United Nations A/77/92

General Assembly

Distr.: General
8 June 2022
English
Original: Arabic/English/Russian/
Spanish

Seventy-seventh session
Item 94 of the preliminary list*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies

Report of the Secretary-General

Contents

* A/77/50.

I. Introduction

1. On 6 December 2021, the General Assembly adopted resolution 76/19, entitled "Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies", under agenda item 95, on "developments in the field of information and telecommunications in the context of international security".

2. In paragraph 6 of resolution 76/19, the General Assembly invited all Member States, taking into account the assessments and recommendations contained in the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, to continue to inform the Secretary-General of their views and assessments on the following questions:

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

(b) The content of the concepts mentioned in the report of the Open-ended Working Group and the reports of the Group of Governmental Experts.

3. Pursuant to that request, on 24 January 2022, a note verbale was sent to all Member States inviting them to provide information on the subject.

4. The replies received at the time of reporting are contained in sections II and III. Additional replies received after 31 May 2022 will be posted on the website of the Office for Disarmament Affairs (www.un.org/disarmament/ict-security) in the original language received.

II. Replies received from Governments

Armenia

[Original: English]
[31 May 2022]

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

The Government of Armenia has established a digitization council to boost the development of digital skills and the digitization of the public administration system and the economy. According to 2021 data, nearly 25 programmes and strategic documents had been discussed and continuous work was being done in the areas of digital identification, authentication of official documents, e-licences, the introduction of individual and public notifications, and the introduction of unified e-justice systems, as well as on a number of other issues on the digital agenda.

The Republic of Armenia approved a digitalization strategy on 11 February 2021. The strategy envisages digital transformation of the Government, the economy and society through the introduction and development of innovative technologies, cybersecurity, data policy, e-services and e-government systems, coordination of digitalization processes, the definition of common standards and a digital environment, as well as initiatives promoting the use of digital technologies in the private sector of the economy and the development and implementation of programmes promoting the use of electronic tools by the public.

The following initiatives are planned to be undertaken in the framework of the digitalization strategy of Armenia for the period 2021–2025:

(a) Carry out legislative and normative-legal amendments in the field of information security;

(b) Elaborate a public open data policy concept;

(c) Implement cybersecurity training for the residents of border villages (currently, cyber security courses are conducted for State employees);

(d) Establish a national cybersecurity centre. In particular, the possibility of the introduction of cybersecurity criteria, the creation of State rapid response groups and the implementation of public awareness activities aimed at raising cyberliteracy are being considered.

The Ministry of High-Tech Industry plans to elaborate a comprehensive policy and action plan for overcoming the challenges in the field of cybersecurity, which will include the process for the creation of the cybersecurity centre and the formation of risk management and rapid response mechanisms during natural disasters, emergencies and martial law.

The Ministry stresses the importance of close cooperation with the private sector, inter-agency cooperation, localization of the international experience and the observation of international cybersecurity standards, inter-State cooperation and membership in international security structures.

Armenia is developing policies and capabilities in the area of cybersecurity with international and regional organizations, including through the participation of relevant Armenian institutions in various thematic seminars, conferences and training.

The Republic of Armenia is a party to the Council of Europe Convention on Cybercrime. More recently, Armenia has initiated a national procedure for signing the Second Additional Protocol to the Council of Europe Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence.

Armenia is actively involved in the efforts of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. The Working Group is uniquely designed to shape the basis for new standards in the field of information and communications technology (ICT).

The ongoing cooperation within the Council of Europe's CyberEast project is aimed at building capacity for the experts of Armenian government institutions in countering threats of cybercrime.

Armenia also values the continuous efforts being undertaken in the framework of the Organization for Security and Cooperation in Europe's confidence-building measures in the field of ICTs, which help to build transparency, predictability and stability in that field.

At the same time, cooperation with supranational companies is noteworthy. Armenia hosts leading information technology companies, such as Synopsys, Mentor Graphics, National Instruments, Microsoft, VMware, D-Link, Oracle, Cisco and others. Microsoft and Cisco regularly provide cooperation or attend forums to support the Government of Armenia with the latest developments on cybersecurity and defence.

Australia

[Original: English]
[31 May 2022]

Australia welcomes the opportunity, in response to the invitation in General Assembly resolution 76/19, to provide the Secretary-General with its views on advancing responsible State behaviour in cyberspace. This submission builds upon information provided by Australia in response to prior General Assembly resolutions,[1] including most recently in May 2021 (see A/76/187). Australia encourages all States to proactively engage in the provision of regular updates to the Secretary-General, so as to increase transparency and build understanding of each other's efforts to advance responsible State behaviour in cyberspace.

Framework of responsible state behaviour in cyberspace

Cumulatively, the 2010, 2013 and 2015 reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[2] 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, these four tenets are often referred to as the framework for responsible State behaviour in cyberspace.

Australia was pleased that the March 2021 report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (A/75/816), which was negotiated and endorsed by all 193 States Members of the United Nations, demonstrated universal commitment to the framework. Australia was further pleased to have a leading expert participate in the sixth Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, which provided further additional practical guidance on how to implement the framework (see A/76/135), which was subsequently welcomed by the General Assembly in its resolution 76/19.

Australia reaffirms its commitment to act in accordance with the cumulative reports of the Group of Governmental Experts and that of the Working Group. Australia remains actively engaged in the open-ended working group on security of and in the use of information and communications technologies 2021–2025, established under resolution 75/240, and a committed co-sponsor of the proposal of France and Egypt for the establishment of a programme of action. Australia supports the establishment of a programme of action that provides a permanent, inclusive and transparent forum for ongoing discussion and practical action on cyberissues under the auspices of the United Nations.

In the interests of transparency, Australia will shortly publish an update on how it implements and observes the 11 voluntary, non-binding norms of responsible State behaviour. While norms do not replace or alter States' obligations or rights under international law (which are binding), Australia reaffirms the 11 norms as a complement to international law, which provides additional specific guidance on what constitutes responsible State behaviour in the use of information and communications technologies. Australia will also make publicly available its initial self-assessment of our implementation of United Nations cybercommitments using the United Nations Institute for Disarmament Research (UNIDIR) national survey via the Institute's

[1] Resolutions 65/41, 68/243, 70/237, 74/28 and 75/32.

[2] A/65/201, A/68/98 and A/70/174, respectively.

Cyber Policy Portal in the near future. Australia commends the national survey to all States and encourages States to consider also making their self-assessments publicly available. Surveying implementation of United Nations recommendations provides several benefits. Namely, States can identify how they have implemented the framework, where gaps in implementation might exist and any barriers to implementation. This in turn is likely to assist in developing targeted cooperation and capacity-building programmes, which might be appropriate to overcome any gaps in capacity and/or barriers to implementation identified.

International law

Australia encourages all States to continue to study and be transparent about their positions on how international law applies to State behaviour in cyberspace. We reiterate that, even where views differ, developing understandings of each other's positions on how international law applies in cyberspace increases predictability and reduces the risk of miscalculation, which can lead to escalation in States' conduct. Australia further reiterates that international law is most effective when States implement and adhere to their international legal obligations and, where necessary, cooperate to uphold international law and ensure accountability for violations.

Australia welcomed the conclusions contained in the 2021 report of the Group of Governmental Experts (A/76/135) that international humanitarian law applies to cyberactivities in situations of armed conflict.

The position of Australia on how international law applies to State conduct in cyberspace is presented in a series of documents:

- Australia's 2021 submission contained in the official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts (A/76/136);
- 2021 international cyber and critical technology engagement strategy;
- 2020 case studies on the application of international law in cyberspace (submitted to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security);
- 2019 International Law Supplement;
- 2017 international cyberengagement strategy.

Further to the engagement of Australia in United Nations processes on how international law applies in cyberspace, Australia also endeavours to engage in such discussions in regional forums. In this regard, Australia delivered a statement at the fifty-ninth session of the Asian-African Legal Consultative Organization on international law in cyberspace in late 2021.

Deterrence and responses to irresponsible State behaviour

Australia does not tolerate activities in cyberspace that are detrimental to international peace and stability or that are contrary to the framework, which has been agreed by all States Members of the United Nations. Australia encourages the global community to shine a light on malicious cyberactivity and hold the actors responsible to account. Australia has a policy of publicly attributing malicious cyberactivity when the source is known and when it is in our interests to do so. This policy is not directed at any one country. To date, Australia has publicly attributed malicious cyberactivity on 13 occasions. Most recently, on 10 May 2022, Australia joined the United States of America and the European Union in attributing a range of destructive, disruptive and destabilizing cyberactivities against Ukraine to the Russian Government.

Multi-stakeholder engagement

Australia thanks Burhan Gafoor, Chair of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, for his constructive efforts to obtain consensus agreement on a set of transparent and balanced modalities for the future participation of non-Government stakeholders in the working group. Australia looks forward to these modalities being formally adopted at the third substantive session of the working group, to be held in July 2022. Australia is a steadfast supporter of multi-stakeholder engagement in discussions on responsible State behaviour in cyberspace. Cyberspace is unique: the private sector, technical community, civil society and academia play a vital role in its technical management and governance, and the multi-stakeholder community can provide perspectives that help us better understand emerging cyberthreats, their impacts and how to address them. Australia was disappointed by some States' efforts to stymie stakeholder participation in the process, which we consider goes against the spirit in which the working group was established. Australia believes that the working group is liable to have a far-reaching impact on many stakeholders, including direct impacts on communities and individuals, and that addressing the threats emanating from cyberspace requires us to leverage the experience, expertise and resources of all relevant stakeholders. Australia therefore welcomes the agreed modalities as a step towards transparency and inclusivity.

Women in cyber

As recognized by the women and peace and security agenda, women and girls are uniquely and disproportionately affected by conflict and crises, as well as underrepresented in (and excluded from) international peace and security processes. As identified by the UNIDIR report "Still behind the curve: gender balance in arms control, non-proliferation and disarmament diplomacy", First Committee processes lag significantly behind the strides towards gender parity seen across other United Nations committees. UNIDIR data show that, in First Committee debates, 27 per cent of speakers are women. This drops to an average of 20 per cent in forums on more specialized topics.

To address this, Australia, together with Canada, the Netherlands, New Zealand, the United Kingdom of Great Britain and Northern Ireland and the United States, launched the Women in International Security and Cyberspace Fellowship in February 2020. The Fellowship provides early- to mid-career women diplomats with training on multilateral negotiations, cyberpolicy and international law, and sponsors travel to New York to join their national delegations to United Nations meetings that consider responsible State behaviour in cyberspace, including at the working group.

Australia is pleased that, through the Fellowship, many fellows were able to join their national delegations to the first and second sessions of the working group and made a significant contribution to the working group and to advancing the women and peace and security agenda. At the first session of the working group, held in December 2021, 37 per cent of interventions were made by women speakers. At its second session, held in March 2022, 43 per cent of interventions, and half of all international law statements, were made by women speakers.

Azerbaijan

[Original: English]
[31 May 2022]

During recent years, several new legal acts have been adopted in Azerbaijan in order to ensure information security. Besides that, concept of development, strategic road map, national strategy and State programmes have been adopted, and cooperation with various countries has been established by the decrees and orders of the President of Azerbaijan.

Due to the need to consider the security of critical information infrastructure as a priority, a normative legal act was adopted to strengthen security in this area. Classification of these infrastructure facilities according to their importance and determination of general and special security requirements is taken into account within the above-mentioned legal act, and it is envisaged that continuous control will be carried out through the application of appropriate methods.

The Coordination Committee on İnformation Security was established in 2018, pursuant to the order of the President of Azerbaijan.

In order to sustain the security of critical information infrastructure, the division of powers between institutions has been determined in accordance with the decree of the President of Azerbaijan of 17 April of 2021.

In order to enhance human capital in this field, various training sessions were organized by the Cyber Academy of the Ministry of Digital Development and Transport, with national and international certificates provided.

Virtual seminars were held by international experts on the protection of personal data, cybercrime and electronic evidence for the representatives of relevant State bodies of Azerbaijan, within the framework of the CyberEast and Cybersecurity East joint programmes of the European Union and the Council of Europe.

Representatives of several State bodies of Azerbaijan attended their first certificated training on cybersecurity, within the framework of the grant programme of the Korea International Cooperation Agency.

In addition to above-mentioned, consultations and cooperation initiatives with the computer emergency response teams of various States have been carried out.

Azerbaijan ranks fortieth in the world and third (following the Russian Federation and Kazakhstan) in the Commonwealth of Independent States in the Global Cybersecurity Index 2020 of the International Telecommunication Union.

Due to the increase in the number of cyberthreats during the coronavirus disease (COVID-19) pandemic, as well as detected weaknesses of programme and technical equipment, relevant notifications and messages on the methods of protection from cyberthreats have been posted on www.cert.az and on social networks.

Cuba

[Original: Spanish]
[31 May 2022]

The misuse of information and telecommunications technologies remains a matter of great concern to the international community, hence the need to address the growing threats in that area.

We condemn the misuse of media platforms, including social media and radio broadcasts, as a tool for interventionism through the promotion of hate speech, incitement to violence, subversion, destabilization, the dissemination of fake news and the misrepresentation of reality for political purposes and as a pretext for the waging of war or for the threat or use of force, in violation of the purposes and principles of the Charter of the United Nations and international law.

In this regard, we reject the methods of unconventional warfare deployed by the United States Government against Cuba, including through the use of new information technologies and other digital platforms to destabilize and discredit our country.

We reaffirm the right and duty of States to combat, as a constitutional prerogative, the dissemination of fake or distorted news that may be interpreted as interference in the internal affairs of other States or as detrimental to the promotion of peace, cooperation and friendly relations among States and nations.

We cannot ignore the fact that the growing development of cyberoffensive capabilities and operations can transform cyberspace into a new theatre of conflict. We reject attempts to equate the malicious use of information and communications technologies with the concept of “armed attack” in order to justify the exercise of the right of self-defence provided for in Article 51 of the Charter of the United Nations.

We repudiate the deliberate use of these technologies to damage the vital infrastructure of other States, including their information systems, or to otherwise hinder the use and operation of critical infrastructure, which is essential to the social stability and security of States.

The United Nations is the preeminent multilateral forum and the main platform for addressing the concerns of its Member States regarding the security and use of information and communications technologies. In this regard, the open-ended working group on security of and in the use of information and communications technologies 2021–2025, established pursuant to General Assembly resolution 75/240, is the only inclusive mechanism available to Member States to discuss cybersecurity issues in a transparent manner and on an equal footing.

We reiterate the importance of the aforementioned working group and hope that this intergovernmental process will contribute to filling the existing legal vacuum with binding norms leading to the adoption of a comprehensive legal instrument on information and communications technologies in the context of international security.

While confidence-building measures are a useful tool, such measures alone do not guarantee the strictly peaceful use of information and communications technologies, given that no such legally binding instrument exists in this area.

Cuba, as a member of the Movement of Non-Aligned Countries, once again calls upon developed countries and the relevant international entities to provide developing countries, upon request, with assistance and cooperation, including through financial resources, capacity-building and technology transfer, taking into account the specific needs and characteristics of each recipient State.

We oppose the application of unilateral coercive measures that, like the economic, commercial and financial blockade imposed by the Government of the United States against Cuba, prevent or limit universal access and the peaceful use and enjoyment of information and communications technologies for the well-being of our populations.

Denmark

[Original: English]
[31 May 2022]

In Denmark, as in many parts of the world, digital solutions are an integral part of everyday life. They are both a platform for basic societal activities and a key driver of economic growth. However, as our societies and our digital infrastructure have become increasingly interconnected, the ability and the willingness of State and non-State actors to conduct malicious cyberactivities has also increased. This should be of global concern, as malicious activities in cyberspace may constitute wrongful acts under international law and lead to potential escalation, which in turn threatens international security and stability. Russia's unprovoked and unlawful invasion of Ukraine, which also includes cyberattacks against critical infrastructure, is particularly concerning and completely unacceptable, as it constitutes a violation of international law and undermines the framework for responsible State behaviour in cyberspace.

As one of the most digitalized countries in the world, Denmark remains determined to prevent, deter and respond accordingly to malicious activities and to enhance international cooperation to this effect. Together with the European Union, Denmark seeks 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. In this respect, Denmark stresses the importance of States adhering to the framework for responsible State behaviour in cyberspace, which supports the international rules-based order, and affirms the applicability of international law, adherence to the voluntary norms of responsible State behaviour and the development and implementation of practical confidence-building measures. The framework has repeatedly been affirmed by all members of the General Assembly as the cornerstone of the international community's efforts to deter reckless and irresponsible State behaviour in cyberspace and to avoid the most damaging cyberattacks and potential escalations. We therefore call on all Member States, including the Russian Federation, to honour their commitments.

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

So far, Denmark has taken several steps to strengthen its cybersecurity and information security and to promote international cooperation on cybersecurity. The Danish Defence Agreement for the period 2018–2023 allocates DKr 1.4 billion to strengthened cybersecurity and cyberdefence, thereby strengthening the resilience and robustness of Danish society against cyberattacks.

With the Danish cyber and information security strategy for the period 2018–2021, 25 initiatives, as well as 6 dedicated strategies, were introduced with the aim of:

(a) Increasing cyber and information security, particularly within critical sectors;

(b) Ensuring systematic and coordinated efforts;

(c) Enhancing the technological resilience of digital infrastructure;

(d) Improving the knowledge of citizens, businesses and authorities with regard to cybersecurity.

As part of the strategy, dedicated cybersecurity and information security units in the six critical sectors (energy, finance, transport, health care, telecommunications and maritime) were established, as well as forums for the units to share experiences.

The Centre for Cyber Security has also launched its own intensive Cyber Academy and broadly supports education and research within the field of cybersecurity. Likewise, the Agency for Digital Government developed several courses, learning materials and events on cybersecurity and information security aimed at chief executives, cyberspecialists and public employees.

In addition, the Agency for Digital Government has developed the website www.sikkerdigital.dk, which offers concrete cybersecurity and information security guidance to citizens and runs national campaigns on secure digital behaviour in close cooperation with municipalities and regions.

Denmark has established a public-private Cybersecurity Council (Cybersikkerhedsråd), which provides the Government with advice on how to strengthen cybersecurity and improve knowledge-sharing between authorities, business and researchers. Finally, with the Danish cyber and information security strategy for the period 2018–2021, Denmark also strengthened its international cyber engagement, allowing the country to step up its engagement in multinational cyberforums such as the United Nations, the European Union, the North Atlantic Treaty Organization (NATO) and the Organization for Security and Cooperation in Europe (OSCE).

In December 2021, the Government presented a new national cybersecurity and information security strategy for 2022–2024. The strategy builds on and expands the current efforts by further strengthening cybersecurity and information security through 34 main initiatives aimed at the public and the private sectors, as well as Danish citizens in general. Overall, the strategy includes four main objectives:

(a) First, the strategy further strengthens the resilience of the critical information and communications technology (ICT) infrastructure that supports vital societal functions. To ensure an adequate level of cybersecurity for both government agencies and businesses, a series of strategic actions, including tightened security requirements for the management of government ICT systems critical to society and a strengthened police response to cybercrime, has been launched. The strategy also expands the number of critical sectors to include a wider range of government agencies with responsibility for information technology-supported vital societal functions. Government agencies within these critical sectors are required to comply with a number of specific security requirements in addition to the minimum requirements that were previously introduced in the 2018–2021 strategy. This is to ensure that ministries with a particular responsibility for vital societal functions are able to act quickly and efficiently in the event of a serious cyberincident;

(b) Second, the strategy includes a number of initiatives that strengthen Danish citizens' cybersecurity skills and increase management's commitment to strengthening cybersecurity. Among the initiatives are new dedicated training programmes for government employees, as well as educational programmes that equip children, young people and adults with the competences necessary to be digitally literate. Furthermore, top managers and leaders face increased requirements and expectations to prioritize cybersecurity and information security;

(c) Third, the strategy strengthens cooperation on cybersecurity and information security between the public and private sectors. The ability to share knowledge and experiences across sectors is vital to achieve a high level of cybersecurity and information security. For this reason, a cyberhotline, which will make it easy to seek advice in relation to cybercrime, as well as a dedicated cybersecurity unit for small and medium-sized enterprises, will be established in order to strengthen the capacity of the Centre for Cyber Security to provide guidance;

(d) Fourth, the strategy further strengthens the international efforts of Denmark on cybersecurity. This includes the allocation of additional resources to its diplomatic service in order to strengthen the country's contribution to multilateral cooperation on cybersecurity within the European Union, NATO and the United Nations and to promote cooperation with the international tech industry, academia and think tanks, as well as export controls on digital products. Finally, the strategy also includes initiatives that will strengthen the country's national and international efforts to set up active cyberdefences and increase deterrence.

In addition to the initiatives launched in as part of the national cybersecurity and information security strategies, Denmark continues its broad engagement in countering hybrid threats such as cyberattacks and influence operations through collaboration with its partners and allies in NATO and the European Union. Denmark also contributes to the 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.

Notably, Denmark supports the idea of establishing a United Nations programme of action which could provide a platform for States and non-State actors to cooperate further, for instance, in terms of putting in place capacity-building activities adapted to their needs or advancing their national implementation efforts under the United Nations framework, thus resulting in greater collective resilience and stability in the ICT domain.

Moreover, Denmark is also an active member of the Network and Information Systems Cooperation Group and the cybersecurity incident response team network, and is a member of the board of the European Union Agency for Cybersecurity.

Content of the concepts mentioned in the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

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 of 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.

State and non-State actors have shown their willingness to take advantage of any opportunity to conduct malicious cyberactivities. This includes interfering with critical infrastructure and cyberenabled theft of intellectual property. Any attempt to hamper the ability of critical infrastructure 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. Specifically, Russia's use of cyberattacks against critical infrastructure as part of the unprovoked and unlawful invasion of Ukraine is completely unacceptable and must therefore be strongly condemned by the entire international community. States must refrain from the use of cyberattacks, exercise due diligence and take swift and firm action against malicious ICT activity originating from their territory, as consistent with international law and the 2010, 2013, 2015 and 2021 consensus reports of the Groups of Governmental Experts and the report of the Working Group in 2021.

As recognized in previous reports of the Group of Governmental Experts, as well as the report of the Working Group, given the unique character of ICTs, the approach of the United Nations and its States Members 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 communications technologies

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

As recognized in the 2010, 2013, 2015 and 2021 consensus reports of the Groups of Governmental Experts, as well as the principles established in paragraph 71 (b) to (g) of the 2021 report and the Working Group, the international community has made it very clear that cyberspace is firmly rooted in existing international law. Denmark emphasizes that existing international law, including the Charter of the United Nations in its entirety, international humanitarian law and international human rights law apply to States' behaviour in cyberspace. We therefore call on all Member States 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. Denmark supports the work of the Group of Governmental Experts and the Working Group, as well as other international and regional initiatives, including the 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, according to which 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 does it 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 such issues. Denmark hopes that the work and recommendations of the Working Group will contribute to further clarifications and thus facilitate State compliance, as well as promote greater predictability and reduce the risk of escalation. To this end, Denmark is currently working on a national position on how international law applies to State action in cyberspace.

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 76/19, and to implement the agreed norms of responsible State behaviour in cyberspace, as well as confidence-building measures, which play an essential role in conflict prevention. We welcome an inclusive and constructive dialogue within the Working Group, as well as the possibility of practical cooperation through a potential United Nations programme of action.

As complementary to and deriving from existing international law, the norms, rules and principles of responsible State behaviour articulated through successive reports of the Group of Governmental Experts in 2010, 2013, 2015 and 2021, as well as the report of the Working Group, hold immense value. Denmark will continue to be guided by international law, as well as adherence to these voluntary norms, rules and principles. Further implementation of these norms should be pursued through increased cooperation and transparency around best practices.

Confidence-building measures

Building effective mechanisms for cooperation on cyberissues between States is critical in order to exchange information, build confidence and prevent conflicts. Regional forums such as OSCE have already established relevant platforms for confidence-building measures and cooperation among actors with shared concerns and common interests in order to address effectively challenges from a regional perspective. Furthermore, the Working Group itself should also be seen as a confidence-building measure, as it provides an international forum for all Member States to exchange information and share their views on cyberissues.

Denmark joins the European Union and its member States in encouraging the international community to further develop and implement of cyberconfidence-building measures which increase the predictability of State behaviour and reduce the risk of misinterpretation, escalation and conflict, and thereby contribute to long-term stability in cyberspace.

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

Strengthening the cyberresilience of our societies is crucial in order to reduce the risks stemming from the malicious use of ICTs, reduce tensions and prevent conflicts. Therefore, as outlined above, the Government of Denmark has introduced a broad number of initiatives to strengthen national cyberresilience. Similarly, the European Union and its member States, including Denmark, are also cooperating in order to strengthen resilience across the European Union, notably through the directives on the security of network and information systems.

In addition to these efforts, Denmark – together with the European Union and its member States – also contributes to increasing the cyberresilience of developing countries through a number of tailored programmes and initiatives, which are aimed at developing skills and capacities in terms of addressing cyberincidents as well as facilitating the exchange of best practices.

Denmark joins the European Union and its member States in recognizing that the promotion of a more resilient digital infrastructure will contribute to a more secure and stable cyberspace and encourages all relevant actors to engage in capacity-building in this regard and further call for stronger cooperation with key international partners and organizations to support capacity-building in third countries.

Moreover, Denmark also supports the establishment of a United Nations mechanism to foster capacity-building programmes tailored to the needs identified by beneficiary States, such as the programme of action, and identifying mechanisms that facilitate the engagement of all stakeholders in implementing the framework of responsible behaviour.

Egypt

[Original: Arabic]
[31 May 2022]

Egyptian views and proposals to strengthen information security and promote international cooperation

I. National efforts

- Over the recent period, Egypt has strengthened its capacity-building efforts and developed regulatory frameworks for communications and information security in line with the recommendations of the final reports of the open-ended working group and the reports of the Group of Government Experts.

- The Egyptian State is adopting balanced policies to keep up with and combat cybercrime and address illegal activities on the Internet and social media in accordance with a legislative framework based on a number of recently created laws, including the following: Act No. 175 (2018) on combating information technology crimes, Act No. 180 (2018) on regulating the press and media, and Act No. 151 (2020) on protecting personal data.

- The Supreme Cybersecurity Council has been established as the competent authority and national reference for cybersecurity matters. A national cybersecurity strategy was launched as part of Egypt Vision 2030. It will establish a national integrated system that incorporates international best practices. It will create national cybersecurity partnerships between government agencies and the private sector and reinforce cyberdefence programmes by establishing and improving the effectiveness of computer emergency response teams and networks formed within various State sectors. It will also set up and develop cybersecurity awareness programmes that target particular social demographics, such as schoolchildren, government agencies and the elderly, and promote scientific cybersecurity research and innovation.

- A number of national policies, governance mechanisms and regulatory frameworks and standards have been adopted. They include basic cybersecurity controls, cybersecurity systems controls, and ongoing cybersecurity monitoring at the national level.

- Egypt is working to promote bilateral and multilateral international cooperation in information security and capacity-building.

- Many national programmes and initiatives have been launched to raise community awareness, forestall cyberrisks, and reduce their impacts by issuing alerts about the latest and most dangerous cybervulnerabilities.
- Cooperation is ongoing with national bodies and academies to build capacities and create a qualified pool of cybersecurity and information security personnel.

II. Proposals

- It is crucial to strengthen international cybersecurity cooperation to minimize cross-border criminal cyberactivities and prevent the commission of cybercrimes. We must also exchange expertise and modern technologies to prosecute all illegal uses of the Internet so as to enable States to confront them. Training courses should be held to develop the capabilities of security agencies tasked with combating cybercrime.
- Action should be taken to govern the circulation of cryptocurrencies so that they are not used to finance illegal activities. Consideration should also be given to the creation of a specialized cybercrime unit at the International Criminal Police Organization (INTERPOL) to facilitate the exchange of information among security agencies involved in combating such activities.

Russian Federation

[Original: Russian]
[31 May 2022]

The twenty-first century has been a time of breakthroughs in the field of information technology, which has conquered practically every aspect of our lives. Traditional government, public and business sectors are undergoing a complete transformation. New opportunities have emerged for growing the economy, creating jobs and improving the quality of life for all. Nonetheless, the new technologies have come with new challenges.

The global digital space has become the frequent site of merciless information wars, computer attacks, including against critical information infrastructure, and unfair competition and misuse by private companies. Key threats include the use of information and communications technology (ICT) in military, political and other areas to undermine sovereignty, violate territorial integrity and interfere in the internal affairs of States; the dissemination of malware through open sources; and the use of ICT for terrorist, extremist or criminal purposes. These threats have fundamentally changed the world and put international security at heightened risk.

Russia was among the first nations to call on the international community to join efforts in this new area. In 1998, at our initiative, the General Assembly adopted a resolution on developments in the field of information and telecommunications in the context of international security. The resolution was a call for the broadest possible cooperation in combating common threats in the information sphere, first and foremost the attempts to use the latest information technologies to undermine international peace and stability. Our efforts have placed the topic of information security on the agenda of the General Assembly and have ensured that the resolution on international information security takes place every year.

Russia was also behind the initiative, in 2004, to establish the Group of Governmental Experts, the first of its kind United Nations expert forum for discussing security aspects of ICT. Since then, there have been six Groups of Governmental Experts. The rapid developments in the information space have made it possible to take discussions to a whole new level.

In 2018, the majority of the States Members of the United Nations voted to adopt the resolution on international information security sponsored by Russia. The resolution set forth an initial set of rules, norms and principles for responsible State behaviour with regard to the use of ICT. The General Assembly also decided to convene an open-ended working group, in order to further develop that list and, in general, conduct the discussion of international information security in a more democratic manner. The group completed its work, and the Member States adopted its final report by consensus on 12 March 2021, in New York.

Russia worked together with like-minded delegations to ensure the continuity of the negotiation process under the auspices of the United Nations by establishing a new open-ended working group on security of and in the use of information and communications technologies 2021–2025. The group's mandate is to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation. The working group will do this primarily by reaching a common understanding of information security threats, the applicability of international law to the use of ICT by States, confidence-building and capacity-building measures, and by strengthening ties among relevant agencies. The group ensures that States play a leading role in the discussion and provides non-governmental organizations the opportunity to participate.

The Russian Federation takes a transparent and consistent approach to ensuring international information security. International information security was designated as a strategic national priority in the national security strategy of the Russian Federation, approved by Presidential Decree No. 400 of 2 July 2021. In accordance with the State policy framework of the Russian Federation in the field of international information security, approved by Presidential Decree No. 213 of 12 April 2021, the purpose of the State policy is to promote the establishment of an international legal regime to regulate the global information space.

We believe universal legally binding agreements are necessary to prevent conflicts and to foster mutually beneficial cooperation in the information space. The draft convention on countering the use of ICT for criminal purposes, put forward by Russia in the special committee established at our initiative, could serve as the basis for such agreements, as could the Russian proposal for a United Nations convention on international information security.

ICT should serve sustainable development goals and enable favourable conditions for scientific inquiry and the rapid implementation of technical solutions. With a view to ensuring that these principles are incorporated into future universally agreed and equitable legal obligations, in 2021, Russia and the United States of America initiated the adoption of General Assembly resolution 76/19, by consensus, with 108 Member States joining the list of sponsors.

Russia believes in the inviolability of the digital sovereignty of States. Every country can and should set its own parameters for regulating its information space and related infrastructure. Russia insists on the internationalization of, and the equal rights of States in, Internet governance. Any attempts to limit the sovereign right of States to regulate and secure national segments of the global network are unacceptable.

It is important for legal measures to be put in place at the national or the international levels to prevent certain States from dominating the digital sphere. It is important to take steps to ensure that the rights of all users in the information space receive reliable and equal protection. No single State or group of countries may unilaterally establish principles, rules and standards for the operation of the Internet. To that end, Russia insists that Internet governance be placed within the competence of the International Telecommunication Union, a United Nations specialized agency with the necessary expertise in the field of telecommunications and ICT.

As before, Russia is open to dialogue and constructive cooperation with all its partners, both bilaterally and through international bodies and forums, primarily, in the United Nations.

Singapore

[Original: English]
[31 May 2022]

Singapore is strongly committed to the strengthening 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. Singapore believes it is crucial that discussions on such issues, including on laws, rules and norms relating to responsible State behaviour, 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 Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, established pursuant to General Assembly resolution 73/27. We are participating actively in and support the Chair's efforts for an action-oriented open-ended working group on security of and in the use of information and communications technologies 2021–2025 to advance discussions on international cybernorms and the agreed framework for responsible State behaviour in cyberspace. We remain committed to contributing constructively to the working group process to further strengthen international cooperation and make progress on advancing responsible State behaviour in cyberspace. As 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.

Rules, norms and principles of responsible behaviour of States

Singapore believes that additional efforts are needed to promote awareness of the existing voluntary, non-binding norms of responsible State behaviour and to support their implementation. Singapore also supports the further elaboration of such norms where needed. For example, cross-border critical information infrastructure that provides services across several States, the protection of which 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 information and communications technology (ICT) threats to such infrastructure could have destabilizing effects regionally and globally.[3]

Regional organisations can play an important role in supporting the implementation of the existing normative framework. The Association of Southeast

[3] Cross-border critical information infrastructure is critical information infrastructure owned by private companies and operating across national borders, but not under any single State's jurisdiction.

Asian Nations (ASEAN) has subscribed in principle to the 11 voluntary, non-binding norms on responsible State behaviour in the use of ICTs and to date remains the only regional organization to have adopted these norms. At the sixth ASEAN Ministerial Conference on Cybersecurity, held in 2021, participants discussed the progress of the ASEAN long-term regional action plan on the implementation of norms of responsible State behaviour in cyberspace, which seeks to ensure effective and practical implementation of these norms, including in the areas of cooperation among computer emergency response teams, protection of critical information infrastructure and mutual assistance in cybersecurity. The regional action plan was endorsed at the second ASEAN Cybersecurity Coordinating Committee in November 2021 and remains a living document for further review. The ASEAN cybersecurity cooperation strategy for the period 2021–2025 updated the ASEAN strategy for cybersecurity cooperation to create a safer and more secure cyberspace in the ASEAN region. ASEAN has agreed to establish a regional computer emergency response team, which will contain the ASEAN computer emergency response team information exchange mechanism, to strengthen the Association's response to cybersecurity incidents. Through the ASEAN Regional Forum points of contact directory on security of and in the use of ICTs, members of the Forum are able to contact their counterparts in the event of a cyberincident.

Capacity-building

Singapore believes that capacity-building is an essential pillar of the agreed normative framework, insofar as it is important to ensure that all States have the capacity to implement the normative framework and their obligations under international law. In line with this, Singapore is committed to sharing our experience and expertise with fellow States Members of the United Nations, especially small developing countries, at the regional and global level.

To support capacity-building at the regional (ASEAN) level, Singapore established the ASEAN Cyber Capacity Programme in 2016 to support capacity-building in ASEAN countries on cyberpolicy, as well as operational and technical issues. Following positive feedback from international partners and participants on the Programme, Singapore announced the establishment of the ASEAN-Singapore Cybersecurity Centre of Excellence in October 2019, with a commitment of $30 million over five years until 2023, to carry out cybersecurity training programmes for senior ASEAN policy and technical officials. The Centre's campus was officially opened in October 2021 during Singapore International Cyber Week. To date, the Centre has delivered more than 30 programmes attended by over 1,250 senior officials from ASEAN and beyond, and has collaborated with over 40 partners across Governments, the private sector, academia and non-governmental organizations. Despite travel restrictions arising from the coronavirus disease (COVID-19) pandemic, the Centre continued to conduct training programmes online and has organized 21 virtual capacity-building programmes since May 2020.

At the global level, Singapore is working in partnership with the Office for Disarmament Affairs on the following initiatives:

(a) Under the United Nations-Singapore Cyber Programme, Singapore is developing a norms implementation checklist through a series of workshops across various regions, in partnership with the Office for Disarmament Affairs. The checklist will take the form of a guide setting out a set of actions that developing countries can take towards implementing the 11 voluntary, non-binding norms on responsible State behaviour. Singapore held the first workshop on norms implementation to develop the checklist with States members of ASEAN in March 2022, which focused on implementing norms on critical infrastructure protection, vulnerability reporting and the protection of computer emergency response teams and cybersecurity incident response teams;

(b) In late 2022, the Office for Disarmament Affairs and Singapore will co-organize the United Nations-Singapore Cyber Fellowship, a programme that is designed to equip senior government officials from States Members of the United Nations with the necessary interdisciplinary expertise to effectively oversee national cybersecurity and digital security policy, strategy and operations.

Confidence-building measures

Singapore is also of the view that further efforts should be undertaken by the international community to develop confidence-building measures in support of the agreed normative framework, given that such measures have the potential to reduce the risk of misunderstandings occurring, as well as prevent and de-escalate conflict in cyberspace. In line with this, Singapore supports the establishment of a global directory of national points of contact at the operational or technical level, as recommended by the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. In the second half of 2022, Singapore will also conduct the first of a series of table-top exercises for national cyber points of contact in partnership with the United Nations Institute for Disarmament Research (UNIDIR). The exercises will (a) provide an opportunity for all States Members of the United Nations to participate in a substantive cyberexercise regardless of current technical capacity and/or regional organization affiliation status; (b) improve the capabilities of national cyber points of contact to respond to real-world incidents and cybercrises; and (c) demonstrate the effectiveness and value of the proposed global directory of points of contact. Such exercises have previously been organized at the regional level between computer emergency response teams, but have not been open to all interested States Members of the United Nations, especially those outside of established regional computer emergency response team networks. To address this, Singapore's the table-top exercise programme will be the first exercise open to all Member States.

National-level efforts

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

Building a resilient infrastructure

Entities owning and operating our core digital infrastructure have to abide by a cybersecurity code of practice, which details cyberhygiene measures that such entities should practice, such as keeping systems and software updated, maintaining updated backups of key data and detecting cyberintrusions swiftly. Alerts and advisories are also issued when needed to complement the code of practice to address evolving threats (e.g. ransomware). In addition, 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 the critical information infrastructure sectors of Singapore 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. The Agency also launched the operational technology core competency framework, which enterprises can leverage to establish processes, structures or jobs to manage operational technology cybersecurity within their organizations. In 2022, the Agency will launch a critical information infrastructure supply chain programme, involving stakeholders such as government agencies, critical information infrastructure owners and their vendors. The programme will provide recommended processes and sound practices for all stakeholders to manage cybersecurity risks in the supply chain.

Enabling 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: (a) secure the core digital infrastructure of Singapore; (b) safeguard cyberspace activities; and (c) empower our cybersavvy population. The Master Plan outlines 11 initiatives aimed at increasing the adoption of security by design among enterprises and organizations, as well as enhancing cybersecurity awareness and good cyberhygiene practices among end users. All enterprises and organizations have a role to play in safeguarding our broader cyberspace activities. To facilitate this, the Agency has launched a number of schemes to raise stakeholder awareness of cybersecurity, such as cybersecurity toolkits targeted at different enterprise stakeholders. This is complemented by cybersecurity certification for enterprises in the form of the Cyber Trust and Cyber Essentials marks to recognize enterprises with comprehensive cybersecurity measures and practices.

The Cyber Security Agency has issued public advisories to guide enterprises and the general public on managing and navigating cyberrelated vulnerabilities and threats when they arise. For example, the Agency issued a public advisory on the recent Log4Shell vulnerability and worked with trade associations and chambers to brief Singaporean enterprises on how to address the vulnerability and secure their systems. Additionally, the Agency has standing advisories addressing cybercrime, such as a public advisory discouraging victims from paying ransoms to ransomware actors.

There are increasing cybersecurity risks associated with the proliferation of the Internet of things, given its expansive connectivity and lack of cybersecurity provisioning. The Cyber Security Agency has leveraged technical standards to raise cyberhygiene and provide assurance on products and services. In 2020, the Agency launched the Cybersecurity Labelling Scheme for consumer Internet of things devices. Over 150 labelled products are now on the market. Singapore is also a strong advocate of international rule-based standards and is a certificate-authorizing nation under the common criteria recognition arrangement.[4] International standards will help to raise cyberhygiene, secure cyberspace collaboratively and lower barriers to trade across borders. Singapore hopes to work with like-minded partners to develop a universal labelling framework for the security of the consumer Internet of things to harmonize established international standards and labelling requirements, as well as to facilitate mutual recognition of such standards. This would serve to minimize the fragmentation of standards, eradicate duplicated testing across countries, reduce the cost of compliance with national regulations and facilitate market access for developers.

Developing a vibrant cybersecurity ecosystem

Singapore recognizes that strengthening cybersecurity involves building up the cyberecosystem and encouraging innovation within the industry. Given the rapidly evolving cyberthreat landscape, cybersecurity firms need to constantly innovate and invest in new solutions to stay ahead of the curve. The Cyber Security Agency supports industry-led innovation in cybersecurity through the Cybersecurity Industry

[4] See www.commoncriteriaportal.org.

Call for Innovation. This encourages cybersecurity companies to develop innovative solutions to address the cybersecurity needs of key local end users (e.g. entities owning and operating core digital infrastructure, and the commercial sector), as well as stimulate demand in the country's cybersecurity industry. There is also a growing need to develop a pool of talented individuals who can assume cybersecurity leadership roles in organizations. The 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.

Türkiye

[Original: English]
[31 May 2022]

In accordance with the assessments and recommendations contained in the report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, the views and assessments of Türkiye on the efforts taken at the national level to strengthen information security and promote international cooperation in the field of information and telecommunications in the context of international security, as well as the content of the concepts mentioned in the related reports, are presented below.

As is highlighted in the aforementioned reports, the imperative of building and maintaining international peace, security, cooperation and trust in the information and communications technologies (ICT) environment has never been so clear. Especially due to the spread of digital technologies and their transboundary nature, the security of ICT has become one of the primary elements of national defence and international security as cyberthreats and crimes diversify and expand. Therefore, Member States are making intensive efforts to put in place the required technical infrastructure, institutional capacity and human capital in the field of national security. In order to proactively prevent the potential risks to the national security of Türkiye, necessary actions such as developing technologies relating to cybersecurity and data privacy, addressing the gaps regarding the availability of qualified human resources, completing institutional restructuring, keeping the legal infrastructure up to date and ensuring compliance with evolving technologies are being planned and undertaken. Moreover, there is a need for cooperation, especially at the international level, to counter cybercrime. In this regard, the goal is to further develop knowledge- and information-sharing and international cooperation in order to detect the source of cybercrime and the criminals involved in the most efficient manner.

Türkiye focuses on taking measures necessary in order to improve national cybersecurity. The Ministry of Transport and Infrastructure is the body responsible for policymaking and developing strategies and action plans on national cybersecurity in Türkiye. Within 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. Türkiye has developed the national cybersecurity strategy and action plan for the period 2020–2023 with the participation of all relevant stakeholders in study groups under the coordination of the Ministry.

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

- Protecting critical infrastructure and increasing resilience
- National capacity-building
- Organic cybersecurity network
- Security of new-generation technologies
- Fighting against cybercrime
- Developing and fostering domestic and national technologies
- Integrating cybersecurity into national security
- Improving international cooperation.

Monitoring and measurement related to the action plan are carried out by the Ministry of Transport and Infrastructure on the basis of determined implementation steps, activities that are being implemented by the responsible institutions and organizations, and measurement criteria.

At the same time, the national computer emergency response team of Türkiye, which is located within the Information and Communication Technologies Authority, has been coordinating the country's cyberincident response since 2013. Besides 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 in cybersecurity of the national computer emergency response team are the following:

- Building of cybercapacity
- Technological measures
- Gathering and disseminating threat intelligence
- Protection of critical infrastructure.

Within the context of improving national cybersecurity, 14 sectoral computer emergency response teams for critical sectors and infrastructure (such as energy, health, banking and finance, water management, electronic communications and critical public services) and more than 2,000 institutional computer emergency response teams have also been established since 2013. All teams work 24 hours a day, seven days a week, under the coordination of the national team, in order to mitigate cyberrisks and combat cyberthreats. The national team uses detection and prevention tools for monitoring, and reporting tools for information-sharing with relevant parties. It has developed the communication platform for all computer emergency response teams within Türkiye in order to distribute alarms, warnings and security notices, which provides an efficient and secure communications channel.

The national team organizes and supports training courses, summer camps and competitions on cybersecurity, which are open to several communities. In addition, it provides training to computer emergency response teams on topics such as malware analysis and log analysis. Over 5,000 people had been trained in different areas of cybersecurity by the national team as of April 2022.

The national team has been accepted into the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) programme and, in this context, it assigns CVE numbers for the vulnerabilities of third-party software, hardware or products and provides process coordination in vulnerability management.

In addition, BTK Academy, the training centre of the Information and Communication Technologies Authority, which was established in 2017, provides online training open to the public on cybersecurity and other related areas in order to contribute to increased expertise within the human resources of Türkiye. Training contents are 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 related topics such as cybersecurity and the protection of critical infrastructure.

The annually organized Safer Internet Day is among the awareness-raising activities of the Information and Communication Technologies Authority, the main objective of which is the conscious and safe use of the Internet. An Internet helpline and a safe web website, where families can find advice on the efficient use of the Internet, is publicly available on the official safer web portal (www.guvenlinet.org.tr).

Additionally, online and face-to-face training and seminars are being held for students, teachers and parents on the conscious and safe use of the Internet. Moreover, many students have been reached by making school visits with the Safer Internet Truck, which serves to ensure that children and the young throughout the country interact directly with new technologies, and use technology and the Internet correctly, and to raise awareness on this issue.

Türkiye also takes steps to counter increased digital security risks to ensure cybersecurity and has taken measures during 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, the malicious links of these cyberthreats are determined and prevented in order to protect critical infrastructure and citizens. Within this scope, cyberintelligence reports are prepared and shared with relevant parties. Several 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.

Furthermore, national occupational standards for cybersecurity staff (level 5) entered into force upon their publication in the *Official Gazette*.

Türkiye has assumed important roles in many organizations, either as a founding member or by contributing to cooperation efforts on cybersecurity and information security issues. In this context, Türkiye gives utmost importance to information-sharing with different countries and organizations. Türkiye is a member of the International Telecommunication Union, and the national computer emergency response team is a member of the Forum of Incident Response and Security Teams, Trusted Introducers, 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 Islamic

Cooperation. Türkiye has also taken part in the NATO Cooperative Cyber Defence Centre of Excellence as a sponsoring country since November 2015. In addition, there are ongoing efforts related to bilateral and multilateral cooperation on cybersecurity, such as memorandums of understanding signed with many countries. In addition, Türkiye supports active participation and contribution 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 Organization of Turkic States, the Economic Cooperation Organization, the Developing Eight Countries Organization for Economic Cooperation, 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 at the national and international levels contributes to strengthening cyberspace and the testing of measures to be taken against potential cyberthreats. Since 2011, five national and two international cybersecurity exercises have been carried out in Türkiye. Most recently, the national Cyber Shield 2021 exercise was held on 12 and 13 October 2021 in cooperation with the Ministry of Transport and Infrastructure and the Information and Communication Technologies Authority, with the participation of public institutions and organizations. Furthermore, the international Cyber Shield 2019 Exercise was co-organized by the Ministry and the Authority on 19 December 2019 in Ankara. The exercise was supported by ITU and the Cybersecurity Alliance for Mutual Progress. Additionally, Türkiye continues to participate in and contribute to various international cybersecurity exercises, such as NATO Locked Shields, the NATO Cyber Coalition and the NATO Crisis Management Exercise. In addition to other capacity-building and guidance studies, international cybersecurity exercises remain essential for increasing preparedness levels and building cyberincident response capacities across the world.

Another significant institution in the field of national ICT policies is the Digital Transformation Office of the Presidency of Türkiye.

One of the most important and outstanding studies conducted by the Digital Transformation Office is the publication of the Information and Communication Security Guide on 24 July 2020. The Guide is the primary national reference document published in the field. It plays an important role in strengthening the cyberdefence capabilities of public institutions and providers of critical infrastructure services.

Public institutions and providers of critical infrastructure services are expected to complete their compliance activities within the period specified in the Guide, and should carry out audits at least once a year. Audit policies and procedures that must be conducted by the institutions in that regard are documented in the Information and Communication Security Audit Guide published by the Digital Transformation Office.

Furthermore, the Critical Infrastructures National Test Bed Centre, which hosts studies to ensure the security of electricity distribution and water management infrastructure, was inaugurated with the cooperation of related parties in Türkiye. The Centre, where energy and water management systems are modelled, is designed to present a working environment in order to search for and develop protective and preventive solutions related to the security of critical infrastructure and to contribute to the cybersecurity ecosystem.

Developing projects to improve the security of information and cybersecurity is one of the main responsibilities of the Digital Transformation Office as defined by the articles incorporated by Presidential Decree No. 48 published in *Official Gazette*

No. 30928, dated 24 October 2019, into the Presidential Decree on Presidential Organization No. 1, published in *Official Gazette* No. 30474, dated 10 July 2018.

In this context, various projects related to information and cybersecurity have been conducted, including the Cyber Intelligence Contest and the HackZeugma Capture the Flag competition:

- The Cyber Intelligence Contest is a part of training and awareness-activities aimed at increasing the number of individuals with cybersecurity awareness; it has proven very effective in this regard. The Digital Transformation Office organized the second Cyber Intelligence Contest as part of cyberawareness month activities in 2021
- The HackZeugma Capture the Flag competition was organized by the Digital Transformation Office as part of the 2020 Teknofest Aerospace and Technology Festival. HackZeugma is a competition that opens its doors to thousands of hackers around the world to allow them to demonstrate their talents. The competition is prepared with a special focus on the security of operational technology systems.

Furthermore, the 1 Million Employment Project was launched in order to create a qualified workforce in the field of information technologies and to increase employment by bringing the trained workforce together with employers. New features of the Project, which enable employers to scan résumés by registering for free and without conditions, are available. The Project, which is under the ownership of the Ministry of Treasury and Finance, aims to make 1 million people ready for employment in the field of information technologies by 2023 and is carried out within the scope of the “National Technology Move” goals in order to achieve digital transformation in our country.

The Turkish Cyber Security Cluster is a platform closely followed and supported by the Digital Transformation Office, principally aiming for a Türkiye that produces technology in the field of cybersecurity and is able to compete with the world, in accordance with the missions of building a national cybersecurity ecosystem, developing local and national cybersecurity products and disseminating their usage. Activities conducted by the Cluster include:

- Establishing a test and analysis laboratory that provides infrastructure for the testing and development of the sector
- Establishing a certification laboratory
- Establishing the cybersecurity academy
- Organizing national and international activities such as conferences, training, seminars, panels and fairs, and coordinating requests and supplies of internship activities
- Supporting the opening of associate degree, undergraduate and postgraduate education programmes.

In addition to the above-mentioned efforts, industry standards as an approach to improving cybersecurity among critical infrastructure owners and operators have been established by the Turkish Standards Institution and the Digital Transformation Office. Studies related to International Organization for Standardization/International Electrotechnical Commission standards 27701, 27011, 27017, 27018, 27019, 27031, 27799, 31000 and 62443 have been completed, and standards regarding critical infrastructure have been published by the Turkish Standards Institution.

Developing international cooperation, along with national activities, is of great importance given the nature of cybersecurity. With the use of ICT spreading over a wide spectrum, the relationship established by these technologies with topics such as international peace, stability and security, and fundamental rights and freedoms is continuously developing. This situation necessitates efforts to use ICTs for peaceful purposes and to ensure that international stability and security is addressed continuously by States. It is evident that international law, norms and rules expressed in the reports of the Group of Governmental Experts and the Working Group and the relevant studies contribute to a common framework of responsible State behaviour in the use of ICTs in the context of international peace and security. As articulated in the said reports, concepts such as the development of international cooperation, respect for fundamental rights and freedoms, protection of critical infrastructure and prevention of malicious use of ICTs will maintain their importance in efforts towards international stability and security in the coming period.

At the same time, the importance of protecting State sovereignty in cyberspace and the need to develop new norms in addition to existing ones should also be considered. Improving collaboration and supporting information- and experience-sharing mechanisms are vital for fighting against cyberthreats and need to be given due consideration.

Türkiye is aware of the importance of the implementation of international law, the norms of responsible State behaviour in cyberspace and confidence-building measures, and the need for effective international cooperation, and resolutely takes the steps necessary to accomplish these goals.

Ukraine

[Original: English]
[31 May 2022]

Ukraine has long been a victim of Russia’s ongoing armed aggression and a target of cyberattacks within its framework, including against Ukraine’s critical infrastructure. Accordingly, Ukraine fully shares the justified concern expressed in the fifth preambular paragraph of General Assembly resolution 76/19, with the proviso that information technologies and means not only can potentially be used, but already are a tool actively applied in practice by the aggressor State, and not only against Ukraine.

Russia’s repeatedly confirmed inability to observe its international obligations calls into question its willingness to also comply with the provisions of operative paragraphs 3 and 6 of resolution 76/19.

The same applies to the conceived comprehensive international convention on countering the use of information and communications technologies for criminal purposes that Moscow proposed to elaborate. This is because if Russia’s designed provisions for its draft, which create the risk of a serious restriction of the rights and freedoms of citizens, do not pass into the convention’s final version, then the convention will not be of interest to Moscow.

Such a restriction, which is proposed in the Russian draft convention, is unacceptable to Ukraine and other democratic States that are parties to the 2001 Council of Europe Convention on Cybercrime, but it suits authoritarian regimes, including those in Russia and Belarus, that did not become a party to the Convention.

Despite Russia’s military and cyber aggression, Ukraine is further strengthening its cybersecurity system, with the material and advisory assistance of Western partners.

The national cybersecurity system put in place by the Cybersecurity Strategy of Ukraine is based on the Ministry of Defence, the State Service of Special

Communications and Information Protection, the Security Service, the National Police and the National Bank. It ensures collaboration between all government agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civil groups, businesses and organizations, irrespective of their form of ownership, that deal with electronic communications and information security or are owners of critical information infrastructure.

The subjects of ensuring the national cybersecurity system are familiar with the assessments and recommendations contained in the reports of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.

The National Security and Defence Council of Ukraine coordinates and controls activities of the entities of the security and defence sector, ensuring the cybersecurity of Ukraine through its working body, the National Cybersecurity Coordination Centre.

The Centre has a supervising function and undertakes tasks related to analysing the state of national cybersecurity and preparedness for combating cyberthreats, as well as forecasting and detecting relevant potential and actual threats.

Having implemented the previous Cybersecurity Strategy of Ukraine for the period 2016–2020, the State was able to form the core of the national cybersecurity system. Ukraine has increased the potential that allows for further development of the system on the basis of deterrence, cyberresilience and interaction.

The purpose of the current Cybersecurity Strategy of Ukraine, established for the period 2021–2025, is to create conditions for the safe functioning of cyberspace and its use in the interests of the individual, society and the State. The document is based on the principles of deterrence, cyberresilience and interaction.

The above-mentioned efforts allowed Ukraine to identify the Russian preparation of the malicious cyberattacks against Ukrainian infrastructure which coincided with the physical aggression. From autumn 2021, we saw the increasing number of Russian-affiliated hackers' groups attacks against important Ukrainian suppliers of digital and telecommunications services. These attacks also increased in quality, becoming more targeted and using more sophisticated tools.

It should be noted, however, that most of those cyberattacks were not successful. Our stakeholders, with the support of our international partners, detected and mitigated them.

Ukraine is actively developing cooperation in the cyberdomain, primarily with the United States, the United Kingdom, Estonia and other Western partner countries, the European Union and the North Atlantic Treaty Organization (NATO). It is receiving financial assistance, as well as advice, through bilateral and multinational training courses, seminars and conferences abroad and in Ukraine, along with assistance, modern hardware and software to address cybersecurity needs, conduct professional computer forensics and investigate cybercrimes.

Ukraine is grateful for the recent statement of the United States, the United Kingdom, the European Union and other countries and institutions which condemns Russian aggressive actions in cyberspace against Ukraine and other countries.

Since 2016, the Ministry of Foreign Affairs of Ukraine has organized 22 rounds of bilateral cyberconsultations with 13 countries (Japan, Singapore, Malaysia, Finland, United States, Germany, United Kingdom, Estonia, Netherlands, Slovenia, Spain, Brazil and Israel). Such consultations with a number of States were planned for 2022, but were postponed due to the Russian military invasion.

In the cyberdefence field, Ukraine has been closely cooperating with the NATO cyberdefence trust fund to enhance the country's technical capabilities in countering cyberthreats and looks forward to effective cooperation with the alliance as a contributing country of the NATO Cooperative Cyber Defence Centre of Excellence.

Ukraine will be grateful to all those States Members of the United Nations that may assist in the implementation of the following projects that are being implemented in accordance with the country's current cybersecurity strategy to strengthen capacities in the field of cybersecurity and cyberdefence, and to develop the information technology infrastructure and services of a network of State situation centres:

- Building cyberrange and conducting nationwide cyberexercises
- Cyberthreat intelligence tools for technological platforms
- National backup centre for critical State information resources
- National cyberthreat monitoring system
- State cloud cybersecurity service platform.

The Ministry of Foreign Affairs is ready to provide detailed information about these projects and assist in establishing contact with their executors.

Ukraine's experience demonstrates that in order to address serious and persistent cyberthreats and cyberattacks, there is a need for enhanced collaboration at multiple levels: among national authorities, with the private sector and with international partners, in order to build the necessary capacities and respond effectively to such threats.

III. Replies received from intergovernmental organizations

European Union

[Original: English]
[31 May 2022]

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 an open, free, global, 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 and information and communications technologies (ICTs) become more embedded in our lives, our reliance on these technologies has made us increasingly vulnerable to their misuse. Cyberspace is increasingly being exploited for malicious purposes, and increased polarization at the international level is hindering effective multilateralism. Russia's irresponsible behaviour in cyberspace forms an integral part of its illegal and unjustified invasion of Ukraine and is contrary to the expectations set by all States Members of the United Nations, including the Russian Federation, on the agreed United Nations norms of responsible State behaviour. Equally, 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 ICT products and services, threaten an open, free, global, stable and secure cyberspace, as well as democracy, the rule of law, human rights and fundamental freedoms.

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 risk of conflict. Malicious use of ICTs undermines the benefits that the Internet and ICTs provide to society at large and shows the readiness of some actors to threaten international peace, security and stability. All actors should refrain from conducting irresponsible and destabilizing activities in cyberspace.

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

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 ICTs for malicious purposes and strengthens the ability of States to effectively respond to and recover from cyberincidents. The European Union and its member States strongly support the aforementioned vision of an open, free, global, stable and secure cyberspace, through advancing and implementing an inclusive and multifaceted strategic framework for conflict prevention and stability in cyberspace, including through bilateral, regional and multi-stakeholder engagement. As part of this strategic framework, the European Union works to strengthen global resilience, advance and promote a common understanding of the rules-based international order in cyberspace, and develop and implement practical cooperative measures, including regional confidence-building measures.

The 2013 cybersecurity strategy entitled “An Open, Safe and Secure Cyberspace”,[5] 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 the 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.

In February 2015, the Council of the European Union stressed in its Council conclusions on cyberdiplomacy[6] 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 freedom of 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.

[5] 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”.

[6] 6122/15, Council Conclusions on Cyber Diplomacy.

Based on a review of the 2013 cybersecurity strategy, the European Union further strengthened its cybersecurity structures and capabilities in a coordinated manner, with the full cooperation of the member States and the different European Union structures concerned, while respecting their competencies and responsibilities. In 2017, the joint communication entitled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[7] 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 ever-increasing cybersecurity challenges gave an impetus to the development of a framework for a joint European Union diplomatic response to malicious cyberactivities: the cyberdiplomacy toolbox.[8] 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 an open, free, global, stable 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[9] for a cybersecure digital transformation in a complex threat environment. The European Union's cybersecurity strategy for the digital decade aims to promote and protect an open, free, global, stable and secure cyberspace grounded in human rights, 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's adherence 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 law in 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 an open, free, global, stable and secure

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

[8] 9916/17, Draft Council Conclusions on a Framework for a Joint European Union Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

[9] See Joint Communication to the European Parliament and the Council on the European Union's Cybersecurity Strategy for the Digital Decade and 7290/21 of 22 March 2021, Council Conclusions on the European Union's Cybersecurity Strategy for the Digital Decade.

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 advance peace and security in cyberspace, there is a clear need to implement the United Nations framework for responsible State behaviour in cyberspace as agreed upon by the previous Group of Governmental Experts and the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and endorsed by the General Assembly. Together with 60 States Members of the United Nations, the European Union proposes to establish a programme of action to advance responsible State behaviour in cyberspace.

Building on the existing acquis as unanimously endorsed by the General Assembly, the programme of action offers a permanent, inclusive and action-oriented mechanism at the United Nations to advance the implementation of the consensus reports and to support States in their national cybersecurity policies, in particular through 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 programme of action would operate in a complementary and coordinated manner with other relevant processes, such as the open-ended working group on security of and in the use of information and communications technologies 2021–2025.

In order to strengthen its ability to anticipate, deter and respond to current and fast-emerging threats and challenges, and safeguard the European Union's security interest, the European Union formally approved the Strategic Compass[10] on 21 March 2022. The Compass gives the European Union an ambitious plan of action for strengthening its security and defence policy by 2030, including strengthening the European Union cyberdiplomacy toolbox and further developing the European Union cyberdefence policy to be better prepared for and respond to cyberattacks.

The European Union and its member States recall the adoption on 23 May 2022 of the Council of the European Union conclusions on developing the Union's cyberposture. The posture aims to demonstrate the European Union's determination to provide immediate and long-term responses to threat actors seeking to deny the European Union secure and open access to cyberspace.

Content of the concepts mentioned in the report of the Working Group and 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, the serious ICT threats identified in previous reports by the Group of Governmental Experts and in the report of the Working Group[11] persist and present continuously evolving challenges.

The European Union and its member States are concerned by the rise in malicious behaviour in cyberspace, including the misuse 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

[10] 7371/22, "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security".

[11] A/75/816.

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.

The coronavirus disease (COVID-19) pandemic has demonstrated the risks and consequences of malicious ICT activities. The European Union and its member States have observed cyberthreats and malicious cyberactivities targeting essential operators and acknowledge the vulnerability of critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet, and health and other critical sector entities in member States and their partners. The European Union and its member States are in particular alarmed by the increase in activities affecting the security and integrity of ICT products and services, which might have systemic effects. Also in the context of Russia's irresponsible behaviour in cyberspace as an integral part of its illegal and unjustified invasion of Ukraine, the European Union and its member States have seen the use of cyberattacks involving destructive instruments, such as wipers to cause system breakdowns, but also service disruptions, intrusion attempts, defacements and distributed denial of service attacks targeting Ukraine, with the potential for spillover into other countries, in particular Ukraine's neighbours.

The European Union and its member States condemn this malicious behaviour in cyberspace, including malicious ICT activity aimed at exploiting vulnerabilities, and underline their continued support for increasing global cyberresilience. Any attempt to hamper critical infrastructure is unacceptable and can put people's lives at risk.

The European Union and its member States call upon every country to not knowingly allow their territory to be used for internationally wrongful acts in cyberspace using ICTs and to take appropriate actions against actors conducting such activities from their territory, consistent with international law and the 2010, 2013, 2015 and 2021 consensus reports of the Groups of Governmental Experts and of the Working Group in 2021. The European Union and its member States emphasize again that States should take all appropriate measures and reasonably available and feasible steps to detect, investigate and address the situation.

In addition, as recognized in previous reports of the Group of Governmental Experts and the Working Group, given the unique character of ICTs, the European Union's approach to addressing cyberissues in the context of international security remains adaptive to new technological developments, while noting that the norms of responsible State behaviour in cyberspace are technology-neutral. This is consistent with the concept and with the acknowledgement by the United Nations that existing international law applies to new areas.

The European Union and its member States can only support the development and use of technologies, systems or services enabled by ICTs that fully respect applicable international law and norms, particularly the Charter of the United Nations, as well as international humanitarian law and human rights law.

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, 2015 and 2021, as well as the principles established in paragraph 71 (b) to (g) of the 2021 report and the Working Group.

International law, including international humanitarian law, which incorporates the principles of humanity, distinction, precaution, military necessity and proportionality, 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 that international humanitarian law is not an enabler of conflict; rather, international humanitarian 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[12] and the General Assembly, as well as the Group of Governmental Experts and the Working Group.

For these reasons, the European Union and its member States do not call for the creation of new international legal instruments for cyberissues at this stage, emphasizing that more work needs to be undertaken to clarify how international law applies to cyberspace.

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

We continue to support ongoing efforts to promote the application of existing international law to cyberspace, including on exchanging information and best practices on the application of existing international law in cyberspace. We are committed to continuing to report on national positions on how international law applies to the use of ICT by States, as it promotes transparency and advances global understanding 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 raising awareness and capacity-building on 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 76/19, as well as to advance implementation of these agreed norms and confidence-building measures, which play an essential role in conflict prevention.

The European Union and its member States are and will be guided in their use of ICT by existing international law, as well as through adherence to voluntary, non-binding norms, rules and principles of responsible State behaviour and their implementation in cyberspace, as articulated in successive reports of the Group of Governmental Experts in 2010, 2013, 2015 and 2021. The continuation of an inclusive and constructive dialogue within the working group ___________ is welcome to further deepen the discussions on this framework and on the security challenges related to the use of ICTs. We believe that a practical way forward should encourage

[12] See Human Rights Council resolution 20/8.

increased cooperation and transparency to share best practices, including on how the existing norms of the Group of Governmental Experts are applied, through related initiatives and frameworks, such as regional organizations and institutions, to facilitate awareness-raising and to effectively implement agreed norms of responsible State behaviour.

Confidence-building measures

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

Developing and implementing cyberconfidence-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 of information and communications technologies

In order to prevent conflicts and reduce tensions stemming from the misuse of ICTs, the European Union and its member States aim to strengthen resilience globally, with particular emphasis on developing countries, as a means of addressing the challenges associated with the digitalization of economies and societies, as well as 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, 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, and identifying mechanisms that facilitate the engagement of all stakeholders in implementing the framework of responsible behaviour.