013 (A/68/98) and 2015 (A/70/174) affirm that existing international law is applicable and essential to maintaining peace and stability in cyberspace. The reports also articulate 11 voluntary, non-binding norms of responsible State behaviour, while recognizing the need for confidence-building measures and coordinated capacity-building. Combined, 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 has been actively engaged in two recent United Nations processes considering responsible State behaviour in cyberspace that concluded in 2021: the sixth Group of Governmental Experts (see A/76/135) and the Open-Ended Working Group (see A/75/816), which reaffirm and build upon this framework.

Australia reaffirms its commitment to act in accordance with the cumulative reports of the Group of Governmental Experts of 2010, 2013, 2015 and 2021 (A/65/201, A/68/98 and A/70/174) and the report of the Open-ended Working Group (A/75/816).

International law

Australia's position on how international law applies to State conduct in cyberspace is presented in a series of documents: Australia's 2017 International Cyber Engagement Strategy (www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy), the 2019 International Law Supplement (https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal %20Supplment_0.PDF), case studies on the application of international law in cyberspace published in February 2020 (https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf), Australia's *International Cyber and Critical Technology Engagement Strategy 2021* and Australia's submission on international law to be annexed to the report of the 2021 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (publication pending).

Multi-stakeholder engagement

Australia recognizes the importance of the multi-stakeholder community, including civil society, the private sector, academia and the technical community, in contributing to a free, open, secure, stable, accessible and peaceful cyberspace.

To this end, Australia was pleased to co-sponsor the LetsTalkCyber initiative (letstalkcyber.org), which provided a platform for multi-stakeholder input into and engagement with the Open-ended Working Group, and consultations among States, civil society, the private sector, academia and the technical community. Australia also conducted several rounds of national multi-stakeholder consultations and actively sought the views of the multi-stakeholder community to inform its positions in the Open-ended Working Group and Governmental Group of Expert processes.

In addition, Australia established the Quad Tech Network to support research and promote engagement between States and academic and think-tank partners from Australia, India, Japan and the United States of America on cyber and critical technology issues. The Quad Tech Network will produce policy-relevant research and recommendations; deepen and strengthen public understanding of cyber and critical technology issues; and promote informed public dialogue. The Network was launched on 9 February with a series of public papers on international peace and security, connectivity and regional resilience, human rights and ethics, and national security (www.internationalcybertech.gov.au/node/139).

Colombia

[Original: Spanish]
[31 May 2021]

In accordance with General Assembly resolution 75/32 on 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, 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.

The present report builds on that submitted in 2020, highlighting the progress made in the last year, mainly in relation to the recommendations set forth for States' consideration in the 2015 report of the Group of Governmental Experts, in order to promote an open, secure, stable, accessible and peaceful environment in the field of information and communications technology (ICT).

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

Consistent with the purposes of the United Nations, including to maintain international peace and security, States should collaborate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are considered to be harmful or that may pose threats to international peace and security.

The concept of ownership was emphasized in the national digital trust and security policy (National Council for Economic and Social Policy document No. 3995/2020), one of whose main stated objectives is to build the digital security capacities of citizens in the public and private sectors.

The Government of Colombia, through the Ministry of Information and Communications Technology, the National Training Service and the Ministry of Education, has implemented a series of specific activities based on the ownership strategy, as follows:

- As part of the "Let's talk about digital government" programme, covering the period from 2020 to 2021, the Ministry of Information and Communications Technology held 15 awareness-raising sessions relating to digital security for citizens, reaching more than 4,000 people. In 2020, the Ministry held three digital security training workshops for entrepreneurs and micro-, small and medium-sized enterprises, with the participation of 483 people, including 156 women. It also held two workshops relating to specific aspects of the information security and privacy model.

- For "Digital Security Month", several activities were conducted, including four workshops on specialized topics relating to incident management, with the support of Cisco and the Computer Emergency Response Group of Colombia; two workshops on the importance of auditing and risk management in public entities; two "Let's talk about digital government" sessions on the results of the exercise conducted with the Organization of American States (OAS); the first cybersecurity innovation council meeting held in Colombia; and talks entitled "Recommendations to avoid becoming a victim of cybercriminals" and "Disinformation on the web from a legal perspective", aimed at the general public. To conclude the month's activities, the second cybersecurity innovation council meeting was held in conjunction with OAS. A total of 1,040 people, including public officials and end users, participated in these activities, and 45 per cent of the participants were women.

- During the "Colombia 4.0" event, as part of the activities carried out during the CIO Summit 2020, which brought together technology leaders of public entities, a conference under the theme "How to survive COVID-19 and the digital transformation and not be hacked while trying" was held, bringing together 490 people. A workshop under the theme "Best practices for threat detection and response based on the MITRE ATT&CK and XDR model", in which an estimated 40 per cent of participants were women, was also held. Awareness-raising activities relating to the information security and privacy model were conducted for approximately 3,196 officials from 1,834 entities, including 131 national entities and 1,224 local entities.

- As part of its "Digital Talent" initiative, the Ministry of Information and Communications Technology launched the "Digital Skills – Cybersecurity Training" competition for the selection of Colombian personnel for training and capacity-building in matters related to cybersecurity. Two diploma courses for training in the development of specialized skills were offered: (i) a course on cybersecurity for executives and managers and (ii) a course on cybersecurity for technical personnel.

- The National Training Service offers programmes on the following topics: computer network security, database management and security, digital security monitoring, device firmware programming, introduction to information security management systems in accordance with ISO IEC standard No. 27001, the application of diagnostic techniques in the area of cybersecurity, and computer security management.

- To promote ownership, the Ministry of Education has implemented activities related to the dissemination of content (use of social networks, and campaigns and workshops with public entities and micro-, small and medium-sized enterprises). It has also established partnerships with the private sector and has engaged in international cooperation.

- The Ministry of Education has also developed diploma courses benefiting 2,216 teachers, and has incorporated the digital security strategy into the Digital Learning project for primary, basic and secondary school students, benefiting 4,093 students, including on the "Colombia Learns" (*Colombia Aprende*) portal, with more than 30 pieces of content.

In response to the recommendation that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, the Government of Colombia has implemented the activities described below.

- The national digital trust and security policy (National Council for Economic and Social Policy document No. 3995/2020) established, as a coordination and governance mechanism, the role of national coordinator, performed by the President's Office of Economic and Digital Transformation Advisers, and the Digital Security Committee, a collegiate body composed of entities involved in promoting digital security whose purpose is to consider specific issues pertaining to digital security at strategic levels, within the areas covered by its mandate: (1) digital security policy and laws; (2) protection and defence of the national critical cyberinfrastructure; (3) digital security risk management; (4) crises and cyberthreat monitoring; (5) personal data protection; (6) international digital security issues; and (7) strategic communications for digital security.
- The Government has established a unified command post for cybersecurity in order to ensure the security and integrity of government technological infrastructure and websites during national holidays, elections and other milestone events. The post's objectives are: (i) to protect citizens and the Government against cyberthreats; (ii) to prevent and anticipate cyberthreats and conduct judicial investigations; (iii) to address cybersecurity incidents; (iv) to ensure the stability of governmental and institutional bodies; and (v) to strengthen software. The Government has also established action protocols to respond to possible attacks, such as distributed denial-of-service attacks on web portals (DDOS), web vulnerabilities and fake news.
- The Government has carried out activities in coordination with the national Senate, including training in the development of best practices for the use of virtual platforms.

With regard to the best ways to cooperate to exchange information, provide mutual assistance, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats, on 16 March 2020, Colombia acceded to the Convention on Cybercrime, adopted in Budapest in 2001, and brought it into force on 1 July 2020. Efforts to implement the Convention are currently under way.

Colombia has taken appropriate measures to protect critical infrastructure from ICT threats by strengthening the Government's computer security incident response team in order to protect public institutions. Through that initiative, Colombia aims to develop a comprehensive solution to ensure that the Government's computer security incident response team provides stronger and more efficient services to State entities, enhancing the team's impact throughout the country by developing IT and physical infrastructure and human talent and guaranteeing 24/7 service.

Colombia has also proposed a number of initiatives, including the preparation of a current assessment and a plan for the continuous improvement of its operational, administrative, human and scientific capacities and technological infrastructure, in order to leverage resources to strengthen those entities' digital security capacities.

The project to relocate and optimize the Government's computer security incident response team is also under way.

In response to the recommendation that States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure, Colombia, in conjunction with OAS and the Organisation for Economic Co-operation and Development, is encouraging the responsible reporting of ICT vulnerabilities, and is taking reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques and harmful hidden functions.

The new public policy document (National Council for Economic and Social Policy document No. 3995/2020) entitled "National Digital Trust and Security Policy" established specific measures for the development of a model for the periodic reporting of vulnerabilities in all sectors between the points of contact of owners and operators of assets that support critical activities and relevant national government bodies. Many stakeholders will be involved, and international experiences will be taken into account in the development of this model.

In response to the recommendation that 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, and that a State should not use authorized emergency response teams to engage in malicious international activity, Colombia has taken steps in accordance with international law and the Charter of the United Nations, recognizing that it has a primary responsibility for maintaining a secure and peaceful ICT environment.

The Government of Colombia also issued decision No. 500 and Presidential Directive No. 3 of March 2021 in order to establish guidelines and standards for the digital security strategy and to adopt the security and privacy model as an enabler of the digital government policy.

Article 16 of Decree No. 2106 of 2019 sets forth rules to simplify, eliminate and reform unnecessary public administration formalities, processes and procedures, and states that authorities must have a digital security strategy for electronic document management and the preservation of information, in accordance with the guidelines issued by the Ministry of Information and Communications Technology.

As an enabler of the digital government policy, the Ministry of Information and Communications Technology sets out guidelines for the implementation of the information security and privacy model and the management of information security risks, as well as procedures for the management of digital security incidents and guidelines and standards for the digital security strategy.

Colombia has opted for measures involving law enforcement, intelligence and diplomatic tools for stopping cyberattacks and preventing the destruction of property and loss of life, exhausting all options for defending the network before carrying out an operation in cyberspace.

In developing the national digital security policy, the Government of Colombia focused on three basic areas: (i) building capacities for risk management in the digital environment; (ii) establishing institutions that support governance; and (iii) evaluating activity frameworks and international best practices. In order to implement the policy, the Government's strategy is to:

- Prepare a current assessment and a plan for the continuous improvement of its operational, administrative, human and scientific capacities and technological infrastructure.

- Formulate guidelines for the establishment of a digital civic participation network through which various stakeholders can interact and cooperate in addressing cyberthreats, in order to strengthen and expand digital security capacities in Colombia in accordance with international law.

- Coordinate the development of guidelines for digital security improvement plans with the aim of strengthening the capacities of the comprehensive social security system to handle, manage and exchange information, as that system constitutes critical cyberinfrastructure.

- Establish, under the national incident management model, guidelines indicating the special conditions for managing risks and addressing digital security incidents related to the handling, management and exchange of information from the comprehensive social security system; those conditions would have to be incorporated into the general incident management procedure established by the Digital Security Committee.

- Coordinate the incorporation of appropriate technical, legal, organizational and other mechanisms for gathering necessary digital evidence in the event of a cybersecurity incident in the handling, management and exchange of information from the health subsystem of the comprehensive social security system.

- Design, develop and present the draft plan for the establishment of the computer security incident response team for the comprehensive social security sector.

- Design, develop and present the draft plan for the establishment of the computer security incident response team for the intelligence sector, to help ensure national digital security.

- Design a proposal for a single central registry of digital security incidents at the national level, in order to analyse incident types and periodically assess the need to prioritize strategies and resources for incident management. This registry should include existing reports on the subject from various stakeholders and should be aimed at simplifying the sending of information, establishing secure means of delivery and ensuring the confidentiality, conservation and appropriate use of the information exchanged between parties.

Colombia is seeking to protect citizens' constitutional rights and freedoms with respect to obtaining and using information.

Colombia has adopted the legislative measures necessary to establish as criminal offences: (i) intentional and unauthorized access to the whole or any part of a computer system; (ii) the intentional and unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; (iii) the intentional and unauthorized interception, by technical means, of computer data; and (iv) the production, dissemination or transmission of child pornography.

Colombia is developing clear definitions of national and international critical infrastructure, is identifying sectors whose products or services qualify as critical infrastructure and maintains a list of critical assets. It is sharing those definitions with the international community as a confidence-building measure.

Colombia is also working to establish crisis resolution networks among relevant public sector stakeholders that request support. In addition, it is planning to collaborate with the international community to establish a network of points of contact "at the policy and technical levels". In that regard, Colombia has:

- Designed national and international cybersecurity exercises to regularly test its ability to communicate with other States and to respond to requests for assistance and mitigation (in particular channels of communication, protocols and procedures), through joint cybersecurity exercises.
- Participated in activities within the framework of CyberEx and the CyberDrills of the International Telecommunications Union, and coordinated national crisis simulation exercises with the Joint Cyber Command.
- Used pre-established national multi-stakeholder crisis resolution networks and relied on the mitigation expertise provided by the State, as well as non-State actors, during cyberoperations of this type, following best practices relating to incident reporting at the national and international levels.
- Carried out activities with associations. Since the attacks by hacktivist groups against both the Government and private companies that occurred in the midst of social protests in cyberspace, the Colombian Software and IT Industry Federation has been collaborating with the Government on behalf of a group of companies to develop specific digital security solutions. As part of that collaboration, it has held meetings with the Government to consider the areas in which the Federation could support the Government and has, to that end, conducted a survey among its member companies regarding their intelligence and monitoring capacities.

The Government of Colombia has cooperated with the United States in addressing malicious cyber operations against critical infrastructure.

Voluntary confidence-building measures

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, the National Police, through the Cyber Police Centre of the Directorate for Criminal Investigation and the International Criminal Police Organization (INTERPOL), has been collaborating with the member entities of the national Government's Digital Security Committee in addressing three components of cybersecurity: prevention, investigation and computer forensics.

Consequently, in 2020 and 2021, 32 anti-cybercrime operations were carried out, resulting in 219 arrests for cybercrimes; 14,072 cybersecurity incidents were addressed through the 24/7 virtual CAI service; the banning of 7,139 websites containing child sexual abuse material and of 1,648 illegal gambling websites was requested; and 454 news bulletins were issued.

Colombia has also fostered active cooperation by implementing cyber command posts, led by the Cybersecurity Capacities Centre of Colombia, in order to consolidate cybersecurity and cyberdefence capacities in the country.

The Cybersecurity Capacities Centre of Colombia has been implementing the Comprehensive Cybersecurity Strategy in order to ensure active coordination between the central judicial police and the 51 local criminal investigation units, with the aim of standardizing investigation techniques, as well as tools and mechanisms for active cooperation.

As reported by the Attorney General's Office, cybercrime has been on the rise since 2009, and increased sharply in 2019. In 2018, 22,238 cybercrimes occurred, while in 2019, 24,197 occurred, an increase of 9 per cent. That trend was consolidated in 2020: from 1 January to 31 December 2020, 35,346 cybercrimes occurred, representing an increase of 70 per cent. The number of cybercrime cases in the country therefore rose during the pandemic.

The Attorney General's Office has a permanent communication channel through which it exchanges information with the Cyber Police Centre, which is the 24/7 point of contact pursuant to article 35 of the Convention on Cybercrime.

In order to improve cooperation between the two entities, the Cybersecurity Capacities Centre of Colombia of the National Police has provided training to groups responsible for cybercrime in the Attorney General's Office on the capabilities of the Cyber Police Centre.

As already noted, through National Council for Economic and Social Policy document No. 3995/2020, Colombia seeks to strengthen cybersecurity and cyberdefence policy and international cooperation. It also hopes to improve information-sharing, cooperation and robust, effective and timely coordination among cybersecurity stakeholders at the national level through crisis response mechanisms such as unified command posts.

With regard to cooperation, in accordance with national and international law, with respect to requests for assistance from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes, or in mitigating malicious ICT activity emanating from Colombia, as indicated in the 2020–2024 strategic guidance of the Attorney General's Office, a road map established by the Office which comprehensively sets forth its envisaged work for the coming years, the Attorney General's Office will prioritize the investigation of cybercrimes. Accordingly, the Office will develop a strategy to strengthen and coordinate the investigative capacities of the investigators and prosecutors involved in such cases.

Monthly statistics on cybercrime for the period from the promulgation of Act No. 1273 of 2009 to the present can be found in the section entitled "Open data of the Attorney General's Office: search and downloadable files" of the website of the Attorney General's Office, using parameters such as the type of crime under the Criminal Code of Colombia, the year in which the Attorney General's Office received the crime report or the year in which the events occurred, the department in which the events occurred, the status and stage of the proceedings and the sex and age group of the victims or suspects. The model also has information indicating, for reported crimes, whether charges have been brought, convictions have been handed down, arrest warrants have been issued or the cases have been closed because the events did not constitute a crime or did not occur.

The national-level cybercrime groups of the Attorney General's Office in the country's main cities are responsible for processing, analysing and preserving digital evidence, and for investigating cybercrimes, including theft through the use of a computer and child pornography, which, owing to the place of the events, fall within their jurisdiction. During such investigations, the groups are required to execute interviews and inspections, writs of ne exeat, verifications, searches, seizures and arrests, and to accompany arrested persons to various hearings. The groups are also required to support all offices within their jurisdiction in extracting and preserving digital evidence from devices or Internet sites in all criminal cases in which such activities are required, including cases of homicide, sexual acts with a minor under 14 years of age, pornography involving a minor under 18 years of age and sometimes even libel and slander.

The Directorate of International Affairs of the Attorney General's Office handles all requests for legal assistance, most of which involve the invocation of the Convention on Cybercrime, and has already applied the criteria and filters recommended in the *Practical Guide for Requesting Electronic Evidence across*

Borders, jointly developed by the United Nations Office on Drugs and Crime, the United Nations Counter-Terrorism Executive Directorate and the International Association of Prosecutors, and translated into Spanish with the support of OAS.

Through the Cybersecurity Capacities Centre of Colombia, the National Police, as the 24/7 point of contact under the Convention on Cybercrime, has become one of the main international cooperation entities by having as cybersecurity points of contact important agencies such as the European Union Agency for Law Enforcement Cooperation and INTERPOL, and by strengthening the institutions involved in implementing the Convention.

Through the 24/7 point of contact, Colombia intends to accelerate the processing of requests for mutual legal assistance by cooperating with the 65 other States parties and 13 observers to the Convention on Cybercrime.

The information that follows relates to the following recommendation: given the pace of ICT development and the scope of the threat, there is a need to enhance common understandings and intensify cooperation and, in this regard, efforts should be made to hold regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums and other international organizations.

Colombia continues to participate actively in multilateral dialogues under the auspices of the United Nations and other international forums, in particular on matters related to responsible State behaviour in cyberspace and developments in the field of information and communications in the context of international security.

In the current environment of unprecedented global interconnectedness, States maintain relationships of complex interdependence and share joint problems that they cannot solve alone. They must therefore opt for international cooperation on cybersecurity, as the dissemination and use of information technologies and media affect the interests of the entire international community. It is therefore in the interest of all States to promote the use of ICTs for peaceful purposes and to prevent conflict arising from the use of ICTs. Accordingly, States should:

- Provide assistance to build ICT capacity, which is essential for international security, by improving the capacity of States for cooperation and collective action and promoting the use of ICTs for peaceful purposes, building on the international cooperation led by the computer security incident response team.
- Establish mechanisms for the participation of the private sector, academia and civil society organizations in order to contribute to the field of information and telecommunications in the context of international security, in which all States participate.

With regard to the implementation of voluntary cooperation measures in bilateral, multilateral and regional organizations, in order to ensure effective voluntary cooperation and increase trust to support joint efforts by States to combat national and international ICT threats, the Government of Colombia, through the Ministry of Information and Communications Technology, has:

- Participated in regional programmes such as the cybersecurity round table of the Network of e-Government Leaders of Latin America and the Caribbean, and continued to cooperate with OAS.
- Worked, since 2017, on the Cybersecurity Career Path project, coordinated by the OAS cybersecurity programme and funded by the Citi Foundation, which is aimed at providing training and promoting professional development in the area of cybersecurity for young people aged 18 to 25 from low-income households in Brazil, Colombia, Costa Rica, the Dominican Republic and Peru.

- Developed the "Hacker Girls" initiative, whose purpose is to promote and create educational spaces and work opportunities for women by improving their knowledge of matters related to cybersecurity. Through this initiative, the Ministry of Information and Communications Technology has trained more than 350 women security experts who will form part of a qualified group of first-level women digital security experts in Colombia who, in the future, will comprise the "Colombian Hacker Girls Team", making the country a regional leader in such initiatives.
- Hosted dialogues under the auspices of the cybersecurity innovation councils, during which two events led by regional experts and specialists in design thinking were held, with the participation of high-level executives from the public and private sectors, unions and academia, in order to promote innovation, raise awareness among participants and disseminate best practices in cybersecurity in the region. These innovation councils were established under an agreement between the OAS cybersecurity programme and Cisco and their meetings are being held with the support of OAS.

With regard to the commitment to collective action in order to make the Internet a safer place and encourage technical assistance from technology companies to protect civilians, given that civilian private property is the main target of attacks, the Government of Colombia, through the Ministry of Information and Communications Technology, has implemented the "In ITC I Trust" programme, which fosters the development of digital skills in order to safely address the risks associated with the use of the Internet and ICTs, and promotes Internet use and ownership as an opportunity to create a positive digital footprint. This programme is aimed at females and males between the ages of 6 and 28, and offers differentiated strategies, in virtual and face-to-face work sessions, to help its beneficiaries to develop risk identification skills and promote digital coexistence and activism and the use of technological tools for advocating common positive causes on the Internet.

In addition, the Government of Colombia, through the Ministry of Information and Communications Technology, is providing specialized training in information security to public entities that request the support of the computer security incident response team, and is broadening the scope of cybersecurity research and strengthening operational, administrative, human and scientific capacities and physical and technological infrastructure. For example, it has:

– Established a guide containing advice and assistance for the implementation of the cross-cutting information security and privacy enabler for entities, anchored in the digital government policy, which is based on: (i) the information security and privacy model; and (ii) the digital security risk model – guide for risk management and the design of controls for public entities of the administrative department of the civil service.

– Established a strategy for ownership of the digital security policy defined through workshops, awareness-raising discussions and the development of interactive tools and training courses.

– The Government's computer security incident response team provides basic proactive and reactive security management services to all State entities by issuing alerts and warnings about threats and vulnerabilities, performing incident treatment, analysis, response and coordination, and improving security awareness, fostering a culture of digital security among all digital security workers and officials.

– Through its portfolio of services, the Government's computer security incident response team has provided assistance and support to State entities in order to improve technological infrastructure security processes, cybersecurity incident management and digital security awareness. The Government's computer security incident response team is composed of a group of specialized technicians who implement and develop activities to prevent and manage cybersecurity incidents.

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

With regard to the facilitation of cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders, the Attorney General's Office has noted that it is important to develop capacities in the region to combat cybercrime. Colombia has thus sought to develop strategic partnerships and has participated in various forums; for example, it has officially become a State party to the Convention on Cybercrime, has been involved in various United Nations working groups and has signed memorandums of understanding against cybercrime with various other States.

In addition, as part of its cooperation and coordination efforts, Colombia is working in conjunction with the network of computer security incident response teams in the Americas, a platform for the exchange of threat-related information and for cooperation among incident response groups in the region.

Colombia also participates in international information exchange projects, such as bulletins and early warnings for financial-sector-related governmental and supervisory entities of other countries in the region (for example, the Central American Council of Comptrollers of Banks, Insurance Companies and other Financial Institutions and the Pacific Alliance).

The Attorney General's Office has promoted the signing of a number of memorandums of understanding with other States in order to combat cybercrime and related offences.

With regard to further work in capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs, efforts to upgrade technology and capacities have progressed less rapidly owing to the high cost of licensing, equipment and training.

With regard to the recommendation to consider, in the interest of ICT security capacity-building, forming bilateral and multilateral cooperation initiatives that would build on established partnership relations, in order to build ICT security capacity, to help improve the environment for effective mutual assistance in the response to ICT incidents among States and competent international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations, the Government of Colombia, through the Ministry of Information and Communications Technologies, has chaired the Executive Committee of the Network of e-Government Leaders of Latin America and the Caribbean, which brings together digital government authorities from 34 countries in the region in order to address cybersecurity matters.

The following activities have been proposed in order to promote an understanding of the cybersecurity situation and put forward, for the Network's approval, measures to improve the level of cybersecurity in the Network's member countries and in the region:

- Study of the Inter-American Development Bank and OAS on cybersecurity maturity level.

- Maturity level of computer emergency response teams and computer security incident response teams SIM3.
- Archiving of cybersecurity guides, procedures and good practices.
- Cybersecurity event for decision-makers.
- Regional cybersecurity strategies.
- Development of regional voluntary good practices in handling sensitive data (improvement of cross-border digital signature use and interoperability).
- Study of the status of the computer security incident response teams of Network members.
- Development of sectoral computer security incident response teams and collaboration among computer security incident response teams in the region.
- Capacity-building in cybersecurity.
- Capacity-building for computer security incident response teams.
- Malware Information Sharing Platform (computer security incident response teams in the Americas).
- Analysis of regional data protection frameworks.

In addition, the Government of Colombia, in agreement with OAS and the Ministry of Information and Communications Technology, has taken steps to develop a series of proposals for a digital security governance model and a methodological guide for the identification and management of digital security risks in the adoption of emerging technologies for Colombia by:

- Compiling sources and references for both products to be proposed.
- Analysing best practices for both products through benchlearning, using governance models applicable to digital security.
- Analysing the local context (institutions, stakeholders, etc.).
- Developing the proposed principles and objectives of the governance model.
- Approving the proposed objectives and obtaining suggestions from many stakeholders on the governance model.
- Identifying stakeholders' expectations regarding the governance model.

In order to approve the proposed principles and objectives and the interests of stakeholders with respect to the governance model, on 30 October 2020, Colombia conducted the first working group session during the formal session of the Digital Security Committee, which was attended by more than 80 participants representing the many stakeholders in the national cybersecurity ecosystem.

With a view to developing a platform for operational cooperation not only with other States but also with the national private sector in order to address and respond to large-scale cybersecurity incidents and crises, the Government of Colombia, led by the Ministry of Defence, is working to implement the following objectives set forth in the action plan of National Council for Economic and Social Policy document No. 3995/2020:

(a) Developing digital trust through improvements in digital security, in order to make Colombia an inclusive and competitive society in the digital future through capacity-building and the updating of the digital security governance framework;

(b) Adopting models that emphasize new technologies and make it necessary to implement the technology underlying the national cybersecurity incident management system, in order to coordinate institutional efforts to manage cybersecurity incidents in a timely manner and establish the official source of statistics relating to cybersecurity incidents reported in the country;

(c) Standardizing a mechanism for periodic reporting of cybersecurity incidents and vulnerabilities so that they can be identified, assessed and communicated to stakeholders, and so that they can inform decision-making by the national Government.

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, to the extent applicable, international humanitarian law, applies to the "virtual" as well as "physical" domains, with the understanding that international humanitarian law only applies in situations of armed conflict in the virtual or physical domain.

International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Accordingly, the principle of sovereign equality, among other principles of international law such as State sovereignty, the peaceful settlement of disputes and non-intervention in the internal affairs of other States, is the basis for greater security in the use of ICTs by States.

Concepts

In order to promote a deeper understanding of concepts related to international peace and security in the use of ICTs at the legal, technical and political levels, given the specific nature and novelty of their application, Colombia believes that these concepts should continue to be discussed in multilateral forums, in accordance with the conclusions of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security set out in its final report, adopted by consensus in March 2021.

In order to promote a deeper understanding of the application of international law in cyberspace, capacity-building tools should be established to help States to develop a common vocabulary and more extensive knowledge so that they can adjust the international legal framework to the challenges of cyberspace and reach consensus on how international law is applied in the virtual domain.

It is important to continue to implement the recommendations of the Group of Governmental Experts and of the Open-ended Working Group.

It is also important to establish a global mechanism for regular institutional dialogue under the auspices of the United Nations in order to make progress in that regard, and to continue and strengthen the work being done at the regional level.

Colombia is therefore supporting and co-sponsoring the initiative to establish a programme of action on the responsible use of ICTs in the context of international security, as a permanent, inclusive, consensual and action-oriented international instrument designed to promote responsible behaviour in the use of ICTs in the context of international security.

Denmark

[Original: English]
[28 May 2021]

In Denmark, as in many parts of the world, 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, free, 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 2018–2023 allocates 1.4 billion Danish krone to strengthened cybersecurity and cyberdefence, thereby strengthening Denmark's resilience. The 2018–2021 Danish National Cyber and Information Security Strategy takes further steps to increase cyber and information security and ensure a systematic and coordinated effort. Through 25 initiatives and six targeted strategies addressing what is 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 the knowledge and skills of citizens, businesses and authorities and strengthened coordination and cooperation regarding cybersecurity.

As part of the 2018–2021 National Cyber and Information Security Strategy, dedicated cyber and information security units have been established in the six critical sectors mentioned above. Furthermore, the national strategy established a forum for the sectoral dedicated units and the Centre for Cyber Security focusing on sharing their experience in working with cyber and information security. The Agency for Digitisation 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. Beyond the Academy, the Centre for Cyber Security also supports education and research within cybersecurity.

In addition to these efforts, the Agency for Digitisation has developed and executed several courses, learning materials and events on cyber and information security targeting the chief executive level and cyberspecialists as well as public employees.

As a part of the 2018–2021 National Cyber and Information Security Strategy, the Agency for Digitisation has developed the website sikkerdigital.dk, which offers citizens guidance, articles and learning tools on cyber and information security and knowledge on different threats. In addition to the website, the Agency for Digitisation runs national campaigns on secure digital behaviour in cooperation with municipalities and regions.

Denmark also has a public-private Cyber Security Council, which was established to advise the Government on how to strengthen cybersecurity and improve knowledge-sharing among authorities, businesses and researchers. With the 2018–2021 Danish National Cyber and Information Security Strategy, 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 Tech Ambassador's Office in Silicon Valley; and joining the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence in Tallinn. This has allowed Denmark to step up its engagement in multilateral cyberforums such as the United Nations, the European Union, NATO and the Organization for Security and Cooperation in Europe (OSCE).

The Government of Denmark is currently working on a new national cyber and information security strategy for 2022–2024. The strategy will build on and expand current efforts by further strengthening cyber and information security through initiatives targeting the public and private sectors and Danish citizens.

At the same time, Denmark is maintaining engagement in countering hybrid threats such as cyberattacks and influencing operations through collaboration with its partners and allies in NATO and the European Union. The increase in attacks and operations during the coronavirus disease (COVID-19) pandemic has led to sustained diplomatic efforts within the United Nations, the European Union, NATO and OSCE, in order to consistently promote a free, open, stable, peaceful and secure cyberspace. Furthermore, Denmark is an active member of the NIS Cooperation Group and the network of Computer Security Information Response Teams and is a member of the board of the European Union Agency for Cybersecurity.

Denmark stresses that, as the international community has made clear, cyberspace is firmly rooted in existing international law, as the 2013 and 2015 consensus reports of the Groups of Governmental Experts have attested. 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 and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible information and communications technology (ICT) environment. Denmark furthermore stresses the importance of the 11 voluntary non-binding norms for responsible State behaviour articulated in the 2015 Group of Governmental Expert report as complementary to and deriving from existing international law.

Despite national and international 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.

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

Existing and emerging threats

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 and vulnerabilities.

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

Never before has the need for a global, free, open, secure, stable and peaceful cyberspace been more evident than during the COVID-19 pandemic. 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, and cyberenabled theft of intellectual property. Any attempt to hamper the ability of critical infrastructures is unacceptable and can put people's lives at risk. Denmark is particularly alarmed by the recent increase in activities affecting the security and integrity of ICT products and services, which might have systemic effects. 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 territory.

In addition, as recognized in previous reports of the Group of Governmental Experts and the Open-ended Working Group, given the unique character of ICTs, the approach taken by the United Nations and its Member States to addressing cyberissues 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.

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

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

The international community has made it clear that cyberspace is firmly rooted in existing international law, as the 2013 and 2015 consensus reports of the Groups of Governmental Experts also attest. 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. Denmark is pleased that the General Assembly concluded this by consensus earlier this year with the endorsement of the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Now all Member States have to live up to the commitment.

Sovereignty, non-intervention and the prohibition of the use of force are fundamental principles of international law and States' violation thereof may 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, as well as other international and regional initiatives such as a new programme of action to advance responsible State behaviour in cyberspace, in pursuing this outcome.

Importantly, the principle of sovereignty should not be used by States to limit or violate international human rights law within their 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 violating 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 where military leaders are obliged 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 report of the Group of Governmental Experts, 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 existing international law applies in cyberspace, 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 existing international law applies to cyberissues. Hopefully, the work and recommendations of the current Group of Governmental Experts and the new Open-ended Working Group will contribute to further clarifications and thus facilitate State compliance as well as promote greater predictability and reduce the risk of escalation.

Norms, rules and principles for the responsible behaviour of States

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

As complementary to and deriving from existing international law, the norms, rules and principles of responsible State behaviour articulated through successive reports of the Groups of Governmental Experts 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.

Republic of Moldova

[Original: English]
[24 May 2021]

Information technologies, informational resources and electronic communication systems have become an indispensable part of all fields of activity of a person, society and State. Information technologies contribute to the essential transformations of social order and serve as a generator for a consolidated informational society on the national, regional and international levels. Therefore, information technologies have overcome the legal framework of State borders or State communities.

Beside the incontestable benefits of modern technologies, the informational space is liable to several security threats. Thus, it facilitates disloyal competitiveness, espionage, mass misinformation, propaganda, terrorism and organized crime, spreading forms of hate and the incitement of violence, especially on the criteria of gender, race, nationality, ethnic origin, language, religion, political affiliation and other criteria, which remain underestimated and rarely remediated or countered.

An increased information security level and the creation of favourable conditions for certain activities of both public and private actors, including for simple users of the information systems, are the basic priorities for national policy to ensure the information security of a State of law. The achievement of these actions implies the existence of an updated and comprehensive regulatory framework, which would cover the main issues in the informational security field. In this respect, in the Republic of Moldova, the Strategy for Informational Security and the Activity Plan for its implementation have been approved. Therefore, the purpose of the Strategy is to ensure the protection of fundamental rights and freedoms, democracy and rule of law in the informational space.

The classification of risks, threats and vulnerabilities, as well as the systematization of activities ensuring informational security, contribute to an increased trust level in cyberspace, a fact that is reflected in the Strategy for Informational Security of the Republic of Moldova.

The aim of the Strategy is to legally correlate and systemically integrate the priority fields with responsibilities and competences to ensure informational security on the national level based on cyberresilience, multimedia pluralism and institutional convergence in the security area with the aim of protecting the sovereignty, independence and territorial integrity of the Republic of Moldova.

Thus, the Strategy provides concrete and clear mechanisms for identifying, counteracting and responding to informational security threats, as well as the deadlines for achieving the objectives for its implementation.

The mechanisms and objectives included in the Strategy are oriented towards the creation and updating of the normative framework and the implementation of the technical performance and programme components that will confront the challenges from within and outside the country, staff training and intensifying cooperation with national and international competent bodies.

In this regard, the Strategy provides for the creation of an integrated communication and evaluation system for the informational security threats and the elaboration of operative response measures. This involves the creation/designation of an entity as a national cybersecurity incidents response centre that would be the single point for reporting cybersecurity incidents for competent public authorities, individuals and legal entities. The creation of a national computer emergency response team would strengthen the team network on the territory of the Republic of Moldova and ensure a fast response to incidents.

In addition, considering the necessity of constantly monitoring and ensuring a high cybersecurity level, the Strategy provides for the implementation of an audit of informational technology infrastructures of national interest and the implementation of international standards for informational security.

Moreover, the Strategy provides protection mechanisms for the Republic of Moldova's special communication networks and for restricted-access information. The communication systems, informational systems and data-transmission networks are designed for the storage, processing and further transmission of important data for the State, thus requiring a specific approach in terms of their protection and development.

The increasing number of cryptographic protection means and the complexity of cryptographic algorithms make it necessary to ensure control over the import, certification and use of information protection means. Therefore, the Strategy requires the certification of technical and cryptographic information protection means, the development of import monitoring systems of information protection means, the alignment of the national legal framework in the field of cryptographic information protection with the European legal framework and the creation of a database on technical and cryptographic information protection means.

Furthermore, the free access to the Internet global network, the existence of data of pornographic and extremist character, along with the difficulty of establishing the source and veracity of the uploaded data make it necessary to develop protection mechanisms for users, especially children, against any form of abuse in the online space.

An evaluation of the Internet space aimed at identifying the entities and/or individuals involved in the production and dissemination of online media content with an impact on the informational security of the Republic of Moldova was necessary in order to identify, counteract and respond to informational security threats in the informational media space.

Also, in order to develop strategic communication mechanisms, promote the national interests of the Republic of Moldova and ensure the security of the informational media space, the Strategy provides for the realization of a comprehensive study aimed at detecting and evaluating the vulnerable elements of the media component within the informational security system, as well as the creation of an informational resource for strategic communication containing information on security incidents and on detected disinformation and/or manipulation attempts.

Furthermore, it is worth mentioning that the Strategy contains objectives that are necessary for international cooperation in the field of informational security and counteracting cybercrimes.

The Strategy for Informational Security was approved for the period from 2019 to 2024 and sets out a number of objectives and measures to be gradually achieved, including with the assistance of international partners.

Despite the fact that on the national level, the Republic of Moldova is trying to implement several measures to consolidate its informational security capacities, we assess that on the international level, the situation in cyberspace is becoming more and more complex, with malicious State actors conducting sophisticated cyberattacks to interfere in the electoral processes of other countries, damaging critical infrastructures and carrying out cyberespionage attacks of the “supply chain” type, all of which are contrary to United Nations resolutions.

At the same time, non-State cyberactors fully exploit informational system vulnerabilities for criminal purposes in order to obtain financial gains, using “Malware-as-a-Service” instruments.

The above-mentioned issues cause the population to be reluctant towards new technologies and represent an impediment to the good development of informational technologies.

Singapore

[Original: English]
[24 May 2021]

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, open and interoperable cyberspace 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 and multilateral forum where all States have an equal voice.

Singapore participated in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security for the period from 2019 to 2021 and the recently concluded Open-Ended Working Group established pursuant to General Assembly resolution 73/27. We remain committed to contributing constructively to the United Nations work to develop and implement norms and rules on cybersecurity and will continue to participate actively in future United Nations processes. In our view, it is important for future cybersecurity discussions at the United Nations to take into account a wide range of views, especially from small States and developing countries that are particularly vulnerable to the effects of cyberconflict. To this end, any future United Nations process on cybersecurity should be open, inclusive and collaborative to further strengthen international cooperation and make progress on advancing responsible State behaviour in cyberspace. As a co-chair of the Group of Friends on e-Governance and Cybersecurity with Estonia, Singapore will continue to use this platform to raise awareness of cyberchallenges, share best practices and promote capacity-building at the United Nations.

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, cross-border critical information infrastructure, of which their protection is the shared responsibility of all Member States, could be considered a special category of such critical infrastructure and should be included in the existing set of norms, as ICT threats to such infrastructure could have destabilizing effects regionally and globally.[2]

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, participants in the third ASEAN Ministerial Conference on Cybersecurity decided to subscribe in principle to the 11 norms in the 2015 report of the Group of Governmental Experts, as well as to focus on regional capacity-building in implementing these norms. In October 2019, participants in 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. Participants in the fifth ASEAN Ministerial Conference on Cybersecurity, held in 2020, reiterated the commitment of ASEAN to develop an action plan to chart the implementation road map for the norms at an appropriate pace for all ASEAN member States. Participants also agreed on the urgent need to protect national and cross-border critical information infrastructures.

Capacity-building is essential to ensure that individual States develop the ability to successfully implement the norms of responsible State behaviour and their obligations under international law. As part of this effort, Singapore established the

[2] Cross-border critical information infrastructures are critical information infrastructures owned by private companies and operating across national borders, but not under any single State’s jurisdiction.

ASEAN Cyber Capacity Programme in 2016 to support capacity-building in ASEAN countries on cyberpolicy, as well as operational and technical issues. To date, the ASEAN Cyber Capacity Programme has trained more than 600 officials from ASEAN member States. As an extension of the Programme, the ASEAN-Singapore Cybersecurity Centre of Excellence was launched in 2019 with a commitment of $30 million to offer policy and technical programmes for senior ASEAN officials. The Centre of Excellence has been operational since April 2020. Notwithstanding the travel restrictions due to the COVID-19 pandemic, the Centre of Excellence continued its training programmes online and organized seven virtual capacity-building programmes in 2020.

Singapore also co-organized a workshop under the United Nations-Singapore cyberprogramme to build awareness of cybernorms among ASEAN member States. In addition, Singapore partnered with the Office for Disarmament Affairs to develop a flagship online training course open to all United Nations Member States. The course is aimed at promoting greater understanding of the use of information and communication technologies and their implications for international security. We remain committed to sharing our experience and expertise with United Nations Member States, especially small developing countries.

At the national level, Singapore has continued to strengthen the cybersecurity of its systems and networks on three fronts, namely, building a resilient infrastructure, creating a safer cyberspace and developing a vibrant cybersecurity ecosystem.

(a) *Building a resilient infrastructure*. The Cyber Security Agency of Singapore launched the Operational Technology Cybersecurity Master Plan in 2019 as part of our efforts to enhance the security and resilience of Singapore’s critical information infrastructure sectors in delivering essential services. The Master Plan is aimed at improving cross-sector response to mitigate cyberthreats in the operational technology environment and strengthen partnerships with industry and stakeholders by outlining key initiatives covering the areas of people, processes and technology to enhance the capacities of our critical information infrastructure owners and organizations that operate operational technology systems. In 2021, the Cyber Security Agency will develop and launch a critical information infrastructure supply chain programme, involving stakeholders including government agencies, critical information infrastructure owners and their vendors. The programme would provide recommended processes and sound practices for all stakeholders to manage cybersecurity risks in the supply chain;

(b) *Creating a safer cyberspace*. As part of our efforts to raise the national cybersecurity posture in Singapore, the Cyber Security Agency launched the Safer Cyberspace Master Plan in 2020 to: (i) secure our core digital infrastructure; (ii) safeguard our cyberspace activities; and (iii) empower our cybersavvy population. The Master Plan outlines 11 initiatives aimed at increasing the adoption of security-by-design amongst enterprises and organizations as well as enhancing cybersecurity awareness and good cyberhygiene practices amongst end users. One of these initiatives is the Cybersecurity Labelling Scheme for network-connected smart devices. The Cybersecurity Labelling Scheme was launched in 2020 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 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 cyberecosystem 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. The Cyber Security Agency has worked with government agencies, associations, industry partners and academia in Singapore to expand and develop the cybersecurity workforce. The SG Cyber Talent initiative is aimed at attracting and nurturing talented cybersecurity enthusiasts from a young age and helping cybersecurity professionals deepen their skills. It aims to reach out to at least 20,000 individuals over three years to strengthen the cybersecurity talent pipeline in Singapore.

Switzerland

[Original: English]
[28 May 2021]

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

Switzerland has adopted a range of measures at the national, regional and global levels designed to advance a more stable, open and free cyberspace.

The Swiss Foreign Policy Strategy 2020–2023[3] sets out the broad outline and priorities, including Switzerland's continued engagement for an open and secure digital space that is based on international law and revolves around people and their needs. Switzerland is also committed to bolstering Geneva's position as a leading global digital hub. Switzerland's first Digital Foreign Policy Strategy 2021–2024[4] builds on the Foreign Policy Strategy and sets out key principles aimed at guaranteeing an open, free and secure digital space.

The second National Strategy for the Protection of Switzerland against Cyber Risks 2018–2022 builds upon the strategic objectives outlined in the first National Strategy for the Protection of Switzerland against Cyber Risks of 2012.[5] Both strategies acknowledge the importance of information and communication technologies (ICTs) as indispensable drivers of social, economic and political activities and lay the foundation for a comprehensive, integrated and holistic approach to address ICT-based threats. Switzerland seeks to improve its early detection of cyberrisks and emerging threats, increase the resilience of its critical infrastructure and generally reduce cyberrisks. The underlying rationale of the strategies is the need for a cybersecurity culture, shared responsibility between different levels of government and between the public and the private sectors, as well as the need for a risk-based approach. They advocate stronger coordination at the governmental level and foster private-public partnerships and enhanced cooperation in the international arena. Cooperation, whether at the national or international level, was defined as one of the cornerstones of the Swiss approach to tackling cyberthreats. The National Cyber Security Centre was established in 2019 and serves as the point of contact for businesses, academia, the general public and governmental agencies. Led by the Federal Cybersecurity Delegate, the Cyber Security Centre also helps increase cybersecurity awareness.

[3] Available at www.eda.admin.ch/eda/en/fdfa/foreign-policy/implementing-foreign-policy/aussenpolitischestrategie.html.

[4] Available at www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2020/11/digitalaussenpolitik-strategie.html.

[5] Available at www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html.

In September 2020, the Federal Council adopted the new Digital Switzerland Strategy.[6] It identifies a number of action fields for cooperation among government, academia, the private sector and civil society in order to shape the digital transformation of our society to the benefit of everyone in Switzerland and to ensure that the opportunities it presents are available to all.

In March 2021, the Federal Department of Defence adopted its Cyber Defence Strategy 2021–2024.[7] The strategy is aimed at anticipation and early detection of cyberthreats and malicious activity, prevention and attribution of cyberincidents targeting Swiss interests and education and training of civilian and military staff, as well as the cyberresilience of critical infrastructures.

With regard to the protection of critical infrastructures, Switzerland pursues a decentralized approach. The mandate pertaining to the protection of critical infrastructures is assigned to various Federal Departments and Offices such as the Federal Office for Civil Protection, the Federal Office for National Economic Supply and the Federal Intelligence Service and is therefore not limited to one agency.

Since the adoption of the National Strategies for the Protection of Switzerland against Cyber Risks, capacities designed to attribute malicious cyberactivities to perpetrators have been further developed. The identification of perpetrators is a holistic approach that includes the analysis of technical characteristics of a cyberincident, takes into account the geopolitical context and uses the entire intelligence spectrum to obtain relevant information. Switzerland has defined an inter-agency standardized process to attribute publicly (political attribution) a cyberincident that poses a threat to Switzerland's national security. The criteria for a legal attribution of a cyberincident according to international law form part of this assessment.

In January 2019, Switzerland established a "Cyber Defence Campus"[8] that undertakes research to anticipate and monitor possible threats stemming from technologically driven developments, proposes solutions and trains cyberexperts. The Campus brings together experts from the Federal Office for Defence Procurement, industry and research institutions.

With respect to outreach and engagement with the private sector and academia, Switzerland fosters various initiatives. For example, in order to counter espionage and proliferation activities, the Federal Intelligence Service has used, since 2004, its prevention and awareness campaign programme "Prophylax" to advise companies, universities and research institutes on possible preventive measures to identify and respond to illegal espionage and proliferation activities.

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

Regarding threat assessment, malicious cyberactivities directly targeting critical infrastructures can cause severe damage and have a negative impact on the functioning of essential services, such as health care. In recent years, several Swiss federal agencies and private companies have been victims of State-sponsored malicious cyberactivities (cyberespionage). The ultimate goal of these malicious cyberactivities is generally to gain economic, political and military advantages. In the course of 2020, Swiss critical infrastructures were affected mainly by financially motivated attacks. In the future, Switzerland expects an increase in ransomware attacks by criminal groups as well as cyberoperations conducted, sponsored or

[6] Available at www.digitaldialog.swiss/en/.

[7] Available at www.newsd.admin.ch/newsd/message/attachments/66203.pdf.

[8] See www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

condoned by States. Furthermore, malicious cyberactivities can have unintended effects on Switzerland and result in collateral damage. As threat actors continue to develop techniques and tools to undermine and manipulate legitimate software, attacks on the supply chain are of particular concern.

Switzerland actively participated and contributed to the sixth Group of Governmental Experts (2019 to 2021) and the Open-Ended Working Group (2019 to 2021) pertaining to international cyberstability and aiming to strengthen the implementation of the United Nations framework for responsible behaviour of States in cyberspace. Switzerland is convinced that the application of international law, including human rights law and international humanitarian law, voluntary non-binding norms, confidence-building measures and capacity-building are key to ensuring and maintaining international cybersecurity. The Permanent Representative of Switzerland to the United Nations in New York chaired the Open-ended Working Group. Under his chairship, the Group agreed on a consensus outcome report in March 2021 (A/75/816).

Switzerland is engaged with the International Telecommunications Union, in particular in its consultations on the guidelines for the utilization of the Global Cybersecurity Agenda, with the aim of building coherence with other processes at the United Nations level.

Switzerland is committed to advancing the role of the Organization for Security and Cooperation in Europe (OSCE) in promoting cyberstability and actively participates in its informal working group on cybersecurity. Since the establishment of the OSCE mandate to develop and implement confidence-building measures, Switzerland has increased transparency on its own cyberposture by sharing information on national structures, organizations and policies at the regular informal working group meetings, through platforms maintained by OSCE and the OSCE Communications Network. Together with Germany, Switzerland has also continued its engagement to operationalize the information and consultation mechanism enshrined in confidence-building measure No. 3.

Switzerland is a State party to the Council of Europe Convention on Cybercrime and considers its implementation and practical application as crucial in the fight against cybercrime. Switzerland is participating in the negotiations on a second additional protocol to the Convention, which is aimed at enhancing international cooperation.

Bilaterally, Switzerland holds regular political consultations with countries on cyberrelated issues.

Switzerland joined the Freedom Online Coalition in 2019 as its thirty-first member. Switzerland strongly believes that the same rights that people have offline must also be protected online. The Freedom Online Coalition is a key initiative to strengthening engagement among all stakeholders in order to protect human rights and fundamental freedoms in the Internet age. Switzerland also supports the efforts of the Freedom Online Coalition financially.

In 2019, Switzerland launched a legal expert dialogue on how international law applies in cyberspace. In 2021, Switzerland will continue this effort to foster common understanding of how international law applies, with a focus on the application of international humanitarian law in cyberspace.

In 2018, Switzerland launched the Geneva Dialogue on Responsible Behaviour in Cyberspace, which provides a multi-stakeholder platform for discussions on the roles and responsibilities regarding international cyberstability. Since 2020, the Geneva Dialogue has been focusing on the role of businesses in implementing the norms agreed at the international level.

The National Cyber Security Centre has recently initiated an inter-agency process to formulate a whole-of-government approach to disclose newly identified cybervulnerabilities in a coordinated and responsible manner. This process enables researchers who disclose a vulnerability in hardware, software and digital services to report it to the Centre. The disclosure is aimed at mitigating the vulnerability (for example, patching) before the vulnerability can be exploited for malicious purposes.

Switzerland participates in a range of national and international exercises, such as Locked Shields, to test national capacities, procedures and decision-making processes.

Switzerland is a founding member of the Global Forum on Cyber Expertise and supports various cybercapacity-building projects. Switzerland also financially supports initiatives aimed at strengthening the capacity of diplomats as well as non-governmental representatives to participate and contribute to the relevant United Nations processes on international cyberstability.

Turkey

[Original: English]
[31 May 2021]

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, ICTs play an important role in sustainable growth and development. However, the more we use technology, the more we become dependent on it and vulnerable 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 the 2013–2014 action plan and the 2016–2019 national cybersecurity strategy and action plan were published and implemented. Turkey has developed its national cybersecurity strategy and action plan 2020–2023 with the participation of all relevant stakeholders in study groups coordinated by the Ministry of Transport and Infrastructure.

The national cybersecurity strategy and action plan 2020–2023 was published in the Official Gazette on 29 December 2020, and includes the following main strategic objectives:

- Critical infrastructure protection and increasing resilience
- National capacity-building
- Organic cybersecurity network
- The security of new generation technologies (Internet of things, 5G, cloud computing etc.)
- Fighting against cybercrime
- Developing and fostering domestic and national technologies
- Integration of cybersecurity into national security
- Improving international cooperation

Furthermore, the National Computer Emergency Response Team, 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 incidents, the team ensures the implementation of preventive measures against cyberthreats and cyberdeterrence.

The main focus areas relating to cybersecurity of the National Computer Emergency Response Team are:

- Cyber capacity-building
- Technological measures
- Gathering and disseminating threat intelligence
- Protection of critical infrastructure

In the context of improving national cybersecurity, 14 sectoral computer emergency response teams for critical sectors or infrastructures (such as energy, health, banking and finance, water management, electronic communications and critical public services) and 1,803 institutional computer emergency response teams have been established since 2013. All computer emergency response teams operate 24 hours a day, seven days a week, under the coordination of the national team, in order to mitigate cyberrisks and fight against cyberthreats. The National Computer Emergency Response Team uses detection and prevention tools for monitoring, and reporting tools for information-sharing with relevant parties. The National Computer Emergency Response Team developed the information-sharing platform for all computer emergency response teams within Turkey in order to distribute alarms, warnings and security notices, which provides an efficient and secure communications channel.

The National Computer Emergency Response Team organizes and supports training courses, summer camps and competitions on cybersecurity open to several communities. In addition, the national team provides training to computer emergency response teams on topics such as malware analysis and log analysis. More than 5,000 people have been trained in different areas of cybersecurity by the national team over the past four years.

In addition, the Academy established within the Information and Communication Technologies Authority provides online training open to the public on cybersecurity and other related areas in order to contribute to increased expertise within Turkey's human resources. The training content is available on the Academy's official web portal (www.btkakademi.gov.tr/portal).

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

The annual Safer Internet Day is among the awareness-raising activities, and its main objective is 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, is publicly available on the official safe web portal (www.guvenlinet.org.tr/).

Turkey also takes steps to counter heightened digital security risks to ensure cybersecurity and takes measures within the scope of the coronavirus disease (COVID-19) pandemic.

Malware, phishing attacks and other cyberthreats exploiting the trends of the COVID-19 pandemic are analysed by the National Computer Emergency Response Team, which operates 24 hours a day, seven days a week. Through command and control centres, malicious links of these cyberthreats are determined and prevented in order to protect critical infrastructures and citizens. Within this scope, cyberintelligence reports are prepared and shared with relevant parties. Guidelines have also been prepared and published, including on the following:

- Security principles for remote connections
- Protecting users from phishing attacks
- Fake applications related to COVID-19
- Security principles for setting up and using videoconferencing and meeting software

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 gives importance to information-sharing with different countries and organizations in a large range of areas. The National Cyber Emergency Response Team 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, the Cybersecurity Alliance for Mutual Progress and the Computer Emergency Response Team of the Organization of the Islamic Conference. 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 in and contributor to the studies of international organizations such as the United Nations, NATO, the Organization for Security and Cooperation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the Group of 20, the Cooperation Council of Turkic-speaking States and the Regional Arms Control Verification and Implementation Assistance Centre - 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. Cyber Shield 2019 was supported by ITU and the Cybersecurity 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. 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.

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 Groups of Governmental Experts, the Open-ended Working Groups and in related studies contribute to safer cyberspace.

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

Furthermore, Turkey is aware of the importance of the implementation of international law, the norms of responsible State behaviour in cyberspace and the need for effective international cooperation. Turkey takes the necessary steps with determination to ensure these goals are achieved, and strengthening cybersecurity at the national and international levels will remain one of its key priorities.

Ukraine

[Original: English]
[31 May 2021]

An analysis of the available information shows that, in the conditions of "hybrid" war against our State, one of the main threats to national security is the Russian Federation's destructive information and psychological special operations aimed at undermining the constitutional order, violating the sovereignty and territorial integrity of Ukraine, and aggravation of the sociopolitical and socioeconomic situation in our country. Purposeful dissemination of disinformation and fake information, along with armed aggression, has become an urgent threat not only to Ukraine, but also to the whole world, as it affects the consciousness of citizens of other countries, creates a distorted image of Ukraine and forms public opinion beneficial only to Russia.

The aggressor State is increasingly taking measures aimed at reducing the level of information security of our State, creating levers of influence over State institutions and information space in order to strengthen its own position, forming a favourable foreign opinion and exerting pressure on Ukrainian State institutions to make decisions in its favour. To that end, promotion is carried out in the Ukrainian information and media space, on a systematic basis, and on the Internet, including through social networks, messengers, electronic resources and specially prepared information products, especially of a misinforming nature.

In order to implement this negative informational influence on our country, the Russian Federation has created a powerful system for promoting propaganda content, which includes a network of information platforms (blogs, sites), controlled media and Internet resources, aggregators and news concentrators, bloggers and opinion leaders for publishing content, news agencies and public relations companies to display propaganda messages in top news feeds. There is also widespread use by Russia of bot networks to quickly spread misinformation and anti-Ukrainian messages aimed at manipulating the mass consciousness. The key subjects of the information space used by the Russian side to spread misinformation are the world's leading social networks (Facebook, Instagram, Twitter), whose rapid audience growth has occurred owing to the ban in Ukraine of the Russian social networks VKontakte and Odnoklassniki. There is a tendency to reorient users of the Ukrainian segment of the Internet towards the widespread use of messaging services (Telegram, WhatsApp, Viber, etc.), owing to the possibility of maintaining anonymity, efficiency of placement and further mass distribution of content, and high levels of interactivity and feedback.

Video hosting services (YouTube, Yandex.Video, RuTube, Video@Mail.Ru) are also used to spread misinformation, as the companies that own photo and video hosting services operate under the laws of the countries in the territory where they are located. This is used by Russian propagandists to create and post content on these web platforms that poses a threat to Ukraine's information security. Owing to the fact that the source of such messages is United States and European hostings, the content is freely distributed on the Internet.

In addition, the aggressor country is making efforts to constantly develop a network of controlled information resources. In particular, the occupation administrations in the temporarily occupied territories of our State are taking systematic measures aimed at creating new information platforms, increasing the number of television channels and expanding the coverage area of television and radio broadcasting, including in the territories controlled by the Ukrainian authorities. In addition to the distribution of anti-Ukrainian content, powerful retransmission equipment installed by the Russian occupation authorities is used to suppress the signal of domestic television and radio broadcasting by disseminating so-called "white noise" on the frequencies that are used by the Ukrainian side to convey objective information to the residents of temporarily occupied territories. This is especially relevant in terms of the coding by the largest media groups in the country (Inter Media Group, StarLightMedia, Media Group Ukraine, 1 + 1) of the satellite signal of their television channels and the unsatisfactory state of coverage of the territory of Ukraine by national television and radio broadcasting in digital standard. As a result, residents of border areas of Ukraine are under the constant influence of destructive content from the main propaganda channels of the Russian Federation. Another factor of negative influence, which complicates the delivery of positional content to the residents of the temporarily occupied territories of Ukraine, is the operation of operators and providers of the temporarily occupied territories, which limit the access of the local population to the Ukrainian segment of the Internet. Thus, in violation of European law, registration of IP addresses for the work of so-called Internet providers in Crimea and in occupied areas of Donbass is provided by the non-profit organization RIPE NCC (Netherlands). In order to bring the activities of this organization into line with the current legislation of Ukraine, the Ministry of Foreign Affairs of Ukraine and the Embassy of Ukraine in the Kingdom of the Netherlands are taking appropriate measures at the inter-State level.

There are also cases of the Russian Federation using Apple and Google services to spread misinformation in order to manipulate users of the Ukrainian segment of the Internet. In particular, in the App Store and the Play Market, there are mobile applications developed by legal entities and persons in respect of whom special economic and other restrictive measures (sanctions) have been applied in accordance with the Decision of the National Security and Defence Council of 14 May 2020 on the application, cancellation and amendment of personal special economic and other restrictive measures (sanctions), enacted by Decree No. 184/2020 of the President of Ukraine of 14 May 2020. These software products in their functionality have the technical ability to provide access to the web resources banned in Ukraine.

Despite all the efforts of our State to strengthen information security and block the spread of misinformation, as one of the biggest threats in the information sphere, there is an urgent need to assist the world community and international institutions in adequately counteracting information aggression by the Russian Federation, not only against Ukraine, but also in relation to other countries, from the position of which it conducts actions of destructive influence in the information space.

Until recently, the destructive informational influence of the Russian Federation, its attempts to interfere in the internal affairs of our State and its attempts to impose its conditions in the implementation of international cooperation and domestic processes were carried out through affiliated Ukrainian political parties and movements, direct covert funding of civic institutions and economic entities operating on the territory of our State, forceful pressure through military aggression in eastern Ukraine or blocking international support and Ukraine's accession to the European Union and the North Atlantic Treaty Organization (NATO), and conducting information campaigns, operations and actions through controlled information resources.

However, there is a steady tendency towards reorientation by the Russian Federation of further strategy of so-called “information war” against Ukraine in the direction of concealing its participation in the organization and conduct of destructive measures against our State by implementing them from the position of the so-called “third” countries. On the one hand, this is happening as a result of the economic sanctions imposed by the European Union and the United States against the Russian Federation for interference in Ukraine’s internal affairs, annexation of the Autonomous Republic of Crimea and armed conflict in the temporarily occupied territories of Donetsk and Luhansk regions. On the other hand, it is also due to the measures taken by the Ukrainian side to combat the destructive influence of the aggressor country over the Ukrainian information space and the consciousness of citizens, to mitigate the negative consequences of the messages spread and to increase the level of patriotism and self-consciousness of the population of our State.

In particular, there is an increase in actions of informational influence and facts of interference in the internal affairs of Ukraine. Intelligence and subversive activities are being conducted by the Russian Federation from the standpoint of NATO and European Union member States, which consist of creating and financing lobbyists for Russian interests in State and local authorities and management, political parties and movements, the expert and blogging community, think tanks, advertising and consulting companies, donors, non-governmental organizations and public opinion leaders, as well as through the creation of controlled media, Internet resources and public relations companies.

Owing to pro-Russian European politicians in the so-called “Russian world” cells in the European Union, the Russian Federation is trying to legalize and impose on the world community the idea of the legitimacy of the Crimean plebiscite, justify its armed aggression against Ukraine and consequently achieve the lifting of anti-Russian sanctions and its return to the world political establishment. Currently, pro-Russian branches are active in some European States. Most of the representatives of these political forces, being lobbyists for the interests of the aggressor country both inside and outside their country, propagate pro-Russian views, disseminate Russian narratives and take informational measures that threaten Ukraine’s national interests.

The reorientation of the Russian Federation towards the organization and conduct of special information operations and actions of destructive information influence from the standpoint of “third” countries is manifested in inspiring historical contradictions and territorial claims of other States to Ukraine and provoking separatist and autonomous manifestations among national minorities in Ukraine. On the one hand, this complicates relations between our State and neighbouring countries, from the position of which the Russian Federation carries out such destructive activities, and on the other hand, it becomes a reason for these countries to declare their territorial claims to certain Ukrainian lands. At the same time, by officially distancing itself from this process, Russia avoids direct accusations from Ukraine and the world community of interference in the internal affairs of our State, and directly threatens Ukraine’s good neighbourly relations with other States, to form positions of influence over the domestic political situation in Ukraine.

In view of the above, Ukraine will continue to take comprehensive measures to ensure responsible behaviour in cyberspace in the context of international security, while at the same time calling for the support of the world community and joint efforts to properly counter the Russian Federation’s “hybrid” war.

In order to ensure the implementation of the reform of electronic digital signature legislation through harmonization with the provisions of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EU of the European Parliament and of the Council, the Verkhovna Rada of Ukraine adopted Law No. 2155-VIII on electronic trust services on 5 October 2017, which entered into force on 7 November 2018.

The main purpose is to introduce in Ukraine the models and principles for the provision of electronic trust services used in the European Union, without destroying the system of interaction between the parties in the field of electronic digital signature that has developed in Ukraine. The law defines the legal and organizational principles of providing electronic trust services, including cross-border services, the rights and obligations of the subjects of relations in the field of electronic trust services, the procedure for State supervision (control) of compliance with legislation in the field of electronic trust services, and legal and organizational principles of electronic identification. In developing the provisions of Law No. 2155-VIII, the Cabinet of Ministers of Ukraine adopted a number of resolutions:

- No. 749 on approval of the procedure for the use of electronic trust services in public authorities, local governments and State-owned enterprises, institutions and organizations, adopted by the Cabinet of Ministers of Ukraine on 19 September 2018.

- No. 775 on approval of mandatory requirements in respect of the Reference List, adopted by the Cabinet of Ministers of Ukraine on 26 September 2018.

- No. 821 on approval of the procedure for storage of documentary information and its transfer to the central management body in case of termination of activities of a qualified issuer of electronic trust services, adopted by the Cabinet of Ministers of Ukraine on 10 October 2018.

- No. 992 on approval of the requirements in the field of electronic trust services and the procedure for inspections of observance of the requirements of the legislation in the field of electronic trust services, adopted by the Cabinet of Ministers of Ukraine on 7 November 2018.

- No. 1215 on approval of the procedure for conformity assessment procedures in the field of electronic trust services, adopted by the Cabinet of Ministers of Ukraine on 18 December 2018.

- No. 60 on approval of the procedure for mutual recognition of Ukrainian and foreign public key certificates, electronic signatures and use of the information and telecommunications system of the central body responsible for ensuring recognition in Ukraine of electronic trust services and foreign public key certificates used during the provision of legally significant electronic services in the process of interaction between subjects of different States, adopted by the Cabinet of Ministers of Ukraine on 23 January 2019.

The Administration of Special Communications and Information Protection of Ukraine, in compliance with the requirements of article 8 of the law, by the order dated 14 May 2020 approved the requirements for the security and protection of information on qualified providers of electronic reference services and their separate registration points (registered with the Ministry of Justice of Ukraine on 16 July 2020), which detail and determine the implementation of the law and the requirements in the field of electronic trust services, approved by the Cabinet of Ministers of Ukraine on 7 November 2018 by means of resolution No. 992, to ensure the security and protection of information on providers of electronic trust services and separate registration points.

At present, Ukraine is taking measures aimed at mutual recognition of electronic trust services within the framework of the Association Agreement between Ukraine and the European Union and as a result of agreements reached between Ukraine and the European Union during the twenty-second European-Union-Ukraine Summit.

At the same time, it is necessary to revise some provisions of the law in order to align them as closely as possible with the provisions of Regulation (EU) No. 910/2014, in particular in terms of establishing State regulations in the field of electronic identification, the requirements for improved electronic signatures and seals, and clarification of the requirements for qualified electronic signatures or seals. A draft law that has been prepared by the Ministry of Digital Transformation and the Administration of Special Communications and Information Protection of Ukraine is currently under consideration by the Cabinet of the Ministers of Ukraine.

In addition, by means of resolution No. 24 of 13 January 2021, the Cabinet of Ministers of Ukraine amended paragraph 4 of the Regulations on the Administration of the State Service for Special Communications and Information Protection of Ukraine, which manages the State Special Communications Administration, and established the functions of the Secure Accreditation Body instituted in accordance with article 7 on administrative arrangements for the protection of restricted-access information between the Government of Ukraine and NATO, ratified by Law No. 2068 of 24 May 2017.

The Administration of Special Communications and Information Protection of Ukraine, through the establishment of a national accreditation procedure for the security of the communication and information system intended for the exchange of NATO restricted-access information, takes measures to implement NATO regulations on these issues.

As part of promoting international cooperation and raising the awareness of information security professionals, the Administration of Special Communications and Information Protection of Ukraine participates in international conferences of the Technical Assistance and Information Exchange instrument of the European Commission (TAEIX) and FireEye seminars.

With the aim of strengthening information security, an information security audit system is continuously being introduced at critical infrastructure facilities, as follows:

- Formation of requirements for independent information security auditors at critical infrastructure facilities.
- Development of the procedure for certification/re-certification of information security auditors, as well as of a system of special purpose assessment of professional training for information security auditors and analysis of the results of the independent information security audit at the critical infrastructure objects of ITS “Audit”.

At the same time, in order to implement the State policy in the field of information protection, the staff of the Administration of Special Communications and Information Protection of Ukraine carry out measures of national control over the state of the technical protection in cyberspace of State information resources and information as required by law.

Moreover, the Administration of Special Communications and Information Protection of Ukraine has taken a number of actions to prepare for and ensure the adoption of the following acts:

– It prepared thorough proposals for the draft cybersecurity strategy of Ukraine (2021–2025) in accordance with article 107 of the Constitution of Ukraine, part two of article 2 of the law on fundamentals of national security and Decree

No. 391/2020 of the President of Ukraine on the decision of the National Security and Defence Council of 14 September 2020.

– It provided support for the adoption of resolution No. 518 of 19 June 2019 by the Cabinet of Ministers of Ukraine on approval of the general requirements for the cyberprotection of critical infrastructure, which was initiated within the framework of the formation and implementation of State policy on the cyberprotection of critical information infrastructure and aimed at achieving compatibility with the relevant European Union and NATO standards, as well as the creation of a regulatory and terminological framework on cybersecurity and harmonization of regulations in the field of information security and cybersecurity in accordance with international standards.

– The Cabinet of Ministers of Ukraine adopted resolution No. 1109 on some issues of critical infrastructure facilities and resolution No. 943 on some issues of critical information infrastructure facilities, which were developed taking into account the requirements of European Union legislation, in particular Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems in the Union, and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

– On 11 November 2020, the Cabinet of Ministers of Ukraine adopted resolution No. 1176 on approval of the procedure for reviewing the status of cyberprotection of critical information infrastructure, State information resources and information as required by law, which allows for the regulation of information infrastructure, State information resources and information whose protection is required by law.

The Computer Emergency Response Team of Ukraine constantly takes measures to cooperate with foreign teams to address issues related to overcoming the effects of cyberattacks on critical information infrastructure, analyses data on cyberincidents, provides owners of cybersecurity facilities with practical assistance in preventing, detecting and eliminating the consequences of cyberincidents, prepares and publishes recommendations for combating modern types of cyberattacks and cyberthreats on its official website and provides information on cyberthreats and appropriate methods of protecting against them.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[31 May 2021]

The United Kingdom welcomes the invitation to inform the Secretary-General of its views and assessments on issues pertaining to advancing responsible State behaviour in cyberspace in the context of international security, as detailed in General Assembly resolution 75/32. We encourage all States participating in discussions relating to developments in the field of information and telecommunications in the context of international security to take advantage of this and subsequent opportunities.

Cyberspace does not respect national boundaries. As a responsible cyberpower, the United Kingdom will work to shape the future frameworks that govern cyberspace, upholding existing rules and building consensus on positive norms of behaviour in a world fundamentally shaped by technology.

The United Kingdom recognizes that, over the coming decade, rapid technological change in areas such as artificial intelligence, cyber and data will reshape our societies. Countries must work together to tackle the biggest global challenges, including to promote a free, open, peaceful and secure cyberspace and act as a force for good in the world, defending democracy and human rights in our digital societies.

We will promote uptake and adherence to those rules and norms and we will work in concert with a full range of partners and stakeholders to assert a compelling case for a cyberspace that protects open societies and enables innovation, development and growth. We will also support those countries grappling with the challenges of digitalization – through international capacity-building – to build the confidence to engage with the international debate and to grow their cybersecurity capabilities.

The United Kingdom welcomes the successful conclusion of the concurrent United Nations processes, the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. The Open-ended Working Group has provided an inclusive process that represents the diverse views of all Member States and other stakeholders, while we believe that the report of the Group of Governmental Experts will provide the detailed guide to the initial framework for responsible State behaviour in cyberspace that many States have asked for.

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

On 16 March 2021 the United Kingdom published *Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy*,[9] which describes the Government's vision for the United Kingdom's role in the world over the next decade and the action we will take to 2025. The review identifies the need to shape the international order as it develops in future frontiers – in the domains of cyberspace and space, where the possibilities for economic, social and military activity are expanding rapidly. We will be active in ensuring effective accountability and oversight that protects democratic values, while opposing the overreach of State control.

The United Kingdom will also adopt a new, comprehensive cyberstrategy in 2021, replacing the previous national cybersecurity strategy 2016–2021. The need for a "whole-of-Government" approach to cyberissues will underpin the strategy, as foreshadowed in the integrated review. Under this strategy, our priority actions will be:

- To strengthen the United Kingdom's cyberecosystem, enabling a whole-of-nation approach to cyber and deepening the partnership between Government, academia and industry.
- To build a resilient and prosperous digital United Kingdom, where citizens feel safe online and confident that their data is protected.
- To take the lead in the technologies vital to cyberpower, such as microprocessors, secure systems design, quantum technologies and new forms of data transmission.
- To promote a free, open, peaceful and secure cyberspace, working with other Governments and industry and drawing on the United Kingdom's thought leadership in cybersecurity.

[9] www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

- To detect, disrupt and deter our adversaries.

Through these strategies, we will work with other Governments and in partnership with industry to ensure that cyberspace is governed by rules and norms that enhance collective security, promote democratic values and support global economic growth, and counter the spread of digital authoritarianism. The United Kingdom will uphold the rule of law in cyberspace: embodying responsible State behaviour and shaping international best practice, and incentivizing compliance, deterring attacks and holding others to account for irresponsible State behaviour. Where needed, we will shape the rules so that offensive cybertools are developed and used responsibly and in accordance with international law.

In addition we will:

- Protect an accessible and interoperable global Internet for future generations.
- Ensure human rights are protected online as they are offline.
- Ensure that transparency and accountability are embedded from the outset in the design and deployment of new technologies.
- Champion the international flow of data, enabling secure, trusted and interoperable exchange across borders, while maintaining data protection standards.

The United Kingdom considers cyberdiplomacy to be a critical element of its cyberleadership, with a network of officers stretching across six continents. In addition to our cybersecurity capacity-building programmes, we have initiated cross-Government dialogues with 20 countries. Through these, we will continue to grow the partnership to strengthen the case for a free, open, peaceful and secure cyberspace, and to respond to and deter State-directed malicious cyberactivity.

We continue to participate in an extensive range of global and regional forums dedicated to cybersecurity discussions, including both the United Nations Open-ended Working Group and the United Nations Group of Governmental Experts, the Organization for Security and Cooperation in Europe (OSCE), the International Telecommunication Union and the Global Forum on Cyber Expertise.

The United Kingdom can and does attribute malicious cyberacts to States where it believes it is in its best interests to do so, and in furtherance of its commitment to clarity and stability in cyberspace. We continue to consider that the decision to attribute malicious cyberactivity to a State, and crucially to make that attribution public, is ultimately a political decision for States. Statements and other relevant information are available online at www.gov.uk and www.ncsc.gov.uk.

In 2020, the United Kingdom established the National Cyber Force. We are one of a number of countries that have publicly confirmed that they are developing such capabilities. The National Cyber Force conducts targeted, responsible offensive cyberoperations to support the United Kingdom's national security priorities, bringing together defence and intelligence capabilities. Used in combination with diplomatic, economic, political and military capabilities, examples of cyberoperations could include:

- Interfering with a mobile phone to prevent a terrorist from being able to communicate with their contacts.
- Helping to prevent cyberspace from being used as a global platform for serious crimes, including fraud and sexual abuse of children.
- Keeping military aircraft of the United Kingdom safe from targeting by weapons systems.

The United Kingdom is committed to using its cybercapabilities in a responsible way, in line with the law of the United Kingdom and international law. Past and future cyberoperations have operated and will continue to operate under existing laws, including the Intelligence Services Act of 1994 and the Investigatory Powers Act of 2016. This ensures that cyberoperations of the United Kingdom are responsible, targeted and proportionate.

All Member States have agreed that it is in the interest of all States to promote the use of information and communications technologies (ICTs) for peaceful purposes. The United Kingdom reconfirms that ICTs are not in and of themselves a "threat". Rather, it is when States (or other actors) choose or are perceived to use them "for purposes inconsistent with international peace and security" that the threat or risk arises. In this context, furthering the conversation about how States understand international law applies when acting in cyberspace is a practical step to increasing transparency, predictability and stability.

The latest information about approaches of the United Kingdom to cybersecurity, including with regard to international cooperation, can be found online at www.gov.uk/government/cyber-security and www.ncsc.gov.uk.

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

The United Kingdom welcomes that both processes saw Member States reaffirm the previous three Group of Governmental Expert consensus reports of 2010, 2013 and 2015, which confirmed that international law applies to cyberspace and established a framework of responsible State behaviour consisting of a set of voluntary and non-binding norms and confidence-building measures, underpinned by capacity-building. The new reports in 2021 will be an important contribution to the acquis.

The United Kingdom considers that the proper implementation of the framework outlined in the existing reports, in its entirety by all States, provides a practical starting point for our efforts to increase stability in cyberspace. Universalization and operationalization of the cumulative assessments and recommendations would be a practical step forward. Practical, action-oriented approaches are therefore required.

Existing and emerging threats

With regard to developing trends, during the coronavirus disease (COVID-19) pandemic, attackers took advantage of the crisis in their selection of targets, which included hospitals and other health-related critical infrastructure. Malicious actors actively targeted organizations involved in both national and international COVID-19 responses. These organizations include health-care bodies, pharmaceutical companies, academic institutions, medical research organizations and local government. Such actors frequently target organizations in order to collect bulk personal information, intellectual property and intelligence that aligns with national priorities.

Ransomware has become one of the most frequent and disruptive types of incident dealt with by the United Kingdom's National Cyber Security Centre. In the 2020 annual review,[10] we noted that the Centre handled more than three times as many incidents as the previous year. The United Kingdom also saw a spike in ransomware attacks affecting the education sector at a time when institutions were working hard to manage online learning, admissions and testing procedures. Attackers are increasingly raising the stakes by threatening to leak stolen data publicly where

[10] www.ncsc.gov.uk/news/annual-review-2020.

victims are reluctant to pay the ransom. We have also seen attackers grow more sophisticated, sitting on a network over time and looking around for the most high-value data to encrypt, as well as any online back-ups to obstruct recovery.

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

The United Kingdom affirms that all existing international law, including respect for human rights and fundamental freedoms and the application of international humanitarian law to cyberoperations in armed conflict, forms part of our mutual commitment to behave responsibly in cyberspace. International law applies in its entirety in the same way it applies to State activities offline.

In this regard, we welcome the call by the International Committee of the Red Cross for all States to reaffirm that international humanitarian law applies to the conduct of cyberoperations during armed conflicts. When States engage in cyberoperations, they are governed by international law just like activities in any other domain. The application of international humanitarian law to cyberoperations in armed conflicts provides both protection and clarity. It does not encourage such conflict and ensures that the existing body of principles and rules that seek to minimize the humanitarian consequences of conflict apply.

However, we believe that we all need to go further as individual States and set out our own understandings of how international law applies to cyberspace. The United Kingdom did so in 2018 when former Attorney General Jeremy Wright QC MP set out the United Kingdom's position on applying international law to cyberspace. This was the first time a Government Minister had placed the United Kingdom's view on record.

We also recognize the need for capacity-building in relation to international law, including through possible exercises relating to our understanding of the application of international law. Capacity-building in this area could make a tangible difference to the ability of States to develop their own positions and defend their national interests in future negotiations, as well as to ensure we do not inadvertently deepen the digital divide in this way.

Norms, rules and principles of responsible behaviour of States

In September 2019, the United Kingdom submitted to the Open-ended Working Group the "Non-paper on efforts to implement norms of responsible State behaviour in cyberspace, as agreed in the United Nations Group of Governmental Expert reports of 2010, 2013 and 2015".[11] This remains an effective guide to efforts by the United Kingdom to implement the norms of responsible State behaviour. We welcomed the submission by the Multi-stakeholder Advisory Group on Cyber issues of the United Kingdom of a complementary paper,[12] which provides suggestions on how stakeholders can contribute to norm implementation in support of States.

The United Kingdom believes that norms must be implemented to be effective. The key factors in implementation are as follows:

- Awareness within Governments and stakeholder communities to help develop a shared understanding of the value of the norms and promote their adoption.

[11] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf.

[12] www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf.

- Resources to support implementation. Implementation of the norms can and should be an element of any national cybersecurity strategy. In 2019, only 40 per cent of States had such a strategy. The United Kingdom continues to support a range of States in building their national cybercapacity.
- Availability of best practice guidance on implementation. The United Kingdom believes the report of the Group of Governmental Experts will provide a detailed guide to the initial framework for responsible State behaviour in cyberspace that many States have asked for. The non-paper and the complementary paper referenced above also contribute to building best practice in this area.

Confidence-building measures

The United Kingdom considers that States should focus on operationalizing existing confidence-building measures rather than developing new ones. Regional organizations are important vehicles in the universalization and operationalization of the recommendations of the previous Groups of Governmental Experts, alongside the private sector, academia and civil society organizations. However, the operationalization of confidence-building measures remains limited, leaving a major gap in the potential efficacy of our framework.

The United Kingdom actively participates in the OSCE Informal Working Group on Cyber Confidence-building Measures. We have adopted OSCE confidence-building measure 5 on capacity-building, undertaking to support its operationalization among OSCE States. In 2019 we hosted a cyber scenario-based discussion to practise implementation and understanding of the confidence-building measures among 40 member States. In 2020 and 2021, the United Kingdom has chaired the OSCE Security Committee, using its role to host two cyber-focused events.

Capacity-building

The United Kingdom is a major bilateral cybercapacity-building donor. We consider that the United Nations can use its convening power to raise the profile of cybersecurity capacity-building and encourage coordinated good practice. In order to maximize efficiency and effectiveness, it will be important to involve all stakeholders and avoid the duplication of existing work. The Global Forum on Cyber Expertise is already an effective coordination mechanism for capacity-building. Independent capacity review tools, best practice guides and organizations, like the Forum of Incident Response and Security Teams in the cybersecurity incident response team community, are also important contributors to this objective.

During the period 2019–2021, the United Kingdom was a sponsor of the Women in International Security and Cyberspace Fellowship. We are particularly proud to have contributed to the increased participation of women in the Open-ended Working Group through this programme.

Regular institutional dialogue

The United Kingdom is a sponsor of the proposal for a programme of action to facilitate inclusive regular institutional dialogue on responsible State behaviour in cyberspace at the United Nations. We support further work to elaborate and establish this proposal.

III. Replies received from intergovernmental organizations

European Union

[Original: English]
[31 May 2021]

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 and secure cyberspace grounded in the rule of law, human rights, fundamental freedoms and democratic values that bring social, economic and political development globally.

As the Internet becomes more embedded in our lives, a number of the same issues we face in the physical world arise in cyberspace. Cyberspace is increasingly exploited for political and ideological purposes, and increased polarization at the international level is hindering effective multilateralism. The threat landscape is compounded by geopolitical tensions over the global and open Internet and over control of technologies across the whole supply chain. The malicious targeting of critical infrastructure is a major global risk. Restrictions of and on the Internet, the increase in malicious cyberactivities, including an increase in activities affecting the security and integrity of information and communications technology (ICT) products and services, threaten global and open cyberspace, as well as the rule of law, fundamental rights, freedom and democracy. 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.

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, by 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 cyberresilience is a crucial element in maintaining international peace and stability, by reducing the risk of conflict and as a means of addressing the challenges associated with the digitalization of our economies and societies. Global cyberresilience reduces the ability of potential perpetrators to misuse ICT for malicious purposes and strengthens the ability of States to effectively respond to and recover from cyberincidents.

The cybersecurity strategy entitled "An Open, Safe and Secure Cyberspace",[13] of 2013, as well as the subsequent policy documents, instruments and strategies cited below, represent the European Union's comprehensive vision on how best to prevent and respond to cyberdisruptions and cyberattacks. They are aimed at promoting European Union values and ensuring that conditions are in place for the digital economy to grow. Certain specific actions are aimed at enhancing the cyberresilience of information systems, reducing cybercrime and strengthening European Union international cybersecurity policy and cyberdefence.

[13] 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".

In February 2015, the Council of the European Union stressed in its Council Conclusions on Cyber Diplomacy[14] the importance of further developing and implementing a common and comprehensive European Union approach to cyberdiplomacy 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 cyberspace and 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 to cyberdiplomacy.

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”[15] set 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 those challenges gave impetus to the development of a framework for a joint European Union diplomatic response to malicious cyberactivities, the cyberdiplomacy toolbox.[16] 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 destabilizing 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 cyberdiplomacy, 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 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.

In December 2020, the European Union further outlined its strategy for a cybersecure digital transformation in a complex threat environment.[17] The European Union’s cybersecurity strategy for the digital decade aims to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights,

[14] 6122/15 Council Conclusions on Cyber Diplomacy.

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

[16] 10474/17. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”).

[17] See joint communication to the European Parliament and the Council, entitled “The EU’s Cybersecurity Strategy for the Digital Decade”, and 7290/21 (22 March 2021), Council Conclusions on the EU’s Cybersecurity Strategy for the Digital Decade.

fundamental freedoms, democracy and the rule of law. The strategy contains concrete proposals to address resilience, prevent, deter and respond to cyberthreats and advance a global and open cyberspace. Preventing the misuse of technologies, protecting critical infrastructure and ensuring the integrity of supply chains also enables the European Union to adhere to the United Nations norms, rules and principles of responsible State behaviour.

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 to cyberspace, while assisting countries outside the European Union with cybersecurity capacity-building and promoting international cooperation on cyberissues. The European Union continues to work with international partners to advance and promote a global, open, stable and secure cyberspace where international law, in particular the Charter of the United Nations, is respected, and the voluntary non-binding norms, rules and principles of responsible State behaviour are adhered to. To promote an effective multilateral debate to advance peace and security in cyberspace, there is a clear need to take forward the United Nations framework for responsible State behaviour in cyberspace. Together with 53 States Members of the United Nations, the European Union proposes to establish a programme of action for advancing responsible State behaviour in cyberspace. Building on the existing acquis as endorsed by the General Assembly, the programme of action offers a permanent platform for cooperation and the exchange of best practices within the United Nations. It offers the opportunity to foster capacity-building programmes tailored to the needs identified by beneficiary States. It also provides an institutional mechanism within the United Nations to improve cooperation with other stakeholders such as the private sector, academia and civil society on their respective responsibilities to maintain an open, free, secure, stable, accessible and peaceful ICT environment.

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 ICTs for malicious purposes, by both State and non-State actors, as well as the increase in cyberenabled 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 destabilizing and cascading effects with enhanced risks of conflict.

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 are in particular alarmed by the recent increase in activities affecting the security and integrity of ICT products and services, which might have systemic effects.

The European Union and its member States condemn this malicious behaviour in cyberspace and underline their continued support to increasing global cyberresilience. Any attempt to hamper the ability of critical infrastructures is unacceptable and can put people's lives at risk. Malicious use of ICTs undermines the benefits that the Internet and the use of ICTs provide to society at large, and shows the readiness of some actors to effectively risk international security and stability. 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 and the Open-ended Working Group, given the unique character of ICTs, the European Union's approach to addressing cyberissues 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 ICT that fully respect applicable international law and norms, particularly the Charter of the United Nations, as well as international humanitarian law and human rights.

How international law applies to the use of information and communications 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. 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 Group of Governmental Experts in 2010, 2013 and 2015, as well as the principles established in paragraphs 28 (a) to 28 (f) of the 2015 report and the Open-ended Working Group.

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 the context of conflict. The European Union underlines its conviction that international law is not an enabler of conflict; 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[18] and the General Assembly.

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

For these reasons, the European Union and its member States do not call for and do not see the necessity of creating new international legal instruments for cyberissues 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 for efforts to bring legal clarity concerning how existing international law applies, as this 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 concerning how international law applies to the use of ICTs by States, as this promotes transparency and advances global understanding of 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 awareness-raising and capacity-building regarding the applicability of existing international law as a means of promoting stability and preventing 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 resolution 70/237, and further build on the Open-ended Working Group, as well as on advancing 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 ICTs 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 the successive reports of the Group of Governmental Experts of 2010, 2013 and 2015. We believe that a practical way forward should encourage increased cooperation and transparency with respect to sharing 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

Effective mechanisms for State cooperation and interaction in cyberspace are critical components of conflict prevention. Regional forums have proven to be a relevant platform to create space for dialogue and cooperation among actors with shared concerns and common interests in order to address challenges effectively 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, the Regional Forum of the Association of Southeast Asian Nations, the Organization of American States 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 in 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 and reducing the ability of potential perpetrators to misuse ICTs for malicious purposes. 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 cyberincidents, 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. The European Union and its member States attach particular importance to enhancing international security and stability in cyberspace by encouraging and facilitating concrete action on responsible State behaviour in cyberspace and by strengthening cybercapacity-building cooperation, including with the support of a facilitation mechanism in the United Nations to foster capacity-building programmes tailored to the needs identified by beneficiary States, such as the programme of action.