United Nations S/2021/621

Security Council

Distr.: General
1 July 2021

Original: English

Letter dated 1 July 2021 from the President of the Security Council addressed to the Secretary-General and the Permanent Representatives of the members of the Security Council

I have the honour to enclose herewith a copy of the briefing provided by Izumi Nakamitsu, High Representative for Disarmament Affairs, as well as the statements delivered by Kaja Kallas, Prime Minister of Estonia; Mahamadou Ouhoumoudou, Prime Minister of Niger; Simon Coveney, Minister for Foreign Affairs and Defence of Ireland; Bui Thanh Son, Minister for Foreign Affairs of Viet Nam; Joe Mucheru, Cabinet Secretary for Information Communications and Technology, Innovation, and Youth Affairs of Kenya; Linda Thomas-Greenfield, Permanent Representative of the United States and Member of President Biden's Cabinet; Harsh Vardhan Shringla, Foreign Secretary of India; Keisal M. Peters, Minister of State with responsibility for Foreign Affairs and Foreign Trade of Saint Vincent and the Grenadines; Audun Halvorsen, Deputy Minister for Foreign Affairs of Norway; Lord Tariq Ahmad of Wimbledon, Minister of State for the Commonwealth, the United Nations and South Asia of the United Kingdom of Great Britain and Northern Ireland; and Franck Riester, Minister Delegate for Foreign Trade and Economic Attractiveness attached to the Minister for Europe and Foreign Affairs of France, as well as by the representatives of China, Mexico, the Russian Federation and Tunisia in connection with the videoconference on the topic "Maintenance of international peace and security: cybersecurity" convened on Tuesday, 29 June 2021.

In accordance with the understanding reached among Council members for this videoconference, the following delegations submitted written statements, copies of which are also enclosed: Argentina, Australia, Austria, Bahrain, Belgium, Brazil, Canada, Chile, Czechia, Denmark, Ecuador, Egypt, El Salvador, European Union, Georgia, Germany, Greece, Guatemala, Indonesia, International Committee of the Red Cross, International Criminal Police Organization, Islamic Republic of Iran, Italy, Japan, Kazakhstan, Latvia, Liechtenstein, Malta, Morocco, Netherlands, New Zealand, Pakistan, Peru, Poland, Qatar, Republic of Korea, Romania, Senegal, Singapore, Slovakia, Slovenia, South Africa, Switzerland, Thailand, Turkey, Ukraine and United Arab Emirates.

In accordance with the procedure set out in the letter dated 7 May 2020 (S/2020/372) from the President of the Security Council addressed to the Permanent Representatives of the members of the Security Council, which was agreed in the light of the extraordinary circumstances caused by the coronavirus disease (COVID-19) pandemic, these briefings and statements will be issued as a document of the Security Council.

(*Signed*) Nicolas **de Rivière**
President of the Security Council

Annex I

Statement by the High Representative for Disarmament Affairs, Izumi Nakamitsu

I wish to express my appreciation to Estonia for organizing this meeting and for inviting me to provide a briefing at this open debate on maintaining international peace and security in cyberspace.

As of January this year, there are over 4.6 billion active users of the Internet worldwide. It is estimated that there will be 28.5 billion networked devices connected to the Internet by 2022, a significant increase from the 18 billion in 2017.

As advances in digital technologies continue to revolutionize human life, we must remain vigilant in our understanding of the malicious use of such technologies that could imperil the security of future generations.

Digital technologies are increasingly straining existing legal, humanitarian and ethical norms, non-proliferation, international stability, and peace and security.

They are also lowering barriers to access and opening new potential domains for conflict and the ability of both State and non-State actors to carry out attacks, including across international borders.

Specifically on information and communications technologies (ICT), we have seen a dramatic increase in the frequency of malicious incidents in recent years. These incidents have come in many forms, from disinformation to the disruption of computer networks. Such acts are contributing to a diminishing trust and confidence among States.

These developments also pose a specific risk to critical infrastructure that are enabled by ICT, such as the financial sector, electrical power grids and nuclear facilities. The Secretary-General has drawn attention to cyberattacks on health-care facilities during the pandemic, calling on the international community to do more to prevent and end these new forms of aggression, which can cause further severe harm to civilians.[1]

Such ICT threats also have a gendered impact and must be examined through this lens. Online violent extremism and trafficking have an often-overlooked differentiated impact on women, men and children, as do other ICT-related threats such as cyberstalking, intimate partner violence and the non-consensual dissemination of intimate information and images. This is also why we need to make every effort to secure the equal, full and effective participation of both women and men in decision-making in the digital arena.

ICT threats are increasing, but efforts are also under way to address them. Over the last one and a half decades at the United Nations, a series of five Groups of Governmental Experts have studied the existing and emerging threats of ICT to international security and recommended measures to address them. Two further United Nations processes, an Open-ended Working Group and a sixth Group of Governmental Experts, both established in 2018, have recently and successfully concluded their respective work, taking important steps forward on the topic through the adoption of concrete, action-oriented recommendations.

These two Groups affirmed a suite of voluntary, non-binding norms of responsible State behaviour, recognizing that additional norms could be developed

[1] See www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered.

over time. They also reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment. The Groups recommended confidence-building, capacity-building and cooperation measures, building on the work of previous processes. The Open-ended Working Group additionally, in accordance with its mandate, made conclusions and recommendations on establishing regular institutional dialogue on the issue of ICT.

As the most recent Group of Governmental Experts noted in its report, the measures recommended by the previous Groups of Governmental Experts and the Open-ended Working Group together represent an initial framework for responsible State behaviour in the use of ICT.[2]

A new, second Open-ended Working Group has also just held its organizational session and will begin its substantive work later this year.

At the regional level, regional organizations are now undertaking key efforts on ICT issues. Regional approaches have taken various forms as determined by different priorities and needs. Some regions have placed greater emphasis on implementing voluntary, non-binding norms of responsible State behaviour through capacity-building efforts, while others have pioneered their own regional confidence-building measures to reduce the risks of conflict stemming from ICT activities or adopted other regional tools for addressing ICT threats. Various regional instruments are also in place addressing specific aspects of ICT.

While States carry primary responsibility for maintaining international security, ICT are an integral part of our societies and other stakeholders have a key role and interest, as well as responsibility, in securing cyberspace.

Many excellent private-sector-led cyberinitiatives have been established, such as the Cybersecurity Tech Accord led by Microsoft, the Charter of Trust led by Siemens and the Munich Security Conference, and the Global Transparency Initiative of Kaspersky Lab.

The Paris Call for Trust and Security in Cyberspace of 2018 brought together industry, States, civil society and academia in a commitment to nine principles for cybersecurity. These principles cover a range of issues from developing ways to prevent the proliferation of malicious ICT tools and practices, to the promotion of widespread acceptance and operationalization of international norms for responsible behaviour, as well as confidence-building measures for cyberspace.

Perspectives from the private sector, civil society and academia contribute a unique and important part of the collective solution to cybersecurity that the international community is seeking.

The United Nations, for its part, stands ready to support States together with other stakeholders in promoting a peaceful ICT environment. The Secretary-General convened a high-level panel on digital cooperation, which issued its report in 2019. Through a subsequent series of roundtable discussions with States and other key stakeholders, a road map was developed, which recommended further actions to take forward cooperation in key areas in the digital space.

In the context of peace and security, the Secretary-General also launched an agenda for disarmament which places emphasis on understanding and addressing new

[2] See para. 21 of the report of the Group of Governmental Experts. An advance copy is available at https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

generation technologies that pose possible challenges to existing legal, humanitarian and ethical norms; non-proliferation; and peace and security.

In his agenda, the Secretary-General makes the commitment to engage and work with scientists, engineers and industry to encourage responsible innovation of science and technology and to ensure its application for peaceful purposes.

He also makes a second commitment to engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace.

While the digital space has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of ICT "insecurity" is also now recognized as a major concern. The political and technical difficulty of attributing and assigning responsibility for ICT attacks could result in significant consequences, including in unintended armed responses and escalation.

These dynamics can encourage States to adopt offensive postures for the hostile use of these technologies. It can also enable non-State armed and criminal groups and individuals seeking to develop or access potentially destabilizing capabilities with a high degree of impunity. Given these implications for the maintenance of international peace and security resulting from ICT threats, engagement by the Security Council on this issue is paramount.

I therefore welcome this opportunity to brief the Council, and I am looking forward to the discussion that will follow.

Annex II

Statement by the Prime Minister of Estonia, Kaja Kallas

The United Nations was created with the future in mind. Even as we face a number of new challenges, the values and principles agreed upon in the Charter of the United Nations 76 years ago remain just as valid today. Upholding them in our increasingly digital future has become one of the most pressing global tasks. Today, I want to talk about opportunities, threats and the mechanisms we have in place to address them.

First, opportunities: the last year and a half of remote working, studying and living has demonstrated clearly that our dependence on digital and communication technologies will only grow in time. We are responsible for building a future where all actors follow certain obligations in their behaviour in cyberspace.

This is why today's debate is not about technology, but about how cyberspace can be used. Steve Jobs described it well: "Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them".

As a thriving digital society, Estonia has experienced this first-hand. A free, open, stable and secure cyberspace is part of our lifeblood. We have saved an extra 2–3 per cent of our gross domestic product every year thanks to moving most government services online. Our routine public administration has been paperless for more than 15 years now. Estonia has also produced the highest number of technology unicorns per capita.

Second, threats: we must recognize that there is also a dark side to rapid digitalization.

Malicious actors can use cyberspace as another domain through which to wreak havoc. For example, imagine what would happen if in the middle of a drought, a country's water supply chain stopped operating or during the cold winter months, a nation's power grid was disrupted.

Over the past year, we have seen how harmful cyberactivities targeting the health-care sector can pose a real and tangible threat. The humanitarian effects of tampering with critical infrastructure could be devastating.

While we can put up high fences and guards around our power plants and other critical infrastructure, this can never be part of the solution in cyberspace. Instead, we must collectively take on the role of guardians.

Finally, how to address these threats: fortunately, as our distinguished briefer Ms. Nakamitsu also outlined, we have a solid basis from which to work.

During the last decade, Member States have agreed on an effective normative framework for cyberstability and conflict prevention. This consists of existing international law, 11 voluntary non-binding norms of responsible State behaviour, confidence-building measures and capacity-building.

Estonia holds the strong view that existing international law, including the Charter of the United Nations in its entirety, international humanitarian law and international human rights law, applies in cyberspace.

Let me emphasize that States are accountable for any acts committed contrary to their obligations under international law.

To ensure the protection of civilians and civilian objects in situations of armed conflict in particular, which the Security Council also regularly discusses, it is vital that any use of cybercapabilities in this context would be subject to obligations deriving from international humanitarian law.

The 11 norms of responsible State behaviour that we have agreed on reflect the expectations of the international community and set important additional guidelines for State activities in cyberspace.

This spring the international community delivered a very powerful reaffirmation of this normative framework. We are encouraged and guided by the successful consensus outcomes of both the latest Group of Governmental Experts and the Open-ended Working Group. Implementing this framework is a major goal for the international community.

Global efforts also need to be accompanied by regional activities and capacity-building. In this respect, we highlight the important work done by regional organizations to enhance confidence and advance cooperation. Estonia also prioritises efforts to close the digital divide, which must go hand in hand with capacity-building in cyberresilience, and with the protection of human rights online.

We must also recognize that we tackle cyberthreats together with the private sector, civil society and academia. Companies in particular have an important part to play by investing into cybersecurity and helping to eliminate vulnerabilities.

I am confident that today's discussion will leave a mark on Security Council history as we address the issues that will be all the more relevant for maintaining international peace and stability for years to come.

Our digital future will be secured only if we follow common rules of the road.

Annex III

Statement by the Prime Minister of the Republic of Niger, Ouhoumoudou Mahamoudou

[Original: French]

Allow me first of all to commend Estonia for its commitment to placing the question of security risks related to cyberspace on the agenda of the Council. I would also like to thank Ms. Izumi Nakamitsu for her briefing and her strong commitment to this issue.

Over the past two decades, the penetration of the Internet and the use of information and communications technologies (ICT) have grown at lightning speed. Today, cyberspace has become a geopolitical factor allowing various nations to expand their sphere of influence at the economic, political and cultural levels.

The digital revolution, which has brought us so close together by eliminating our borders, has also opened the way to new challenges to sovereignty owing to the extra-territorial nature of laws relating to it. In the same way that this space can strengthen our democracies by providing a platform and means for all voices to be heard, even those of dissidents, it can also prove to be a refuge for criminal actors and groups whose sole purpose is to destabilize our nations.

The coronavirus disease (COVID-19) pandemic has shown us the two facets of cyberspace: on the one hand, our growing dependence on digital technologies, of which this virtual meeting is an example, and on the other, the fragility of our systems when faced with possible cybercrimes and cyber espionage, demonstrated by ransomware attacks on health systems and disinformation campaigns with the purpose of undermining the confidence of our countries' citizens in vaccination efforts.

Furthermore, the flourishing of social networks and other discussion platforms gave rise to the proliferation of certain types of discourse inciting acts of insurrection, terrorism, attacks on moral values and the foundations of our democracies.

Given all the foregoing, allow me to make some recommendations that I believe could be likely to strengthen respect for international law, as well as the implementation of responsible rules for State engagement in cyberspace.

First, the digital divide between nations must be bridged, principally with the African continent, where three quarters of the populations do not have adequate access to the Internet, or no access at all.

As the experts have mentioned, this situation is a factor in deepening poverty, and its impact has repercussions on everyone and on every component of society, from health care to economic prosperity to education; it makes those areas more vulnerable to disinformation campaigns and other digital threats. We cannot hope for cyberspace that is healthy and safe without ensuring digital equity.

On this basis, my second recommendation is the development of a global architecture through an integrated and coordinated approach that will allow the rules of international law applicable to cyberspace to be clearly identified, in such vast fields as health care, international humanitarian law, the electoral process and economic activity, to name just a few.

But in so doing, we must also be aware that this architecture must be equitable, both in implementation and in making use of its benefits, in order to avoid creating new mechanisms applying double standards that will only deepen the inequalities among nations by forcing them to deal with other negative effects.

Along this line of thinking, it would be appropriate for any new regulatory architecture at the global level to be inspired by structures already established at the regional level, which are required to harmonize applicable regulations at the national and State level. We should thus mention the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime, which imposes obligations in that area on member States, including penalties for certain acts, and which creates a framework to facilitate regional cooperation on cybersecurity.

My final recommendation would be for the Security Council to work on a more inclusive and less discriminatory interpretation of the Charter of the United Nations, but also of its own mandate, so that our deliberations might reflect the realities of today’s world, and thus address such topics as cybersecurity, climate change and pandemics, for these are real threats, and just like COVID-19, they do not respect borders.

Annex IV

Statement by the Minister for Foreign Affairs and Defence of Ireland, Simon Coveney

My congratulations to Estonia on a successful Presidency of the Council.

My thanks also to the High Representative for her valuable insights.

I welcome this timely discussion, the first of its kind at the Security Council.

Speaking last year, the Secretary-General called on States to bring order to what he called the "Wild West of cyberspace".

While welcome progress has been made at the United Nations in recent months, the cybersecurity challenges faced by States continue to grow, endangering international peace and security.

I would like to focus my remarks today on three areas:

- Challenges and opportunities
- The need for States to implement measures agreed at the United Nations
- The importance of a values-based approach to this issue

Firstly, the challenges and opportunities.

Digital and communications technologies continue to drive economic growth and transform how we live, communicate and work.

Innovation is key to addressing some of today's critical global challenges, including climate change. It also facilitates important advances in medical research, improves access to education, and enhances the capabilities of our peacekeepers, helping them to keep safe.

Over the past year, the pandemic has highlighted our increasing reliance on information and communications technologies, bringing people together at times when they had to stay apart, while at the same time exposing our vulnerabilities.

I speak from recent experience on this last point. Ireland's public health-care systems were subjected to a very damaging ransomware attack last month that impacted critical medical services.

An attack of this kind during a global pandemic is appalling. Unfortunately, Ireland's experience is not isolated internationally.

Malicious cyberactivity, including crippling ransomware attacks, cybercrime, intellectual property theft and the spread of disinformation and hate, has surged in recent years.

Critical infrastructure is increasingly being targeted.

Ireland is gravely concerned that this activity poses a threat to international peace and security.

Existing security challenges are being compounded by cyberthreats, such as the vulnerability of nuclear-weapon command and control systems to cyberattacks. This adds fresh urgency to the need to make progress on nuclear disarmament.

We cannot allow cyberspace to be unconstrained by rules or laws, where malicious actors operate at will.

International disputes in cyberspace must be resolved by peaceful means.

The Council must send a clear message of support for a peaceful and secure global cyberspace built on consensus and mutual trust.

Turning to my second point, Ireland welcomes the recent progress at the United Nations on agreeing the framework for responsible State behaviour in cyberspace.

States have now reaffirmed that existing international law, particularly the Charter of the United Nations, provides a strong, rules-based foundation for all approaches to cybersecurity.

Ireland supports efforts aimed at promoting deeper understanding among States on the application of international law to cyberspace.

We will soon publish our national position, and encourage others to do likewise.

Responsible State behaviour is, of course, also critical.

All Member States have agreed to be guided by the 11 voluntary norms of State behaviour in cyberspace.

We now need to work on promoting understanding and implementing these norms, building on the foundation of international law, to strengthen global cybersecurity. This will reduce the potential for conflict and improve international relations.

Confidence-building measures, including dialogue, build trust and reduce tensions between States. I know that is stating the obvious, but it does need to be said.

We welcome the leading role played by regional organizations in this regard, including the Organization for Security and Cooperation in Europe. Ireland and our European Union partners are committed to supporting capacity-building initiatives.

In a highly interconnected cyberspace, no country is safe until all countries are safe. Surely, the coronavirus disease (COVID-19) pandemic has taught us that.

We also remain committed to tackling the global digital divide. Online access for all will be a key element in the delivery of the Sustainable Development Goals in the next decade.

My third point is that maintaining international peace and security in cyberspace must be human-centric and values-based.

Ireland supports a safe, secure, and accessible cyberspace where human rights and fundamental freedoms apply, both on and offline.

We strongly reaffirm the applicability of international human rights law to States' actions in cyberspace.

The protection of civilians remains an overarching priority in all aspects of our work. In this regard, Ireland is committed to ensuring respect for international humanitarian law in cyberspace.

It is a sad fact that the gendered violence experienced by too many women and girls is now frequently accompanied and magnified by online violence and cyberthreats.

This makes it all the more important that we, as leaders, all leaders, consciously promote the participation of women in United Nations processes, decisions and policies on cyber.

We need to work harder to overcome the gender digital divide.

Ireland has consistently advocated the inclusion of a broader range of expertise in United Nations discussions on cybersecurity and capacity-building.

Governments, together with those who drive and lead on technological innovation, have the responsibility to maintain a safe and free cyberspace.

The contributions of civil society, technical experts, academics and the private sector have enriched past cyberdiscussions at the United Nations. To date, their engagement has been far too limited, in our view, on the cybersecurity issue.

We also support initiatives, including the Paris Call for Trust and Stability in Cyberspace, which bring State and non-State stakeholders together with the shared objective of promoting peace and security.

We must all work together to reach better shared solutions.

To conclude, Ireland will continue to support constructive, multilateral, and multi-stakeholder approaches, built on consensus, to strengthen cyberresilience worldwide.

We call on all States to behave responsibly, in full compliance with international law, and to implement the normative framework.

We value the role of the Security Council in preventing conflict and promoting peace and security, including in cyberspace.

And we urge all States to build on the achievements made at the United Nations in recent months.

In this way we can ensure a more secure and peaceful global cyberspace for everyone to benefit from.

Annex V

Statement by the Minister for Foreign Affairs of Viet Nam, Bui Thanh Son

I thank the President and the Estonian presidency for convening this meeting on a very pertinent topic. I am grateful to Under-Secretary-General Nakamitsu for her insightful remarks.

The explosive development of information and communications technologies (ICT) has significantly transformed the way people live, work and interact with each other. It has facilitated global communication, knowledge sharing and cultural exchange, helped peoples and countries get closer, and also renewed production towards more efficient, sustainable and inclusive patterns.

On the other hand, these advanced technologies, if in wrong hands and used maliciously, can pose grave threats to the sovereignty, security and prosperity of nations. Deployed by terrorists or transnational criminals, they are capable of sabotaging economic systems, damaging social stability, eroding cultural and humane values.

Let us take economic losses caused by cyberattacks for an example. Global annual expenditure on cybersecurity reached $1 trillion in 2020, an increase of 50 per cent compared with 2018 and a three-fold increase since 2013. Most of the expenditure goes to damage repair and recovery.

More worryingly, there have been reports of transnational cyberattacks that undermined global and national security, even potentially triggering cyberwarfare.

As such, cybersecurity is very urgent and critical to peace, security, development and prosperity at both the national and global levels. Against such backdrop, I would like to share the following thoughts.

First, every State has its own sovereignty and interests over cyberspace that need to be fully respected. Each Member State bears the primary responsibility in creating the legal framework to regulate behaviour in cyberspace within its territory and applicable to its citizens. Also, regulating behaviours in compliance with the law, preventing illegal malicious acts and facilitating positive activities are guiding principles to create a safe, stable cyberspace for peace, development and humanity.

Viet Nam is a country with high Internet coverage, with nearly 70 per cent of our population active on the Internet and social networks. Our success lies in the comprehensive legal framework that facilitates ICT development and prevents ICT misuse. Viet Nam also prioritizes on improving self-protection, self-reliance and resilience, combined with effective international cooperation.

Second, the nature of cyberattacks is transnational where global Internet networks become target for constant exploitation by perpetrators. It correspondingly requires global and trans-national solutions to cybersecurity. Viet Nam supports an international framework that sets out rules and norms of responsible behaviour in cyberspace, on the basis of consensus and with the widest participation of countries, including ongoing processes at the United Nations. We are concerned and oppose to the malicious, harmful use of ICT, especially cyberattacks on medical, electricity, water and food facilities so essential to people. Activities in cyberspace have to comply with the principles of the Charter of the United Nations and international law, in particular, respect for sovereignty, non-interference in internal affairs of States, and non-use of force and the peaceful settlement of disputes.

Third, enhancing international cooperation, confidence-building and accountability are indispensable to strengthen cybersecurity. All countries, irrespective of their size and level of development, benefit from a global secured and safe cyberspace. Therefore, they need to participate actively and make more practical and responsible contributions to ensuring safety and security in the global cyberspace for peace, stability and sustainable development of every nations.

The development of ICT is an important launchpad in our common quest for prosperity. Viet Nam has actively implemented a national digital transformation strategy. We aim to have the digital economy to account for 30 per cent gross domestic product by 2030. In South-East Asia, Viet Nam has actively participated in regional cybersecurity mechanisms, including the cybersecurity cooperation strategy of the Association of Southeast Asian Nations. We also hold effective bilateral cooperation with many countries and international partners on this field. Viet Nam stands ready to further contribute to enhancing international cooperation towards a peaceful, stable, secured and safe cyberspace for our shared prosperity and sustainable development.

Annex VI

Statement by the Cabinet Secretary for Information and Communications Technologies, Innovation and Youth Affairs of Kenya, Joe Mucheru

I congratulate the President for convening, for the first time in the Security Council, an independent discussion on cybersecurity. I thank the High Representative for Disarmament Affairs, Ms. Nakamitsu for her informative briefing.

Our increasing dependence on information and communications technology (ICT) comes with both benefits and vulnerabilities.

The efforts of those who develop and use ICT and emerging technologies for peaceful purposes are closely matched by their opposites who use them for control, illicit surveillance, fraud, radicalization and destabilization.

Kenya is committed to the sustenance and protection of a free and open Internet domain. We regard it as a key driver of national development, and we seek our young people to be empowered and competitive in its use.

We are a world leader in digital currency having pioneered M-Pesa – the first widely used mobile money platform. Our Government has also embraced digitized public service platform delivery through our one-stop service facilities, known as Huduma Centres, which are spread across the country.

Young Kenyans are innovating and building transformative companies. This has been recognized by investors globally with our “Silicon Savanna” attracting the most investment in our region. We believe that many of our decent jobs of the future will emerge from these companies.

With such extensive exposure to the digital domain, Kenya regards it a critical national security aim to secure ICT.

To this end, we have a robust regulatory regime. And we also have growing capabilities to respond to threats. Our Computer Emergency Incident and Response Team collaborates with other national computer incident response teams, and internationally through the global Forum of Incident Response and Security Teams.

Our task today is to offer proposals on how the Security Council can better secure international peace and security from threats delivered through, or that exploit, cyberspace.

I will highlight three areas that we believe would benefit from better international cooperation and collaboration.

The first area concerns ICT and emerging economies. Cybercrime is increasingly focusing on emerging economies. Enhanced cooperation in strengthening existing regional and international economic conflict settlement mechanisms is needed including coordinated efforts to identify and mitigate risks associated with ICT-linked activities such as digitized fraud, the impact of crypto currencies on national central banking systems, and cyberattacks on critical infrastructure.

As industrial automation accelerates, the jobs lost must be replaced by other decent ones otherwise peace and security will suffer. More will need to be done to invest in the digital skills that allow countries with underdeveloped industry to attract the investment that offers millions of new jobs.

The second area relates to ICT and violent extremism. The ubiquitous, programmable and data-driven nature of emerging technologies, although beneficial, has also opened a door for misuse by armed groups and terrorists. These groups capitalize on the opaque control mechanisms, algorithms, 3D printing, the application of cryptography and simplified user interface to recruit, plan and carry out terrorist acts. This has enhanced radicalization and militarization.

Kenya calls for enhanced cooperation between the Security Council and the Office of Counter-Terrorism to build a cyberspace security capability that is robust and responsive in responding to Member State capacity-building needs.

United Nations peace operation mandates will also need to consider the use of cyberspace by hostile militarized actors.

My third focus area is ICT and social media. The growing impact of fake news, deep fakes, misinformation and disinformation on peace and security cannot be overstated. Recently, we have seen the impact of fake news blunting the responses to the coronavirus disease (COVID-19) pandemic threat by promoting vaccine hesitancy.

The social media companies are going to need to be held to account and made to ensure that fake news, in particular by sophisticated actors, some supported by States, is not proliferating on their platforms. Such a regulatory effort will need to be built on a multilateral platform to ensure uniformity of effect.

I conclude by affirming Kenya’s readiness to contribute to enhanced global efforts, institutional frameworks and norms that will amplify the potential of a free, peaceful and stable cyberdomain, and at the same time mitigate the threats.

Annex VII

Statement by the Permanent Representative of the United States of America to the United Nations, Linda Thomas-Greenfield

I thank the President and thank Estonia for organizing this important discussion today. We are very grateful to Estonia for bringing this issue to the Council's attention. I also thank High Representative Nakamitsu for her insightful briefing.

This debate comes at an opportune time. Especially with the coronavirus disease (COVID-19) pandemic, we have never relied on technology more, and we're seeing that today. But both State actors and non-State actors alike are taking advantage of this increased reliance. In the United States, separate high-profile ransomware incidents disrupted JBS, a major food processing company, and Colonial Pipeline, a company that provides fuel to much of our East Coast. These incidents demonstrate the serious and the unacceptable risk that cybercrime poses to critical infrastructure. The effects of these malicious activities are often not contained within borders, either. Malicious cyberactivity targeted the software company SolarWinds, for example, and Microsoft's Exchange Server software.

The risk is clear. Our infrastructure – online and off – is at stake. Our most basic and critical services, from the food we eat, to the water we drink, to the health-care services we all relied on during the pandemic, are targets. So, in today's world, when we talk about global security, we have to talk about cybersecurity. Fortunately, despite our ideological differences, Member States have repeatedly come together over the past decade to try to prevent conflict stemming from cybercapabilities. Together, we have articulated a framework of responsible State behaviour in cyberspace through the Group of Governmental Experts process. The framework makes it clear that international law applies to cyberspace. It also outlines voluntary norms and the practical cooperative measures that States should take.

In recent months, the Open-ended Working Group, consisting of all Member States, reached consensus on a new report that explicitly endorses the framework of responsible State behaviour in cyberspace. And just last month, the sixth United Nations Group of Governmental Experts also successfully ended with a robust set of recommendations and new guidance on the framework. That is progress. These reports provide real guidance, from State use of cybercapabilities to approaching the complicated issue of attributing cyberincidents. The framework also considers how States should cooperate to mitigate the effects of significant malicious cyberactivity emanating from a particular State's territory, including those activities undertaken by criminals.

We all share this responsibility. As President Biden recently noted, and I quote, "countries need to take action against criminals who conduct ransomware activities on their territory". So, let me be clear: when a State is notified of harmful activity emanating from its own territory, it must take reasonable steps to address it. Given the transnational nature of cyberspace, this cooperation is essential.

The framework Member States have worked so hard to develop now provide the rules of the road. We have all committed to this framework. Now, it is time to put it into practice. We have substantial work to do to ensure that all States that want to act responsibly in cyberspace have both the policy knowledge and the technical capacity to do so. As we do this work, we also need to continue to protect Internet freedom. The same rights that people have offline – including the rights of freedom of expression, association, and peaceful assembly – must also be protected online.

Member States have demonstrated a remarkable willingness to bridge differences and reach consensus on these issues. Let us continue to show that good faith and provide the world a united front on cybersecurity. Together, we will build an open, secure, and stable cyberspace that benefits everyone.

Annex VIII

Statement by the Foreign Secretary of India, Harsh Vardhan Shringla

I thank the President and welcome Estonia’s initiative in organizing this open debate to highlight one of the significant emerging areas of cybersecurity. I also thank Under-Secretary-General Nakamitzu for her briefing.

While the meaning of peace has remained constant since the establishment of the Security Council, the nature of conflict and its underlying tools have transformed tremendously over the decades. Today, we are witnessing growing security threats to Member States emanating from cyberspace, which can no longer be ignored. Hence, the open debate is timely.

The increasing use of cybertechnologies and of information and communications technologies (ICT) has accelerated economic development, improved services delivery to citizens, generated greater social awareness, and placed information and knowledge in the hands of every individual. Most activities in this cyber-age – political, social, economic, humanitarian and developmental (including this high-level meeting of the Security Council) – are now conducted in or connected to cyberspace. The coronavirus disease (COVID-19) pandemic has only accelerated and expanded the digitalization of these activities.

The dynamic and continuously evolving feature of cyberspace has also brought cybersecurity into the discourse of peace and security. The borderless nature of cyberspace and more importantly anonymity of actors involved have challenged the traditionally accepted concepts of sovereignty, jurisdiction and privacy. These unique attributes of cyberspace present their own set of numerous challenges for Member States. I will focus on three key challenges in my intervention:

First, some States are leveraging their expertise in cyberspace to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism. The world is already witnessing the use of cybertools to compromise State security through, inter alia, attacking critical national infrastructure, including health and energy facilities, even disrupting social harmony through radicalization. Open societies have been particularly vulnerable to cyberattacks and disinformation campaigns.

Second, we are witnessing the sophisticated use of cyberspace by terrorists around the world to broaden their appeal, spread virulent propaganda, incite hatred and violence, recruit youth and raise funds. Terrorists have also used social media for planning and executing their terror attacks and wreaking havoc. As a victim of terrorism, India has always underlined the need for Member States to address and tackle the implications of terrorist exploitation of the cyberdomain more strategically.

Third, the integrity and security of ICT products, which form the building blocks of cyberspace, are being compromised. There are widespread concerns that State and non-State actors are introducing vulnerabilities and harmful hidden functions, including through backdoor channels, into ICT networks and products. Such nefarious acts undermine trust and confidence in the global ICT supply chain, compromise security and could become a flashpoint between States. It is in the interest of the international community to ensure that all actors abide by their international obligations and commitments and not indulge in practices that could have potentially disruptive effects on global supply chains and trade in ICT products.

The interconnectedness of the cyberdomain requires that solutions to the complex problems and threats emanating from cyberspace cannot be resolved in isolation. As Member States, we need to adopt a collaborative rules-based approach in cyberspace and work towards ensuring its openness, stability and security. The momentum generated by the positive outcomes of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and the Open-ended Working Group on the developments in ICT should be leveraged to find further common ground and improve upon the already-agreed cybernorms and rules. These rules must strive to ensure collective cybersecurity through international cooperation. Multi-stakeholder involvement will be key in achieving this objective.

Fostering equitable access to cyberspace and its benefits should also form an important component of this international co-operation. The widening “digital gaps” and “digital knowledge gaps” among countries create an unsustainable environment in the cyberdomain. Growing digital dependency in the post-coronavirus disease (COVID) era has exacerbated risks and exposed these fissures of digital inequalities. These must be bridged through capacity-building. The pervasive and boundary less nature of cyberspace implies that we are only as strong as the weakest link in the global network. “Only together” we can achieve the goal of a globally secure resilient cyberspace and we must ensure that no country is left behind in this collective endeavour.

India is committed to an open, secure, free, accessible and stable cyberspace environment, which will become an engine for innovation, economic growth, sustainable development, ensure free flow of information and respect cultural and linguistic diversity. With our transformative technology initiatives in recent years such as IndiaStack, Aadhar and UPI, we have successfully leveraged the tremendous potential of cybertechnologies in implementing the 2030 Agenda for Sustainable Development and improving governance. As part of its COVID vaccination drive, one of the largest such drives in the world, India has developed Co-WIN – a scalable, inclusive and open technological platform. The Co-WIN platform can be customized and scaled up for health interventions across the globe. We are working on sharing this platform with partner countries.

Our overarching objective is to harness cyberspace for growth and empowerment of the people, not just of our own country, but for all humanity. India stands ready to offer its expertise and share its experience in this endeavour.

Annex IX

Statement by Minister of State with the Responsibility for Foreign Affairs and Foreign Trade of Saint Vincent and the Grenadines, Keisal M. Peters

We would like to express our appreciation to the Estonian presidency for its initiative to hold today's high-level open debate on a topic that is critically important, for taking stock of the Security Council's performance in its task of maintaining international peace and security. Let me also express my appreciation to all of today's briefers for their insightful presentations.

In the contemporary world, cyberspace touches nearly every part of our daily lives. The role of information and communications technology (ICT) in enabling economic and social benefits is clear. Yet, despite these benefits, the world must remain cognizant of the serious ICT problems that exists. The global ICT environment is facing a dramatic increase in the malicious use of ICTs by State and non-State actors. To be sure, the misuse of ICTs poses a risk for all States and has the potential to negatively impact international peace and security. It is therefore imperative that we build on an earlier commitment to generate confidence-building measures that enhance international peace and security and increase cooperation, transparency, predictability, and stability among Member States in this field.

An open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security. Additionally, other actors with different capacities and capabilities from across different sectors at all levels of the global ICT chain, have a key *role* in *ensuring cybersecurity*. We must explore possibilities for further capacity-building and technical assistance resources. The United Nations needs to enhance assistance to Member States and further help ensure coherence of efforts among the range of United Nations entities engaging in cyberspace. These efforts should be tied into the Organization's broader goals.

Despite our many challenges as a small island developing State, Saint Vincent and the Grenadines has taken concrete steps to improve its ability to tackle the scourge of cybercrime. Two laws, the Electronic Evidence Act (2004) and the Electronic Transactions Act (2007), underpin a basic legislative framework for cybersecurity in the country. In August of 2016, lawmakers passed the Cybercrime Bill 2016 into law, thus providing the country with substantive and procedural law to be able to deal with cybercrime more effectively. We are also committed to our regional cybersecurity agreements within the OAS and CARICOM.

Due to the coronavirus disease (COVID-19) pandemic and further disruption due to our recent volcanic eruption, schools within our country have switched to remote education, as is the case all over the world. With thousands of children receiving tablets from the Government to facilitate this transition, there has been increased volumes of Internet use and screen time. Considering this, the Ministry of Education and National Reconciliation has embarked on a #GoCyberSmart campaign to promote cybersafety. The campaign is an awareness-building initiative to empower students to make the right digital decisions. The three focus areas are information security, hardware safety and navigating safely online.

The importance of information exchange among Member States and regional and international organizations are essential for ensuring stability and to prevent escalations of cybersecurity incidents. Moreover, we call on Member States to remain committed to international law and the framework for responsible State behaviour in cyberspace.

In our effort to advance responsible State behaviour in cyberspace in the context of international peace and security, we must be guided by the assessments and recommendations contained in the consensus Group of Governmental Experts (Group of Governmental Experts) reports in 2010, 2013, 2015 and the most recent in 2021, as well as the conclusions and recommendations of the final report of the United Nations Open-ended Working Group.

To conclude, failure to agree on the rules of engagement, policy norms, and international cooperation mechanisms for a peaceful ICT environment would only yield new sources of instability and conflict. In cyberspace, we encourage all actors in the international community to comply with their international legal obligations including the respect of sovereignty and political independence as enshrined in the Charter of the United Nations, and the principles for peaceful dispute settlement in the same manner as in the physical world. The urgent drive to maintain international peace and security in cyberspace must never stop.

Annex X

Statement by the Deputy Minister for Foreign Affairs of Norway, Audun Halvorsen

A globally accessible, free, open, and secure cyberspace is essential to maintain international peace and security. We welcome that Estonia has brought this topic to the attention of the Security Council – the primary United Nations body responsible for the maintenance of international peace and security, in accordance with the United Nations charter.

Information and communication technologies (ICT) are a fundamental part of global infrastructure. They are at the core of the development, stability, and security of all States. Yet cyberspace is also increasingly becoming an arena for competition, and potential conflict between States.

We have witnessed over the last decade how malicious cyberoperations, by both States and non-State actors, have increased in scope, scale, severity, and sophistication. We find ourselves in the midst of a global pandemic, where even critical health infrastructure has been among the targets of such malicious activity – putting at risk the safety of citizens and our global efforts to manage the COVID crisis.

Yet, there is also cause for optimism. This last year has demonstrated the readiness of the international community to rise to the occasion and work together to advance responsible State behaviour in cyberspace. The consensus reports of the Open-ended working Group and of the Governmental Group of Experts (Group of Governmental Experts) demonstrate the commitment of all Member States to uphold the international rules-based order in cyberspace. This is a victory for multilateralism.

The affirmation of the applicability of international law to cyberspace is the cornerstone of both the Group of Governmental Experts and the Open-ended Working Group consensus reports. international law is the basis for States' shared commitment to preventing conflict and maintaining international peace and security. It is key in enhancing confidence among States. Both reports reaffirm that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, and promoting an open, secure, stable, accessible, and peaceful ICT environment.

We consider it a major step forward that the Group of Governmental Experts report has recognized that international humanitarian law applies in all armed conflict, also in a cybercontext.

International humanitarian law aims to minimize the human suffering caused by armed conflict. It regulates and limits cyberoperations during armed conflicts, just as it regulates and limits any other means and methods of warfare. Consequently, attacks against civilians or civilian objects are prohibited, and medical services must be protected and respected. Attacking critical infrastructure, such as power supply, food production, drinking water installations, or other objects indispensable to the survival of the population are therefore prohibited.

Recognizing the applicability of international humanitarian law in cyberspace does not legitimize cyberwarfare. Any use of force by States remains governed by the Charter of the United Nations and the relevant rules of customary international law. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

President,

All Member States have supported a framework for responsible State behaviour in cyberspace. A framework based on: the applicability of international law, adherence to agreed voluntary norms, practical confidence-building measures and capacity-building efforts to bolster the resilience and security of all. This is a major achievement; but its value can only be realized through implementation and compliance by all States.

Today's meeting is a recognition that malicious activities in cyberspace can severely impact international peace and security. Today's meeting is also a clear signal to all States that we are expected to live up to the framework for responsible State behaviour in cyberspace that we have agreed to: That we must comply with our obligations under international law and adhere to the norms to which we have agreed.

Annex XI

Statement by the Minister of State for South Asia and the Commonwealth of the United Kingdom of Great Britain and Northern Ireland, Lord Ahmad of Wimbledon

Today, almost everything has a digital dimension.

The international community needs to grasp the tremendous opportunities that the Internet offers, for learning, for business, for communication and, indeed, for entertainment.

But we also need to treat the threats that go with that, with the seriousness they deserve.

The threats posed by malicious and dangerous activity in cyberspace are now clearer than ever.

Indeed, only last month, a criminal gang targeted Colonial Pipeline, holding to ransom America’s largest fuel pipeline and threatening serious economic disruption.

Some of this activity aims for theft or extortion. Often, it is simply sabotage and disruption.

But we have a collective responsibility, as an international community, to create a cyberspace that benefits all countries and, indeed, all people. Together, we should be shaping the rules that serve the common good.

We are of course not starting from scratch in this regard.

It was ten years ago that the UK brought together more than 60 countries in London, to establish basic principles like universal access to the Internet, and protecting individuals’ rights online.

Ten years later, we have come a long way since then.

Just this year, the General Assembly unanimously reaffirmed the application of international law in cyberspace and agreed a set of voluntary principles, including the importance of protecting health infrastructure.

A Group of Governmental Experts moved forward our understanding of the norms, rules and principles of cyberspace, and set out clear interpretations of how international law applies.

But we want to go further. It is no secret that States are developing cyberoperations to support their military and national security capabilities. Indeed, the United Kingdom is one of them.

Let me be clear: we will use these capabilities to defend ourselves against those who seek to harm us. We are committed to use these capabilities where necessary, in a proportionate way, and in line with international law.

Our collective challenge here is to clarify how the rules of international law apply to State activities in cyberspace, guard against malicious actors bending the rules, and enforce the consequences for those who commit malicious cyberactivity.

The United Kingdom is committed to working with all countries, and with its many stakeholders, to make sure cyberspace is governed by rules and norms that enhance our collective security.

Rules and norms that promote democratic values, rules and norms that support global economic growth, and counter the spread of digital authoritarianism.

We must uphold the rule of law in cyberspace: embodying responsible State behaviour, incentivising compliance, deterring attacks and, indeed, holding others to account for irresponsible State behaviour.

We must also absolutely prioritise and ensure human rights are protected online, as they are offline, to ensure we build a free, open, peaceful and secure cyberspace, accessible to everyone.

The United Nations framework for responsible State behaviour in cyberspace is our starting point. We must support all States to now implement it.

The United Kingdom was pleased to announce last month that we will invest over $30m to support cyberrelated capacity-building in vulnerable countries – in particular across Africa and the Indo-Pacific.

Our work with Interpol will help countries, including Ethiopia, Ghana, Nigeria, Rwanda, and Kenya, support joint operations against cybercriminals.

Elsewhere, UK funding will help build national emergency response teams to protect countries against these threats.

We could of course do none of this without our partners in the private sector, and, of course, in academic and civil society.

But, in all of this, as we join here together today, the Security Council also has a pivotal and an important role to play.

Where malicious activity poses risks to international peace and security – by exacerbating conflict or causing humanitarian suffering – the Security Council must be ready to respond.

The Council should respond just as it would to threats posed by conventional means.

We have the chance to grasp the opportunities of cyberspace and ensure it remains a force for prosperity and progress for all.

To do that, it is vital that we work together to counter those who would risk our collective security.

And let me assure you of this: the United Kingdom is fully committed to protecting a free, open, peaceful and secure cyberspace for generations to come.

Annex XII

Statement by the Minister-Delegate to the Minister for Europe and Foreign Affairs of France, Franck Riester

[Original: French]

I wish to thank the Prime Minister of Estonia for this event. The Security Council oversees the maintenance of international peace and security and should be able to do so in cyberspace.

Cyberspace is a place of opportunity but also of new threats. It has become a territory for strategic competition among powers. Malicious uses of information and communications technologies (ICT) are proliferating, by State and non-State actors alike.

Over the past several months, in particular in the context of the coronavirus disease (COVID-19) pandemic, we have noted our increased dependence on these technologies. I have in mind first of all of the heinous cyberattacks using ransomware launched against hospitals and other critical infrastructure. I would like to express the full solidarity of France with the victims of those attacks. I am also thinking of the campaigns to manipulate information through the spread of "infodemics" or the increasing fragmentation of the Internet, practices contrary to democratic values. Actions in cyberspace have very real consequences that can prove to be severe in our lives and societies.

The challenge for the coming century will be to build collective governance and regulation of cyberspace. We want neither a "digital Wild West", nor a cloistered cyberspace. We have affirmed this in the Paris Call for Trust and Security in Cyberspace, as well as in the framework of the Group of Seven (G7) in the Dinard Declaration on the Cyber Norm Initiative. France is determined to build with its partners a cyberspace that is open, secure, stable, not fragmented, accessible and peaceful.

International law, including the Charter of the United Nations, applies in full to cyberspace. This also implies respect for international humanitarian law by cyber operations conducted during armed conflict.

Faced with the increasing number of threats in cyberspace and cyberattacks, Governments should respond by cooperation and law. For over a decade, France has played a pioneering role in various multilateral efforts. These efforts have led to the emergence of a framework for responsible behaviour by States in their use of ICT. This framework is based on international law, on a coherent set of non-binding norms of behaviour and on measures for transparency and trust. It has allowed progress to be made in mutual cooperation and understanding among States in cyberspace. I would like to commend the recent success of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the sixth Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, which have adopted two balanced and useful consensus reports. France is ready to continue to participate constructively in multilateral discussions within the United Nations, including in the context of the new Open-ended Working Group on security of and in the use of information and communications technologies, established by General Assembly resolution 75/240.

Going forward, agreed norms and principles must above all be put into practice effectively. France, with 52 partners, proposes the establishment of a Programme of Action on cybersecurity by the United Nations. This new tool, which complements the new Open-ended Working Group, will allow a durable structure to be established. Its purpose will be to support capacity building and creating spaces for dialogue with civil society, researchers and private actors. France is open to dialogue with all States and stakeholders interested in refining and building on this action-oriented proposal.

This collective commitment by multiple actors is essential. In cyberspace, States certainly have responsibilities that no other actor can presume to take on, but they cannot act alone. We must enter fully into this new form of diplomacy.

Annex XIII

Statement by the Permanent Representative of China, Zhang Jun

[Original: Chinese]

In today's world, a new round of technological revolution and industrial transformation is just unfolding and digital and cyber technologies are developing rapidly, greatly changing humanity's modes of production and ways of life and spurring the economic and social development of all countries. At the same time, cyber surveillance, cyberattacks, cybercrimes and cyberterrorism have become global public hazards, and cyberspace is becoming increasingly militarized, politicized, insecure and ideologized. In the cyber world, countries not only enjoy shared opportunities and common interests, but also face common challenges and assume shared responsibilities. They are increasingly becoming a community with a shared future through weal and woe.

Chinese President Xi Jinping has stated that although countries are different in national conditions and stages of Internet development, and face different challenges on the ground, they share the same desire to advance the digital economy, the same interest in tackling cybersecurity challenges, and the same need to strengthen the governance of cyberspace. China has always called for the international community to work together in a joint effort to protect cybersecurity and maintain international peace.

- We should promote security by maintaining peace and preventing cyberspace from becoming a new battlefield. The international community should abide by the purposes and principles of the Charter of the United Nations, in particular the principles of sovereign equality, prohibition of the use of force, non-interference in internal affairs, and peaceful settlement of disputes. It is essential to respect the right of each country to independently choose the path of its network development and the model of its network management, and to participate in the governance of cyberspace on an equal footing. Countries should refrain from undertaking cyber activities that endanger the security of other countries. Caution should be exercised in applying the law of armed conflict to cyberspace, and arms races in cyberspace should be prevented.

- We should promote security through exchanges and cooperation and create a favourable cyberspace environment. Protecting cybersecurity is a global issue, and no country can stay aloof from it or deal with it single-handedly. Hegemonism, unilateralism and protectionism in cyberspace will only intensify confrontations and poison the atmosphere for cooperation, and should be rejected and opposed jointly by the international community. Countries should work together to deepen exchanges and cooperation in technology research and development, rule-making and information sharing, and should jointly curb the abuse of information technology. We should jointly oppose cyber surveillance and cyberattacks, combat cyberterrorism and cybercrimes, and enhance cybersecurity protection capabilities. It is essential to provide companies with an open, fair, and non-discriminatory business environment, ensure the openness, stability and security of global information-technology industry supply chains, promote the healthy development of the global economy, and oppose human interference with companies' normal business operations, whatever the pretext.

- We should promote security through improved governance and advance fairness and justice in cyberspace. All countries should uphold effective multilateralism, establish an open, inclusive and sustainable cybersecurity governance process within the United Nations framework and with the equal participation of all, formulate international rules for cyberspace that are generally accepted by all countries, and oppose cliques and group politics. China highly commends the successful completion of the reports on cybersecurity by the United Nations Open-ended Working Group and the Group of Governmental Experts, and looks forward to the new Open-ended Working Group's contributions to maintaining cybersecurity. We stand ready to work with all parties in promoting, within the United Nations framework, the development of an international convention against cybercrime. Full play should be given to the roles of such multi-stakeholders as Governments, internet companies, technology communities, civil society, and individual citizens, in the spirit of extensive consultation, joint contribution and shared benefits.

- We should promote security through inclusive development and achieve shared prosperity in cyberspace. Current world economic development is sluggish. Digital and cyber technology can become important engines for countries to recover and resume economic and social development after the pandemic. Countries should adopt more proactive, comprehensive, coordinated and inclusive policies to promote the balanced development of information and communications technologies on the global scale, vigorously develop new models and new formats such as the digital economy, and oppose attempts to seek scientific and technological hegemony. We should advance the development of digital infrastructure and connectivity, break down information barriers, bridge digital divides, and help developing countries raise their levels of digitization, connectivity and knowledge development, with a view to implementing the 2030 Agenda for Sustainable Development. We should step up cooperation with and assistance to developing countries in the cybersecurity field, and improve their early-warning, prevention and emergency-response capabilities for cybersecurity incidents.

China attaches great importance to cybersecurity and informatization and is committed to building a digital economy, digital society and digital government, using the overall digital transformation to drive changes in modes of production, lifestyles and models of governance. China will continue to improve its national cybersecurity laws, regulations and institutional standards on the basis of the Cybersecurity Law and the Data Security Law.

Last year, China put forward the Global Initiative on Data Security, focusing on such issues as critical infrastructure and the protection of personal information, data storage and retrieval for overseas enterprises, and supply chain security, providing constructive solutions for maintaining global data and cybersecurity. Recently, China, with the League of Arab States (LAS), issued the China–LAS Cooperation Initiative on Data Security, which embodied the two parties' joint appeal for the maintenance of cyber and data security. We welcome all parties' active responses to and participation in the initiative, so as to jointly formulate global rules for digital governance. China is also actively pursuing the construction of the Digital Silk Road, working with other countries to build a new, future-oriented pattern of intelligent interconnection.

Cyberspace embodies the dream of humanity, involving people's well-being, peace and security. China stands ready to work with all countries to seize the opportunity presented by the information revolution to foster a new momentum of innovation and development, open up a new landscape of digital cooperation, forge a new pattern of cybersecurity, build a community with a shared future in cyberspace, and jointly create a better future for humanity.

Annex XIV

Statement by the Permanent Mission of Mexico to the United Nations

[Original: Spanish]

Mexico welcomes the convening of this open debate and the briefing by the Undersecretary-General and High Representative for Disarmament Affairs, Izumi Nakamitsu.

As we have heard here as well as in many other forums, the growing importance of cyberspace is undeniable. The world has become increasingly dependent on information and telecommunications technologies, all the more so in the context of the pandemic. International relations have also quickly entered the virtual realm, and the Security Council cannot and should not be unaware of its implications for international peace and security.

Although almost half the global population does not have internet access, that does not exempt them from becoming victims of some of the thousands of cyberattacks that occur daily against government networks, banking and financial institutions and research and health institutions.

These potential risks have led various bodies of the United Nations system to respond to threats and seek agreements among States to ensure that cyberspace is not used for criminal, hostile and even terrorist purposes, without losing sight of the balance with its peaceful uses and the enormous opportunities it offers for sustainable development.

Mexico considers it essential to prevent any escalation of risk in cyberspace. The use of cyberspace, like any other physical environment, should be regulated according to very clear guidelines and parameters, while it is necessary to help to promote an open, free, secure, stable, accessible and resilient cyberspace.

Mexico therefore applauds the successful conclusion of the work of the Group of Governmental Experts and the Open-ended Working Group that led to the adoption of substantive reports by consensus, which represent fundamental precedents for multilateral efforts. In the view of my country, this fact reaffirms the prevailing confidence in multilateralism, and the constructive role the United Nations can play in achieving integrated, legitimate and long-term responses to the challenges of cyberspace and information and communications technologies.

That is not enough, however. Progress must be made towards the full application of international law in cyberspace, including the Charter of the United Nations, international human rights law, international humanitarian law and the development of jurisprudence in those areas.

We firmly believe in greater transparency in cyberspace activities, accountability, and a call for the development of norms for responsible State behaviour adopted by the General Assembly itself, and supplemented by measures to promote international cooperation to build and strengthen the cyber capacity of States.

Mexico hopes that, in the future deliberations and work of the Security Council, the growing voices of civil society, academia and the private sector will be heard. They rightfully hold a common objective: to ensure the peaceful use of cyberspace for the development and use of digital technologies.

Annex XV

Statement by the Permanent Representative of the Russian Federation to the United Nations, V. A. Nebenzia

[Original: Russian]

The year following the outbreak of the coronavirus disease (COVID-19) pandemic was a major ordeal for the whole world, remembered above all as a year of challenges and losses. Many diplomatic efforts have suffered, and negotiations have stalled on many fronts.

The multilateral discussions on international information security at the United Nations stand out in this regard, as they not only maintained momentum, but also brought about, dare I say, historic results. Both of the designated United Nations General Assembly expert forums – the Group of Governmental Experts and the Open-ended Working Group – were able to adopt their final reports by consensus.

The negotiations in these groups were not easy, which made the hard-won outcomes all the more precious. These outcomes clearly showed that the international community is able to agree on key issues when dialogue is pragmatic, depoliticized and constructive. Thanks to these efforts, we are now entering an important new phase, which began in June 2021 with the organizational session of the new Open-ended Working Group for 2021–2025.

This outcome is a shared achievement of the international community. For our part, we have been striving for decades to contribute to the establishment of a global system for ensuring international information security. In 1998, Russia raised, for the first time at the United Nations, the need to address threats to international information security and proposed a General Assembly resolution to that effect. In the early 2000s, we proposed the establishment of the Group of Governmental Experts to serve as an expert forum for the discussion of international information security. In 2019, when it became clear that this topic had outgrown the narrow focus of the Group, we, together with like-minded delegations, responded to the needs of the international community by launching the open and democratic negotiation process on international information security with the participation of all Member States in the format of the Open-ended Working Group.

This was a very important milestone. For the first time, discussions relating to digital security were open to the majority of States Members of the United Nations. Our rationale is very straightforward: we believe in equitable and mutually respectful dialogue. If we are all equal in the face of threats to international information security, such threats should be discussed not by a narrow circle of technologically advanced States, but by all States Members of the United Nations. States that consider themselves to be more “advanced” should not impose their will.

Our proposals for the establishment of the Group of Governmental Experts and, later, the Open-ended Working Group were not to everyone’s liking at first. Several States, including States participating in today’s meeting, voted against their establishment. However, gradually they began to join the conversation, eventually becoming active and constructive participants.

Effective multilateral diplomacy in the area of international information security at the United Nations, complementing bilateral cooperation between States on this topic, is an excellent example of how these issues should be addressed with a view to overcoming mutual mistrust and allaying concerns. This stands in contrast to the notorious “megaphone diplomacy” to which, unfortunately, some of our partners sometimes resort.

At the same time, we are unfortunately witnessing a dangerous trend of the United Nations Security Council attempting to impose unilateral interpretations of agreements reached within the Group of Governmental Experts and the Open-ended Working Group, effectively calling for the outcomes of the discussions in those designated General Assembly forums to be supported or, worse, revised. We consider such attempts to be destructive. They are driving the international community towards unpredictable and undesirable confrontations.

Specifically, some countries are seeking, by distorting agreements, including on the international legal aspects of the use of information and communications technology (ICT), to justify unilateral pressure and sanctions against other Member States and the possible use of force against them. It is of grave concern that several technologically advanced States are actively pursuing the militarization of the information space by promoting the concept of "preventive military cyberstrikes", including against critical infrastructure. These confrontational doctrines contradict the commitment declared by them, including today, to preventing conflict arising from the use of ICT. This as an attempt to use their position of strength to impose their own "rules of play" in the information sphere.

I wish to emphasize that, while the digital sphere is not unregulated, the debate as to how exactly international law can be applied to it is far from over. These issues will be discussed for at least another five years within the designated General Assembly forum – the new Open-ended Working Group.

In this regard, the final reports of the Group of Governmental Experts and the Open-ended Working Group represent a fine-tuned, balanced set of agreements, including on the need to develop new norms for the responsible conduct of States in the information space, taking into account its particularities. The initial list of such rules was enshrined in the resolution concerning international information security adopted by the General Assembly in 2018 at the initiative of the Russian Federation. It is unfortunate that our Western colleagues are now attempting to pick out from this list the provisions that are of the greatest benefit to them, while incorrectly interpreting the applicability of international law in the digital sphere as being "automatic", which would permit the use of force therein, and to present their national views as though they were the product of global consensus. We will therefore oppose any attempts to revise, through the United Nations Security Council, the balanced agreements reached within the designated General Assembly forums.

As stated by the President of the Russian Federation, V. V. Putin, at the meeting of the Security Council of the Russian Federation on 26 March 2021, Russian doctrinal approaches to the development of a global system for ensuring international information security remain open, transparent and unchanged. They are enshrined in the Basic Principles of State Policy on International Information Security, approved by the President in April 2021. This is a public document, and I encourage everyone to read it.

Our doctrine is based on the premise of using ICT only for peaceful purposes, the need to prevent conflicts in the information space and the importance of strengthening multilateral and bilateral cooperation to that end. We believe that universal international legal agreements should be concluded in order to address those tasks effectively. To achieve this goal, joint efforts must be made to develop and agree upon universal, fair and comprehensive rules for the conduct of States in the information space that take into account current realities; to clearly differentiate between permissible and impermissible activities in the information space; and to make these rules legally binding to ensure that all States strictly observe them.

At the same time, we uphold the inviolability of the sovereignty of States in the digital sphere. It is up to each country to determine the parameters for regulating its own information space and related infrastructure.

An equally important task is to build a peaceful, equitable and fair system for ensuring international information security that takes into account the interests of all countries, regardless of their digital potential. United Nations-led efforts to build such capacity with the aim of bridging the digital divide should be strongly supported. We trust that the new Open-ended Working Group, in accordance with its mandate, will be able to continue to examine this issue in detail and make relevant recommendations.

In addition, we must collectively counter the use of ICT for criminal purposes. We call upon Member States to contribute constructively to the work of the designated special committee tasked with elaborating a draft convention on the issue by 2023.

The General Assembly remains the key forum for discussing international information security. It is in this forum that expert discussions on all aspects of this topic will take place over the next five years. Let us focus on supporting this unique process. We must maintain the constructive atmosphere of multilateral cooperation in international information security under the auspices of the United Nations in the format of the Open-ended Working Group, which has really proved its effectiveness and relevance. This will give the new Open-ended Working Group a real chance of achieving tangible, practical results. It is our common duty as members of the United Nations Security Council to contribute fully to this effort.

Annex XVI

Statement by the Permanent Representative of Tunisia to the United Nations, Tarek Ladeb

At the outset, I would like to express our appreciation to the Estonian presidency for organizing this meeting on cybersecurity and the maintenance of international peace and security in cyberspace.

I thank Ms. Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs, for her informative briefing.

Tunisia is deeply concerned by the significant increase in recent years of malicious activities in cyberspace that can pose a serious threat to international peace and security, especially when critical infrastructures are targeted.

Many States have also been openly developing cybercapabilities for military purposes, a trend that can unleash a cyberarms race and further increase the number of cyberattacks and counter attacks as well as the risks of miscalculations that could lead to armed conflict.

Tunisia is equally worried by the fact that cybercapabilities, which were previously available only to States, have become accessible to and are being used maliciously by non-State actors, including terrorist organizations. These capabilities have reportedly often been acquired through leakage or theft from government entities, which further raises the question of States’ responsibility.

The possibility of terrorist groups launching devastating cyberattacks against critical infrastructures such as nuclear power plants can no longer be excluded and should be seriously addressed.

Tunisia reaffirms the applicability of international law in addressing States’ use of information and communications technologies, and stresses in this regard the importance of respecting the principle enshrined in the Charter of the United Nations including the settlement of international disputes by peaceful means, the refraining from threat or use of force and the respect of human rights and fundamental freedoms.

We would also like to underscore again the applicability of international humanitarian law to cyberoperations conducted during armed conflicts.

My delegation welcomes the consensual adoption earlier this year of the reports of the Open Ended Working Group on developments in the field of information and telecommunications in the context of international security and of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security which both contributed to deepening the understanding of members States on how international law applies and offered additional guidance on how voluntary, non-binding norms can also play an important role in preventing conflicts and promoting an open, secure, stable, accessible and peaceful cyberspace.

We look forward to the continuation of an open and inclusive dialogue on cybersecurity during the sessions of the new Open Ended Working Group (on security of and in the use of information and communications technologies 2021–2025) to reinforce the ability of all State and to prevent or mitigate the impacts of malicious cyberactivities, cyberthreats and cyberattacks.

For its part, and under the supervision of its National Security Council and with the participation of the private sector and civil society, Tunisia has adopted in October 2019 a national cybersecurity strategy which aims at improving Tunisia’s resilience to cyberthreats by developing its national capacities and legal system, in full respect of fundamental rights and freedoms, and through the reinforcement of international cooperation.

Finally, given the interlinked nature of cyberspace, we believe that the sharing of information on known vulnerabilities and capacity-building for those who request it are of crucial importance to reduce the risks to international peace and security posed by cyberthreats.

Annex XVII

Statement by the Permanent Mission of Argentina to the United Nations

[Original: Spanish]

Argentina wishes to thank Estonia for the initiative to hold an open debate to add to greater understanding of the growing risks coming from malicious acts in cyberspace and their impact on international peace and security. The Security Council, by its mandate and nature, is able to address the topic and give it due relevance and significance.

The regular and growing number of reports of serious cyber incidents in various parts of the world calls the attention of all to the need to continue to build greater understanding of how to manage such incidents, some of which might put at risk international peace and security, and the need to create cooperation frameworks and promote national capacity-building to face the challenges affecting the international community as a whole. Actions are therefore required at the national, regional and international level.

At the international level, with the objective of addressing one of the most critical aspects of the question, Argentina considers that it is of the highest importance to maintain broad and inclusive spaces where countries from all regions and with a diversity of views can become actively involved in building consensus on the rules, norms and principles of responsible State behaviour and how international law is applied in cyberspace, among other things. Argentina understands that there is a significant body of voluntary norms, rules and principles that have been accepted by consensus by all the members of the United Nations General Assembly to guide the use of information and communications technology by States and responsible State behaviour in cyberspace, which are essential in maintaining the peaceful use of and stability in cyberspace. This is a starting point and a foundation that should be preserved and developed.

We especially value the consensus obtained by the first Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, which is based on these characteristics of openness. We also give special recognition to the report of the latest Group of Governmental Experts on the promotion of responsible State behaviour in cyberspace in the context of international security. It should be noted that both groups issued consensus reports this year, with important recommendations and contributions to continue to build on consensus already obtained in the past.

The continuation of an open and inclusive forum for discussion with broader horizons is essential in order to continue consolidating the agreements reached and obtaining new ones. We therefore welcome the establishment of a new Open-ended Working Group on security of and in the use of information and communications technologies, whose mandate will extend until 2025, in which our country will continue to participate actively and constructively.

On that subject, and towards a more effective approach, Argentina, along with a number of other countries from all regions, supports the international initiative for a Programme of Action on the development of information and communications technology in the context of international security. That Programme of Action, which is undergoing full conceptual development, proposes an open, inclusive, flexible and continuous framework for discussion under United Nations auspices, conducted by the States and with appropriate participation by the multiple actors involved in cyberspace. We invite all countries to take an interest in this initiative.

Argentina believes that the foundation and principle of our understandings should be the protection and guarantee of human rights and fundamental freedoms enshrined in the Charter of the United Nations and international treaties. The question of gender and special guarantees for vulnerable groups must be a cross-cutting element in all actions we undertake.

In the context of continuing innovation in the field, we must work actively to ensure that the benefits of those technologies can be enjoyed equitably by all nations. We therefore believe that reducing the digital gap among and within States should be an ongoing concern in the debate.

That concern goes hand in hand with the development of national capacity. There is enormous scope for action in this area and it is one of the principles for developing synergies with other actors that participate in cyberspace, such as the private sector, civil society, academia and the technical sector.

Regional and subregional organizations have proven to be important and decisive actors as catalysts of development of national capacity, promotion of common understandings and facilitation of international cooperation.

Without doubt, States must make major efforts at the national level to develop effective capacities, norms and structures to give the matter the importance and priority that it deserves.

We trust that this event will allow us to identify new avenues of understanding that will help us achieve cyberspace that is free, open, secure, interoperable and stable.

Annex XVIII

Statement by the Permanent Representative of Australia to the United Nations, Mitchell Fifield

Australia thanks Estonia for the opportunity to provide a statement to the Security Council addressing international peace and security in cyberspace. As the strategic significance of cyberspace increases, more groups will try to exert power through it. Cyber issues have become strategic foreign policy issues of urgent concern to all countries – and it is vital that they are treated as such by the international community.

While the frequency, scale, sophistication and severity of malicious cyberincidents is increasing, the United Nations has a strong history of fostering international cooperation to understand these threats and promote an open, free, secure, interoperable and peaceful cyberspace.

All members of the United Nations have agreed, by consensus, that existing international law – in particular, the Charter of the United Nations in its entirety – is applicable in cyberspace and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment.[3]

Australia has articulated its views on how particular principles of international law apply to State conduct in cyberspace (2017; 2019; 2021) and published hypothetical legal case studies (2020).[4]

International humanitarian law (including the principles of humanity, necessity, proportionality and distinction) applies to cyberactivities within an armed conflict. International humanitarian law provides rules that apply to cyberactivities in an armed conflict that do not constitute or rise to the level of an "attack", including the general protections afforded to the civilian population and individual civilians against dangers arising from military operations.

International human rights law also applies to State conduct in cyberspace. Under international human rights law, States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realized through or in cyberspace.

Recognizing the unique attributes of cyberspace, in 2015 all Member States agreed to be guided in their use of ICT by 11 voluntary and non-binding norms of responsible State behaviour in cyberspace.[5] These norms complement, but do not replace, States' existing legal obligations. Combined, international law and norms establish clear expectations of responsible behaviour by States, and thereby promote predictability, stability and security.

All States have also recognized the need for confidence-building measures and coordinated capacity-building.[6] CMBs, designed to prevent misunderstandings that lead to conflict, are more important now than ever before, and targeted capacity-building is needed to ensure that all countries are able to respond to the challenges and embrace the opportunities of increased connectivity.

Combined, these measures (international law, norms, confidence-building measures and capacity-building) provide the basis for a secure, stable and prosperous

[3] See General Assembly resolutions 68/243 and 70/237 and decision A/DEC/75/564.

[4] See www.internationalcybertech.gov.au/international-security-at-the-un.

[5] A/RES/70/237.

[6] Ibid.

cyberspace, and are often referred to as the United Nations Framework for Responsible State Behaviour in Cyberspace (the Framework). Each element of the Framework is mutually reinforcing and no one element should be considered in isolation.

Universal endorsement of the Framework[7] by all Member States represents significant progress towards promoting international peace and stability in cyberspace. If adhered to, the Framework provides a robust basis to address the threats posed by State-generated and State-sponsored malicious cyberactivity.

Australia reaffirms its commitment to act in accordance with the Framework for Responsible State Behaviour in Cyberspace, as elaborated in the cumulative reports of the Groups of Governmental Experts in 2010, 2013, 2015 and 2021[8] and the 2021 report of the Open-ended Working Group,[9] and calls on all countries to do the same.

However, a small number of State and State-sponsored actors increasingly flout international law and norms, despite the clear expectations set by the international community. In doing so, they threaten international peace and stability.

What we need is not more – or new – rules, but adherence to the rules we have already agreed, and greater accountability when they are broken. To deter malicious activity, there must be effective consequences for those who act contrary to existing international law and agreed norms of responsible State behaviour.

Australia is committed to countering, deterring and discouraging malicious cyberactivity, especially by States and their proxies. Australia will work with partners to strengthen coordinated responses to unacceptable behaviour in cyberspace. Deterring malicious activity protects international stability. The objective of Australia’s cyberdeterrence policy is to prevent significant cyberincidents that damage the interests of Australia and our international partners.

Effective cooperation between States and the multi-stakeholder community (including civil society, the private sector, academia and the technical community) practically impacts security, lifts capacity, and creates a reinforcing cycle of development, openness and stability in cyberspace. Often the first affected by cyberincidents, protectors of critical infrastructure, benefactor and beneficiary of technical expertise, the evolving equities of non-government stakeholders in cyberspace provide complimentary interests in maintaining a peaceful online environment.

Gender inequality undermines global peace, stability and security in cyberspace. It contributes to, and often exacerbates, a range of challenges, including poverty, weak governance, conflict and violent extremism. The value of gender equality and women’s participation in decision-making, leadership and peace-building associated with international peace and security in cyberspace is indisputable. Australia will continue to take tangible steps to support the active and effective participation of women in all forums discussing international peace and security in cyberspace.

The potential damage or disruption caused by malicious cyberactivities is significant and growing. The increasing attention and awareness of the international community on these issues should not be squandered. This opportunity should be seized – to deepen understandings of how international law applies in cyberspace, promote practical implementation of the norms of responsible State behaviour and confidence-building measures, coordinate capacity-building to so all countries understand and can implement the Framework, and ensure a diversity of voices are heard.

[7] A/DEC/75/564; A/75/816.

[8] A/65/201; A/68/98; A/70/174.

[9] A/75/816.

Annex XIX

Statement by the Permanent Mission of Austria

Austria wishes to thank Estonia in its capacity as presidency of the Security Council for the month of June 2021 for convening this open debate on International Peace and Security in Cyberspace. Austria aligns herself with the Statement by the European Union. In our national capacity, we wish to add the following remarks:

Today marks the first time that the Security Council addresses cybersecurity as a separate issue – this is a welcome development. In order to stay relevant and to discharge of its mandate, it is essential that the Security Council continues to respond to contemporary threats to international peace and security.

A growing number of malicious cyberactivities have increased the threats in cyberspace over the past years. In today's connected world, when infrastructure depends increasingly on digital control systems, the effects of cyberattacks can have similar or sometimes worse effects than conventional attacks. These developments, coupled with challenges in attributing cyberattacks, increase insecurity, the risk of miscalculations and the potential for human error when deciding how to respond to an incoming attack.

While cyberspace differs from the physical world in its functioning, there cannot be any mistake about one simple fact: international law in its entirety fully applies also in cyberspace. This has been reaffirmed, most recently by the outcomes of the Open-ended Working Group on information and communications technology (ICT) as well as the Group of Governmental Experts on Cybersecurity which both agreed by consensus on substantial outcome documents furthering our understanding on the challenges we face in cyberspace. As more and more States develop not only defensive, but also offensive cybercapabilities, it is key that all States in their use of ICT adhere to existing international law as well as to the norms on responsible behaviour in cyberspace. We hope that these documents remind States of their obligations and will, therefore, contribute to more stability in cyberspace.

It goes without saying that the fundamental provisions of the Charter of the United Nations should guide all States in their conduct in cyberspace. In particular, States are obliged to adhere to the prohibition of the use of force as the core pillar of the international security regime. Additionally, past Groups of Governmental Experts have agreed on norms for responsible State behaviour in cyberspace that have been endorsed by all Member States. It is thus clear that it is not a lack of rules and norms but a lack of their implementation that contributes to instability and insecurity. We thus call on all States to fully comply with international law and to follow the norms for responsible State behaviour in their entirety.

In the event that an armed conflict or elements thereof are fought in cyberspace, it is imperative that international humanitarian law is respected and complied with – the principles of humanity, necessity, proportion, distinction fully apply in cyberspace.

In the context of the COVID-pandemic, we note with concern the recent increase in cyberattacks on medical and health facilities which blatantly violate the norms that critical infrastructure, including medical infrastructure, should be off-limits for malicious cyberactivities at all times.

In order to avoid conflict scenarios, confidence-building is key – States should constructively engage in sharing their understanding of cyberspace and the ways in which they engage militarily in order to avoid miscalculations. In this regard, the role of regional organizations cannot be underestimated – many have conducted confidence-building activities. We particularly welcome the 'engagement of the

Organization for Security and Cooperation in Europe on this matter, and we trust that building on their experience of a network of points of contact for cybersecurity affairs, we can also roll out a global network at United Nations level.

While States, international and regional organizations have been at the forefront of developing international law and norms of responsible State behaviour, they cannot tackle the challenges before us by themselves. Commercial actors have a significant role and responsibility in cyberspace, and civil society and academia help us in bringing different perspectives into our discussions. This is why future discussions on cyberspace should be guided by a holistic, multi-stakeholder approach to ensure that those who have a role in maintaining a free, secure, open and stable cyberspace are heard and contribute to the common goals that we seek.

Despite all the progress made in the area of cybersecurity, many open questions still loom – it will be up to the international community to find common answers to these questions. Cooperation will remain key and Austria will stand ready to contribute constructively in relevant processes. In that vein, we hope that future open debates in The Council will revert to the previous practice of allowing non-members to hold oral Statements in order to give visibility to all interested States.

Annex XX

Statement by the Permanent Representative of Bahrain to the United Nations, Jamal Fares Alrowaiei

[Original: Arabic]

Technological and digital transformation and the emergence of modern technologies are helping to achieve progress, prosperity and development for all humanity. Their importance has been amplified by reliance on remote work, education and service delivery across all sectors during the coronavirus disease (COVID-19) pandemic. Notwithstanding the many benefits of technological development, it also carries numerous risks. That is especially the case in the absence of an articulated system for protecting information security and cyberspace, as we are seeing with various cyberattacks that target States' basic infrastructures and threaten vital sectors, institutions or individuals.

The United Nations has devoted great attention to this issue. The Security Council has addressed it indirectly at several meetings on the maintenance of international peace and security, as well as in Arria formula meetings. The General Assembly also has established a number of mechanisms, including the open-ended working group on security of and in the use of information and communications technologies (ICT) (2021–2025). That Group was established in 2020 to consider threats posed by the use of ICT in the context of international security, the formulation of a cyberspace code of conduct for States, the application of international law to the use of ICT, confidence-building measures and capacity-building.

In keep with its belief in the importance of protecting cyberspace from attacks and ensuring the interests of States and peoples, Bahrain has supported the establishment of such mechanisms. It took part in the work of the open-ended working group on developments in the field of ICT in the context of international security, which completed its work in 2021. Bahrain looks forward to active participation in the newly established working group.

As part of the great attention it devotes to cybersecurity in the light of the digital transformation and quantum leap in ICT, Bahrain has worked to build a clear and comprehensive governance system to protect cyberspace through the National Cybersecurity Centre of the Ministry of Interior, which deals with cybersecurity in various sectors in the Kingdom, and also through the Information and e-Government Authority, which protects information security in the Government data network of the Kingdom of Bahrain. The Telecommunications Regulatory Authority tries to strengthen public-private sector cooperation to ensure readiness to face cybersecurity threats.

Bahrain has also taken care to develop legislation and legal frameworks for information security to protect individuals and institutions. Such legislation includes Act No. 30 (2018) concerning the protection of personal data and Act No. 16 (2014) concerning the protection of information and State documents and Act No. 60 (2014) concerning information technology crimes.

At the regional level, Bahrain is actively involved in the work of the Standing Committee on Cybersecurity of the Cooperation Council for the Arab States of the Gulf (GCC). It proposed the creation of an electronic platform for the exchange of information and data on cybersecurity among member States. Each member State has appointed a liaison officer to exchange cybersecurity information, including information on threats and best practices.

The Kingdom of Bahrain ratified the Arab Convention on Combating Information Technology Offences in 2017.

In conclusion, the Kingdom of Bahrain affirms its support for international cybersecurity cooperation, with a view to meeting the aspirations of the world's peoples and achieving progress, prosperity and growth in implementation of the 2030 Sustainable Development Goals.

Annex XXI

Statement by the Permanent Representative of Belgium to the United Nations, Philippe Kridelka

Let me first express my gratitude to the Estonian presidency for hosting this first open debate of the Security Council on peace and security in cyberspace. This timely debate demonstrates the urgency of addressing this topic and the relevance of the Security Council for doing so. Risks stemming from malicious activities in cyberspace are indeed growing and their impact on international peace and security is more detrimental than ever. It is therefore paramount to reaffirm Member States' commitment to international law and to the framework of responsible State behaviour as key elements of conflict prevention and maintenance of peace and security in cyberspace.

Achieving this objective requires both a shared international understanding on the governance of cyberspace *and* real actions to implement this vision on the ground.

The international debate on the governance of cyberspace is in a crucial phase. Belgium strongly supports the ongoing debates within the United Nations framework, among which the First Committee, the various OEWGs and GEEs. The following elements are key:

First, Belgium advocates a shared vision of a global, free, open, stable, peaceful and secure cyberspace, where human rights and fundamental freedoms and the rule of law apply. This shared understanding is built upon an inclusive approach in which all stakeholders – including civil society, the private sector and the academic world – are heard.

Second, the international community must continue to strive for a truly universal cybersecurity framework for responsible State behaviour. This has to be based on the full application of existing international law – including the Charter of the United Nations in its entirety – international humanitarian law, and international human rights law. Last year, Belgium, as a non-permanent Member of the Security Council, took part in an Arria-formula meeting of the Security Council, on cyberattacks on critical infrastructure. Cyberattacks targeting critical infrastructures are putting human lives at risk and have to be condemned by the international community. Cyberattacks against medical facilities such as hospitals are unacceptable.

With regard to the United Nations framework for responsible State behaviour in cyberspace, it must be underlined that Member States of the United Nations have endorsed – through the adoption of United Nations resolution 70/237 – the conclusions of the Group of Governmental Experts reports of 2010, 2013 and 2015, which constitute a solid, consensual basis for further work. The United Nations and its Member States have undertaken substantial efforts to both build a shared international understanding on the governance of cyberspace *and* develop real actions to implement this common vision on the ground. In an efficient and effective multilateral system, it is imperative that we take forward any further discussion starting from this consensual basis, in order to avoid revisiting laborious compromises of the past while stalling future efforts.

Third, we believe that we should better align international criminal justice with the challenges of the twenty-first century. This is why Belgium has joined Liechtenstein in its initiative to create a Council of Advisers on the Application of the Rome Statute to Cyberwarfare in order to explore the role the International Criminal Court could play in this new regulatory framework. We are looking forward to receiving the Council of Advisers' final report which is scheduled to be presented this year.

Guiding principles are to be followed by actions in order to make a difference. In that regard, Belgium is convinced that the proposal by Egypt and France to establish a programme of action constitutes the right structure to implement our vision. Belgium is proud to support this initiative together with more than 50 other countries, and we hope that many other States will join.

At the national level, Belgium has recently adopted, in May 2021, a new National Cybersecurity Strategy 2.0 for 2021–2025 that sets out our country's cross-cutting approach in terms of increasing our cyberresilience and combatting cyberthreats. The primary objective of this national strategy is to "propel Belgium into the rank of the least vulnerable countries in Europe".

Belgium's cybersecurity policy also provides for a new attribution mechanism which is conceived as a deterrent tool. If we want to effectively prevent and deter malicious cyberactivities in an environment where cyberattacks are growing in number and in complexity, formal attribution of malicious cyberactivity targeting a vital organization in Belgium is an important instrument. The national attribution procedure can also be activated with a view to supporting an allied country victim of similar attacks.

Moreover, the national strategy prescribes a clear international commitment. And this is because, Belgium is walking the talk, convinced that increased international cooperation is needed to promote security and stability in cyberspace.

Increased international cooperation also means more capacity-building and more support for confidence-building measures, including through efforts of regional organizations such as the Organization for Security and Cooperation in Europe (OSCE). Belgium takes an active part in the work of OSCE to render those confidence-building measures concrete *and* operational. In terms of capacity-building, the needs are important and urgent globally. Existing cooperation or capacity-building programs such as those offered by the European Union or by the Global Forum on Cyber Expertise need to be reinforced and extended. It is in the interest of us all to enhance global resilience to cyberthreats.

Annex XXII

Statement by the Permanent Mission of Brazil to the United Nations

At the outset, I would like to congratulate Estonia on the great initiative of promoting, for the first time, an official Security Council open debate on cybersecurity in the broader context of maintenance of international peace and security. The rapid evolution of information and communications technologies (ICT), which have come to permeate all domains of human existence, impels us to update the concept of threats, adapt the existing normative framework to this new reality, and develop new patterns of responsible State behaviour in order to overcome modern challenges and curb the emergence of conflicts.

Although the topic of cybersecurity has only just been raised in the body that bears the primary responsibility for the maintenance of international peace and security, Member States have been debating it for more than two decades – at least since 1998, when the topic was first introduced on the agenda of the General Assembly. During this period, we have witnessed the adoption of four consensual reports from Groups of Governmental Experts (Groups of Governmental Experts) – two of them chaired by Brazilian experts – and one equally consensual report from an Open-ended Working Group. Together, these documents form an acquis, a common body of understandings and non-binding, voluntary norms, rules and principles that help guide the use of ICT by States.

One of the greatest contributions of this acquis to the maintenance of international peace and security is the assertion that international law, including international humanitarian law (IHL), is applicable to cyberspace. In our voluntary national contribution to the official compendium of the last Group of Governmental Experts, we reaffirmed Brazil’s firm belief that, in their use of information and communications technologies, States must comply with international law, including the Charter of the United Nations, international human rights law and international humanitarian law. The United Nations and other regional organizations have recognized that international law, and in particular the Charter of the United Nations, is applicable to cyberspace, and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible information and communications technology environment. Hence, in current discussions, the question is no longer whether, but how international law applies to the use of ICT by States.

While analogies in relation to the physical world might work most of the time to determine such application, the unique characteristics of cyberspace create new situations that international law was not originally designed to regulate. The interconnectivity of information systems, the intangible nature of the ICT environment and the complexities of the problem of attribution of responsibility for malicious and offensive acts in cyberspace, among other factors, pose new challenges to international law, whose development has been based on a physical and territorial international order.

Differences in interpretations by States of how international law applies to the use of ICT increase the risk of unpredictable behaviour, misunderstandings and escalation of tensions. Therefore, it is important to progressively identify areas of convergence among States on this matter and, where divergences are identified, to jointly work towards increased coherence in the interpretation of existing rules. If necessary, development of additional norms should also be considered as a means to fill potential legal gaps and resolve remaining uncertainties.

The maintenance of international peace and security depends heavily on the level of trust that prevails between States. Therefore, in addition to the recognition of the applicability of international law and to the establishment and implementation of norms, rules and principles of responsible State behaviour, it is of paramount importance that governments implement confidence-building measures. The establishment of a network of points of contact at technical and political levels, as well as the exchange of national views on threats and on ICT incident management are important cooperative and transparency measures. These initiatives not only help to prevent misunderstandings and misperceptions, but are also useful to address serious ICT incidents and to de-escalate tensions in a scenario of crisis.

Capacity-building is also an essential tool in the promotion of a peaceful ICT environment. As in other domains, inequality among nations can generate insecurity also in cyberspace, with direct impact in the kinetic world. International cooperation for the development of national institutions, human resources and public policies contributes to reducing States' vulnerabilities and are fundamental for the universalization of the implementation of international law and of norms, rules and principles of responsible State behaviour in cyberspace. If there is one thing the pandemic has taught us it is that no one is safe until everyone is safe – the same reasoning can be applied to the highly interconnected and interdependent cyberspace.

Given the multi-stakeholder nature of the cyberspace, Brazil is of the view that no effective discussions on cybersecurity can succeed without the contributions of civil society, academia and the private sector. A multi-stakeholder approach is essential to identifying and combating threats, preventing conflict, promoting common understandings, increasing cyberresilience and fostering cooperation. Broader interaction between public and private actors from different countries, exchanging experiences and sharing best practices, is essential for achieving a more open, secure, peaceful and accessible ICT environment.

Brazil has been actively engaging in discussions on cybersecurity within the United Nations. We have always sought to be proactive in both the Groups of Governmental Experts and the last Open-ended Working Group. Brazil will maintain its constructive approach in the debates of the new Open-ended Working Group, which will hold its first substantive session in December, as well as in other mechanisms of regular institutional dialogue that may be established, such as the programme of action on cybersecurity. At the same time, as a newly elected non-permanent member of the Security Council, we intend to contribute to the development of the discussions on the impact of the use of ICT in the context of international security also in this body. In Brazil's view, the Council should be guided first and foremost by the objective of promoting adherence to past and future recommendations adopted by the General Assembly on the issue of cybersecurity.

I thank you!

Annex XXIII

Statement by the Permanent Mission of Canada to the United Nations

[Original: French]

We thank Estonia for organizing this Security Council session on such a timely and relevant topic. Canada is pleased to have the opportunity to contribute to this discussion.

The world is increasingly reliant on digital technologies and the Internet. Threats to international peace and security emanating from cyberspace are numerous. Interference in democratic processes is one area of particular concern. Another is the recent increase in ransomware incidents. We must therefore continue to take steps to maintain a free, open and secure cyberspace.

The agreed framework for responsible State behaviour in cyberspace is the foundation of peace and stability in this space. The framework consists of recognition of the applicability of international law to cyberspace, adherence to the internationally agreed norms, capacity building, and the use of confidence building measures. Together, these elements reduce the risks of escalation and conflict.

This framework was reaffirmed in the recent consensus reports adopted by the United Nations Open-ended Working Group and Group of Governmental Experts. All United Nations Member States have now committed to be guided by the framework.

International law is vital to ensuring that the rules-based international order extends to cyberspace. The recent Open-ended Working Group and Group of Governmental Experts reports reaffirmed the applicability of international law in cyberspace, and made important advances in this regard. The Working Group report recommended greater cooperation on capacity building in international law, in order to enable more States to develop their national views and build common understandings. In the Group of Governmental Experts report, the applicability of international law was reaffirmed, and international humanitarian law was specifically mentioned.

The May 2021 report produced by the Group of Governmental Experts provides guidance on the implementation of the 11 voluntary norms of responsible State behaviour adopted in 2015 and endorsed by all Member States through General Assembly resolution 70/237. Canada believes that these agreed norms and international law are largely sufficient to guide State behaviour in cyberspace. However, work remains to be done on their dissemination and implementation. The recent high-profile ransomware incidents perpetrated by criminal groups resulted in widespread disruptions of key industries such as energy and food supply. They also affected financial markets.

Although criminal groups were responsible for these acts, these examples highlight the importance of international law, and of the 11 Group of Governmental Experts norms, several of which address threats to critical information and communications technology infrastructure directly or indirectly. One norm stipulates that States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. Another says that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

Criminal actors who engage in ransomware and other criminal activities live in and work from States. They use States' digital infrastructure to undertake their malicious activity. They are subject to those States' laws. When informed of potential malicious activity emanating from their territory, States have a responsibility to respond, enforcing their laws and cooperating with other States. By agreeing to be guided by the Group of Governmental Experts norms, we have all undertaken to do this. This is also why a growing number of States have adopted strong laws to combat cybercrime. In many cases, States have based their laws on the Council of Europe Convention on Cybercrime, also known as the Budapest Convention, which now has parties from all regions of the world.

As we have seen in recent situations, all States do not always respect the framework of responsible State behaviour, unfortunately. Some are allowing cybercriminals to operate with impunity from their territory. Others are using proxies or purposely engaging in malicious cyber activity that goes against the framework. On several occasions, Canada has joined international partners in calling out and responding to such behaviour and the threat it poses to international peace and security.

Canada was one of the 27 signatories of the September 2019 Joint Statement on Advancing Responsible State Behaviour in Cyberspace. In addition to reaffirming the framework of responsible State behaviour, we committed to work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law.

That is what we have been doing, and we will continue to do so. It is important to highlight counter-normative behaviour, in order to uphold the framework of responsible State behaviour. We encourage others to do the same.

Shifting to the way ahead at the United Nations, Canada looks forward to engaging constructively at the Open-ended Working Group on security of and in the use of information and communications technologies (2021–2025). We will also actively contribute to the development of a programme of action on cybersecurity. Canada is a co-sponsor, as we believe that the Programme of Action could serve as a useful, action-oriented forum to promote the implementation of the framework for responsible State behaviour.

The success of these two processes will depend on their ability to integrate diverse voices and perspectives in their working methods and outputs. At the Open-ended Working Group, Canada has argued for meaningful participation of non-governmental stakeholders. Civil society, academia, the technical community and the private sector have much to contribute to these discussions, as they play an important role in implementing their recommendations of the Group of Governmental Experts and the Working Group. We will advocate for strong stakeholder engagement in the Programme of Action as well, as it is being developed.

It will also be important to ensure that the voices of women are meaningfully heard, whether at the Open-ended Working Group or in the Programme of Action. Gender should be mainstreamed in both processes from the outset, to ensure that the work of both groups addresses the gender aspects of cybersecurity. It has been well documented that conflict mediation processes that included meaningful participation of women led to much stronger outcomes and less chance of hostilities resuming after peace processes concluded. United Nations cyber processes can be similarly strengthened by including the meaningful participation of women. Inclusion is important for the success of both processes.

In short, Canada remains a steadfast supporter of the framework for responsible State behaviour in cyberspace. We will continue to promote the implementation of the recommendations of past Groups of Governmental Experts and of the recent Open-ended Working Group. We will also persist in calling out and responding lawfully to malicious cyber activity that goes against the framework. We look forward to continuing to work with the international community to promote international peace and security by enhancing stability and security in cyberspace.

Annex XXIV

Statement by the Permanent Mission of Chile to the United Nations

Chile reaffirms its position that international law, and in particular the Charter of the United Nations, is applicable and essential to maintain peace and stability and to promote an open, secure, stable, accessible, and peaceful information and communications technology (ICT) environment. This, alongside with specific principles of the Charter of the United Nations, in particular the peaceful settlement of disputes, the prohibition of resorting to the threat or use of force against the territorial integrity or political independence of any State, non-intervention in internal affairs of other States, and respect for human rights and fundamental freedoms, are indivisible in the physical as in the digital domains, and as such Chile will continue promoting its application.

Malicious ICT activities by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals. Malicious activity against critical infrastructure that provides services domestically, regionally or globally, has become increasingly serious, including malicious ICT activity affecting 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 sector entities. In future conflicts these malicious activities can be more destructive and seriously affect people’s well-being and lives. In this sense, countries could be seriously affected by cyberattacks generated in the context of armed conflicts.

During armed conflicts, States should plan, lead, and execute their operations in cyberspace will strictly abide by the rules of the international law, with special consideration to the international law in Human Rights and the international humanitarian law.

Chile strongly supports the work of the Group of Governmental Experts (Group of Governmental Experts), and its reports and recommendations adopted in 2010, 2013, 2015 and 2021, because they represented an enormous advance with respect to international law, norms, and confidence-building measures in the field of ICT. Chile also supports the work of the Open-ended Working Group and its recommendations. To reduce the malicious use of cybercapabilities and to build a more stable cyberspace, it is important to follow and to implement these recommendations, in all levels.

The programme of action for advancing responsible State behaviour in cyberspace is a positive, constructive, and realistic initiative that could help us to move forward and achieve concrete results in the framework of the ICT environment. The programme of action could be a permanent, inclusive, consensus-based and action-oriented international instrument to advance responsible behaviour in the use of ICT in the context of international security. As a co-sponsor of this initiative, Chile believes that the programme of action would offer a platform to adopt operational recommendations, to promote international cooperation and foster assistance programs tailored to the needs of beneficiary States, notably in capacity-building.

Regarding compliance with existing international law and the implementation of norms of responsible State behaviour in cyberspace, it is important that States can develop and share their views with other States regarding how international law applies in cyberspace. Capacity-building in this area is also crucial. The existence of guidelines for the implementation of norms is an important step that should help

States to advance in this matter. Regional organizations can play a key role in assisting States in their implementation of norms and compliance with international law, developing regional strategies in this regard, as well as training and capacity-building.

Chile believes that is fundamental to strengthen confidence-building measures in cyberspace and capacity-building for which regional organizations must have a paramount role. In this regard, we highlight the work being carried out by the Organization of American States through its Working Group on Cooperation and Confidence-Building Measures in Cyberspace, as well as the work and progress made by the Organization for Security and Cooperation in Europe and the Association of Southeast Asian Nations.

It is important to promote dialogue across regions regarding this matter, but also in capacity-building and implementation or norms. This dialogue should consider the exchange of experiences, information, guidelines, best practices, lessons learned, and inviting members of organizations to participate in these regional processes. States should strengthen their national points of contact, as well as the role of their Ministries of Foreign Affairs regarding cyberspace and ICT policies. Cyberdiplomacy is an important tool that can help States to improve cooperation between them, building confidence. States should also consider to established bilateral mechanisms for dialogues and cooperation on cybersecurity and cyberspace.

Chile believes that multilateral processes must be as inclusive and transparent as possible. The discussion on ICT should include the private sector, academia, civil society, industry, and the technical community, among others. It is not possible to build a stable and secure environment in cyberspace if we do not guarantee the participation and work of all stakeholders. The more actors are part of the discussion, the more likely we must achieve results that are beneficial to all. In this sense, we believe that it is necessary that we can listen to all interested parties and that they can also present their views and contributions in official sessions. In that sense, States should include all stakeholders when it comes to generating policies, strategies, and other initiatives that aim to prevent conflict, build common understandings, and increase cyberresilience.

Annex XXV

Statement by the Permanent Mission of the Czech Republic to the United Nations

The Czech Republic wishes to express its appreciation to the Republic of Estonia for organizing the historically first open debate of the Security Council on the topic of cybersecurity in the context of international peace and security. States' adherence to international law and responsible State behaviour in cyberspace are key elements of conflict prevention and maintenance of international peace and security.

The Czech Republic aligns itself with the statement submitted by the European Union, and wishes to emphasise two additional points as follows.

Present and emerging cyberthreats to international peace and security

Cyberspace offers tremendous benefits for human and economic development however it is also becoming a domain of growing dependencies and security challenges. Our increased reliance on ICT during the coronavirus disease (COVID-19) pandemic, which is being continuously exploited by malicious actors for their own benefit, is a clear reminder of the growing challenges in cyberspace. Notably, we have seen an alarming increase of malicious information and communications technology (ICT) activities directed against critical infrastructure delivering essential services to the public, including those targeting medical facilities, water, energy, sanitation, electoral infrastructure and the general availability of the Internet. In particular, the growing number of cyberattacks disrupting provision of health-care results in further loss of life, undermines our collective ability to respond to COVID-19, and ultimately threatens international peace and stability.

Such reckless ICT activities aimed at intentionally damaging critical infrastructure also risk potentially devastating humanitarian consequences, and if attributable to a State, would violate States' obligations under international law. The Czech Republic therefore welcomes that all Member States have recently affirmed through the Group of Governmental Experts and the Open-ended Working Group final reports that ICT activities directed against critical infrastructure are unacceptable. While a political commitment is the first necessary step, protecting critical infrastructure from ICT threats will also require sustained practical efforts by the international community, including through intensified technical cooperation and concrete cyberrelated capacity-building programmes. The Security Council can also play a decisive role by ensuring that State-sponsored ICT activities directed against critical infrastructure will have consequences.

New and emerging cyberthreats affect not only national security of States, but also increasingly threaten the well-being and safety of individuals. The Czech Republic is particularly concerned by the growing political divide between States who advocate the protection of personal freedoms in cyberspace and those who call for increased technological surveillance. In our view, the expansion of State-sponsored mass surveillance techniques through ICT, partial or complete Internet shutdowns and extensive content censorship raise serious human rights concerns. A determined action to protect citizens from arbitrary and unlawful exercise of State power in cyberspace is essential. These trends, coupled with potential risks associated with the introduction of artificial intelligence into various facets of our lives, raise new security challenges, threaten to undermine trust and confidence in cyberspace, and may ultimately degrade our ability to maintain international peace and security.

Strengthening compliance with international law and norms of responsible State behaviour

The Czech Republic would like to reiterate that States' compliance with their obligations under international law is an essential ingredient to maintain a free, peaceful, stable, secure, interoperable and accessible cyberspace. The applicability of existing international law to State use of ICT was affirmed by all States, specifically through the universal endorsement of the 2013 and the 2015 Group of Governmental Experts reports in General Assembly resolutions 68/243 and 70/237.

In this regard, the Czech Republic also recalls that the rights of States to exercise exclusive jurisdiction over the ICT located on their territory give rise not only to rights but also to specific obligations under international law. In particular, the Czech Republic wishes to reiterate that existing bodies of law, including international humanitarian law and international human rights law apply to State conduct in cyberspace without exception.

Regrettably, a small minority of States continues to question the applicability of existing international law to cyberspace, including the applicability of the international humanitarian law to the use of ICT in the context of armed conflict. The Czech Republic wishes to underline that in its view, the applicability of international humanitarian law to ICT operations does not promote the militarization of cyberspace, nor does it promote militarization of any other domain. On the contrary, international humanitarian law places limits on the use of force by requiring all used means and methods of warfare in the context of armed conflict to be employed in accordance with its rules; including the principles of humanity, distinction and the rule of proportionality.

Additionally, the Czech Republic recalls that according to the law of responsibility for international wrongful acts, all States have an obligation to exercise due diligence and take concrete measures within their capacity to ensure their territory is not being used to conduct malicious cyberactivities against other States.

The Czech Republic equally recognizes that State's capacity to implement the existing framework of responsible State behaviour in cyberspace, including its ability to adequately exercise due diligence, is intrinsically linked to that State's capacities. In this regard, the Czech Republic stresses the need to step up international efforts to build cybercapacity and increase cyberresilience globally, including through the early establishment of the United Nations programme of action for responsible State behaviour in cyberspace, which would allow the Member States to advance the implementation of existing commitments through practical and results-oriented action.

In conclusion, the Czech Republic is fully committed to a human-centric approach to cybersecurity that emphasises the need to protect the safety and security of individuals in the ICT-environment, be it through protecting critical infrastructure from ICT threats, or through ensuring that cybersecurity measures are not being used as a pretext for constricting the full enjoyment of human rights and fundamental freedoms in cyberspace.

Annex XXVI

Joint statement by the Permanent Missions of Denmark, Finland, Iceland, Norway and Sweden to the United Nations

I have the pleasure to speak on behalf of the Nordic countries: Finland, Iceland, Norway, Sweden and my own country, Denmark. We are grateful to the Estonian presidency for placing this very pertinent topic on the Council's agenda. It is a great opportunity for all Member States to build on our commitment to the application of international law in cyberspace and the framework of responsible State behaviour in cyberspace with the aim of promoting peace and stability.

The world benefits in countless ways from the development of information and telecommunication technology. It has brought tremendous economic progress and societal development. In the current pandemic, cyberspace has allowed many of us to stay in touch with family, friends and colleagues and sustain important functions of society, including the operation of critical infrastructure vital to manage the health crisis. Yet, cyberspace has also been used to spread disinformation about the coronavirus disease (COVID-19) virus, exposing our collective vulnerability to disruption and abuse of the information space. Moreover, the pandemic has exposed deep digital divides, not least the gender digital divide. As Nordics, we strongly believe that a globally accessible, free, open and secure cyberspace is fundamental not just to how the world operates today, but for our shared ambitions to build a better, greener and safer future.

Unfortunately, malicious cyberactivities continue to challenge the safety and stability of cyberspace. The last one and a half years have revealed that State and non-State actors will take advantage of any opportunity, even a global pandemic, to carry out malicious activities in cyberspace. Such activities are unacceptable. They threaten the integrity, security and prosperity of our societies and undermine international peace and stability.

Let me highlight three interrelated trends that pose a challenge to international peace and security.

First, the recent increase in cyberattacks against the supply chains of companies, organizations and governments has left tens if not hundreds of thousands computer systems exposed. Such attacks show a blatant disregard to those affected. The goal is often to steal sensitive information and intellectual property to gain an advantage in geopolitical competition. Such attacks might have additional unintended effects as the backdoors are left open for everyone to exploit.

Second, State-sponsored disruptive cyberattacks such as WannaCry and NotPetya have been released on the world with a complete indifference to their negative systemic effects across the global. Such attacks have resulted not only in vast financial losses, they have also crippled information and communications technology systems including at hospitals and industrial control systems affecting crucial electricity supply. These activities jeopardise the health and safety of our citizens.

Third, States need to take action against the increasingly serious and destabilizing effects of cybercrime originating from their territory. The recent ransomware attacks against fuel supply in the US, hospitals in Ireland and food production in Brazil, the US and Australia illustrate that the consequences of cybercrime have become a national security concern with possible effects on international peace and security. The increasing conflation of State and non-State groups further complicates the threat.

Day by day, the threshold for tolerated behaviour in cyberspace is moving in the wrong direction. We must revert this trend by living up to the shared commitment we, the Member States, made when we endorsed the Group of Governmental Experts reports and the Open-ended Working Group consensus report. In this spirit, we once again reaffirm that international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law applies to States' behaviour in cyberspace. We also call for stronger adherence to the 11 voluntary non-binding norms for responsible State behaviour in cyberspace formulated in the 2015 Group of Governmental Experts-report bearing in mind the guidance and the additional layer of understanding to these norms, provided by the 2021 Group of Governmental Experts-report. This would go a long way in addressing the challenges mentioned above.

We must raise the cost of malicious cyberactivity by collectively holding those responsible to account. All States must exercise due diligence and take appropriate action to address malicious cyberactivity originating from their territory. Hacker groups should not be allowed to operate with impunity.

We support the continued exchange of information and best practices within the United Nations, notably on the implementation of norms for responsible State behaviour, confidence-building measures and the application of existing international law in cyberspace. We should pursue an action-oriented track that builds on the consensus framework we have already agreed upon with the General Assembly's endorsement of the Open-ended Working Group report and Group of Governmental Experts-reports. This constitutes the basis for any further discussion. The proposal of establishing a programme of action is a good way to move towards full implementation of already agreed norms.

We must recognize that while the cyberthreat is a global challenge, it has different manifestations in different countries and regions. Upholding strong cyberresilience throughout all our societies is crucial not only to our shared security, but to the enjoyment of human rights. We need to cooperate to build capacity globally.

States cannot do it alone. Countering the threats in cyberspace requires a multi-stakeholder approach to help prevent conflict, build common understanding and increase confidence- and capacity-building. We need the United Nations as a convener and platform to establish effective cooperation between governments, civil society, academia and the private sector. We support the Secretary-General's Road map for Digital Cooperation, in particular when it comes to private sector engagement, which is vital in managing critical infrastructure, collecting information and protecting systems and personal data.

All States must live up to their responsibility and comply with international law and respect norms in cyberspace. If not, the threat from malicious cyberactivity to international peace and security will keep growing. Cyberattacks will continue enhancing the risk of conflict, endangering human lives, violating human rights, stifling economic activity, deepening dividing lines and causing disputes. All States have a role to play in promoting and upholding a rules-based, predictable, open, equal, free, accessible, stable and secure cyberspace to the benefit of all.

Annex XXVII

Statement by the Permanent Representative of Ecuador to the United Nations, Cristian Espinosa

[Original: Spanish]

Allow me first of all to thank Estonia for including this item on the formal agenda of the Security Council a year after the Arria-formula meeting on the subject. We also note the leadership of Prime Minister Kallas in this area and welcome the presentation of the Under-secretary-General and High Representative for Disarmament affairs Izumi Nakamitsu.

The biennium 2020–2021 marked a milestone in the area of cyber diplomacy not only because of the mandate and substantive results achieved on 12 March 2021 by the first Open-ended Working Group on developments in the field of information and telecommunications in the context of international security and by the consensus achieved on 28 May by the Group of Governmental Experts on responsible State behaviour in cyberspace, but also because of the Coronavirus disease (COVID-19) pandemic which accelerated digital transformation.

The pandemic had an impact on all dimensions of peace and security in different ways. Cybersecurity was no exception. Security of essential services became a major concern, along with the need to preserve critical infrastructure against possible cyberattacks that could cause damage in the physical world.

The threats we are facing today are for the most part transnational, and the only way to counter them, both in the physical and the virtual world, is through international cooperation and dialogue. Thus, if one Member State is not safe, none is safe.

Ecuador thus reaffirms its commitment to the norms in force, as reflected in the reports of the Group of Governmental Experts and the results of the Open-ended Working Group, in conformity with international law. My delegation wishes to stress that no sphere can remain outside the spectrum of international law, including international human rights law and international humanitarian law, which does not mean that the militarization of cyberspace would be acceptable.

On the contrary, Ecuador defends the exclusively peaceful use of cyberspace. The Charter of the United Nations prohibits the use of force, and therefore all international disputes in cyberspace should be settled by peaceful means.

Accordingly, we promote trust and capacity building, for which we believe that an operational platform is required to facilitate the implementation by States of the existing framework. That platform could take the form of a programme of action.

We defend and support any mechanism that would promote greater international cooperation to reduce imbalances in the ability to implement the rules for responsible State behaviour.

In addition, we recognize the contribution that regional organizations can bring to capacity development and implementation of such norms. An example is the valuable work of the Organization of American States in this area, in particular its efforts against cybercrime and terrorism.

I conclude by recalling the need to preserve and promote the responsible use of information and communications technologies as a key guarantee of stability and security in cyberspace. Likewise, we believe that the existing norms should be strengthened, taking into account rapid technological development. For its part, the Security Council must consider mechanisms to strengthen the use of technologies as a means to consolidate peace as a complement to regular efforts.

Thank you.

Annex XXVIII

Statement by the Permanent Mission of Egypt to the United Nations

Egypt attaches great importance to the international security aspects of information and communications technologies (ICT) and strongly calls for a central and leading role by the United Nations in promoting and developing rules and principles for the use of ICT by States through an inclusive and equitable process with the participation of all States.

A number of States are developing ICT capabilities for possible malicious uses and offensive military purposes. The use of ICT in future conflicts between States is becoming a reality and the risk of harmful ICT attacks against critical infrastructure is both real and serious. This new arms race has far-reaching ramifications on international peace, security, and stability, especially as the lines between conventional and nonconventional weapons continue to erode.

Furthermore, the relevant technologies developed by States are being transferred, copied, or reproduced by terrorists and criminals. The malicious use of ICT by terrorist and criminal organizations is a serious threat to international peace and security, especially in light of the attribution-related challenges.

Under international law and the Charter of the United Nations, all Member States should refrain from any act that knowingly or intentionally damages or otherwise impairs the use and operation of the critical infrastructure of other States as well as interfering in their internal affairs.

There is no doubt that the international security aspects of ICT have become too important and strategic to be left without clear binding rules at the international level. An inclusive process within the United Nations System is the best and most efficient way to establish arrangements that are equitable, comprehensive, and effective in this domain.

The United Nations has already taken some steps towards establishing a normative framework that complements the principles of international law. With the recent adoption by consensus of the Final Report of the Open-ended Working Group established pursuant to General Assembly resolution 73/27 on developments in the field of information and telecommunications in the context of international security, the United Nations has already established the initial elements of a framework for conflict prevention and stability in cyberspace.

The General Assembly called on Member States to be guided in their use of ICT by the norms for responsible State behaviour contained in the consecutive reports of the Groups of Governmental Experts under the First Committee. However, the implementation of these modest norms remains quite minimal at best, namely due to their voluntary nature and the lack of any follow-up mechanism.

The success of the Open-ended Working Group, which is the first inclusive process on this important topic, and the establishment of a new Open-ended Working Group by General Assembly resolution 75/240 represent promising progress towards a possible agreement on important mutual understandings among Member States on a number of key aspects.

Inclusive processes within the United Nations, primarily under the auspices of the General Assembly, are the most efficient way to establish equitable, comprehensive, and effective arrangements in this domain. For its part, the Security Council is encouraged to take into account the opportunities offered by emerging technologies while considering topics such as peacekeeping and counterterrorism.

Nevertheless, the Council should not be utilized as a legislative body that attempts to set norms and rules on behalf of the Member States on matters that necessarily require inclusive and transparent processes.

The recommendations which have been endorsed by the General Assembly by consensus can form the basis for politically or legally-binding rules, especially that they are derived from the principles of international law and the Charter of the United Nations.

Egypt has also encouraged the consideration of the establishment of an inclusive institutional platform dedicated to international cooperation on safeguarding the peaceful uses of ICT and mitigating their associated risks.

While we believe that international law and the principles of the Charter do apply to all domains including cyberspace, we also believe that there is a pressing need to identify specific obligations that make State behaviour in cyberspace consistent with international law and the objectives of the Charter of the United Nations.

In an increasingly connected world, any international regime on cybersecurity will be only as strong as its weakest link. Fortunately, there is consensus that capacity-building efforts have to be intensified and strengthened to prevent potential attacks against critical infrastructure and to develop the capabilities and technical skills needed in developing countries. The United Nations should lead a coordinated effort towards the provision of the necessary assistance for to developing countries.

In conclusion, ICT offer both massive opportunities and challenges. And we underscore that there is a pressing need to identify and develop rules for responsible State behaviour to increase stability and security in the global ICT environment and prevent cyberspace from becoming another arena for conflicts and arms races.

Annex XXIX

Statement by the Permanent Mission of El Salvador to the United Nations

[Original: Spanish]

El Salvador thanks the delegation of Estonia in its capacity as President of the Security Council for June 2021 for holding this open debate, which represents the first time that the Security Council has addressed cybersecurity in a substantive and formal manner. The initiative is a very important measure by which this body fulfils the international commitment to consider at the multilateral level the existing and potential threats to security in the field of information and communications technologies.

The development of new technologies represents an important opportunity to promote economic and social development of States. However, those information systems are vulnerable to attacks by persons who intend to manipulate communications networks for ideological purposes or for their own benefit. Given that criminals and terrorists take advantage of new information and communications technologies to meet their goals, efforts and resources must be invested to produce specialized guidelines for the development and application of common norms that will help us to prevent that type of crime and make it easier to bring to justice those who operate outside them.

We would thus like to highlight the importance of the international and regional instruments related to fighting cybercrime, as well as progress in that area, such as the establishment of the Open-ended Working Group for the purpose of elaborating a comprehensive international convention to combat the use of information and communications technologies for criminal purposes.

We welcome with satisfaction the efforts by the United Nations Member States in the area of terrorism within the international peace and security agenda. Nevertheless, we note that among the internationally binding instruments in that area, it is still impossible to find any direct mention of cyberspace. That is a gap that we all must bridge as soon as possible. We commend the efforts of the Security Council to discuss this major threat in a substantive way with a view to offering effective solutions. We urge this body to continue those efforts, leaving aside all political and/or personal interests and upholding the objective of the prevention of new conflicts and the creation of scenarios for its development.

El Salvador recalls General Assembly resolution 58/199, adopted in 2004, which included a list of the elements of critical information infrastructure of States, which, due to growing technological interdependence, are exposed to an ever-increasing number and greater variety of threats. That resolution also recognized that the vulnerabilities of critical information infrastructure continued to pose major problems of security.

Furthermore, in order to create the conditions for progress towards the common objective of international peace and security, the full exercise of human rights and economic and social development, we believe that the framework provided in General Assembly resolution 58/199 should be expanded to address the need to protect the activities of critical infrastructure from cyberattacks, in addition to current efforts to prevent cyberspace from becoming a platform for propaganda for radicalization, recruitment and collection of funds for criminal activities.

The world will continue to confront one of the greatest challenges since the establishment of this Organization, the outbreak of the coronavirus disease

(COVID-19) pandemic having revealed the vulnerabilities of essential systems in States. We have seen how during the COVID-19 pandemic cyberattacks have increased against national health systems, putting at risk the lives of millions of people and directly impacting the most vulnerable communities and sectors. We wish to use this forum to condemn the cyberattacks against the World Health Organization and the attempts at identity theft suffered in recent months. Undoubtedly, increased interconnectivity assumes that an increase in those attacks could be seen in the coming years.

The malicious use of information and communications technologies has extended in recent months to cyberattacks against the energy, financial and food supply sectors; among other sectors, those are highly vulnerable to cyberattacks. Likewise, we have seen how disinformation activities for the purpose of influencing the perception of government officials and institutions have increased, which are often able to delegitimize their work, unleashing instability and social conflict.

All of the foregoing makes it imperative to continue working for prevention and codification of international law aimed at preventing their malicious use, which recognizes the interrelation with applicable international humanitarian law, including the area of cyber operations during armed conflict.

We stress the importance of working on the basis of consensus, without the intention of imposing solutions that are incompatible with the realities of States, as well as ensuring that progress achieved by the General Assembly through the various consensus agreements of the Group of Governmental Experts and the Open-ended Working Group on developments in the area of information and telecommunications in the context of international security are taken into account. In particular, we welcome the adoption by consensus of the agreement by the Open-ended Working Group in 2021, with the participation of the 193 Member States of the United Nations, including the 15 members of the Security Council and other relevant parties to the process.

El Salvador expects to work constructively in the Open-ended Working Group on development in information and communications technologies in the context of international security, which will conduct its substantive work from 2021–2025, and we applaud the work of the Permanent Representative of Singapore to the United Nations, Burhan Gafoor, as the Chair-designate of the process.

The fundamental role of regional organizations, the private sector, civil society, academia and other related sectors in preventing and combating those threats should be noted. It is urgent to continue the work of strengthening regional and international cooperation mechanisms to prevent and combat those challenges, through a dynamic exchange of information and good practices, capacity-building, standardization of legal frameworks and the use of new technologies as the path towards development and fighting organized crime.

Annex XXX

Statement by the Head of Delegation of the European Union to the United Nations, Olof Skoog

I am honoured to contribute the open debate on cybersecurity on behalf of the European Union and its Member States.

The Candidate Countries Turkey, the Republic of North Macedonia*, Montenegro* and Albania*, the country of the Stabilization and Association Process and potential candidate Bosnia and Herzegovina, as well as Ukraine and the Republic of Moldova, align themselves with this statement.

First, we would like to commend Estonia for holding this open debate on this crucial topic, at a moment where malicious cyberactivities continue to be at a rise, and the increasing challenges posed risk international security and stability in cyberspace, in particular under these special circumstances of a pandemic.

Digitalization has a growing impact on our security, economies and societies at large, creating both opportunities and challenges. Transport, energy and health, telecommunications, finance, security, democratic process, space and defence are heavily reliant on network and information systems, which are increasingly interconnected.

In this light, we are in particular alarmed by the recent increase in malicious cyberactivities targeting essential operators globally, including in the health-care sector, and affecting the availability, security and integrity of information and communications technology (ICT) products and services and consequently the continuity of operations, which might have spillover and systemic effects and enhanced risks of conflict.

We welcome therefore the opportunity to discuss this important issue in the Security Council, which has the primary responsibility for maintaining international peace and security. It is an opportunity to underline a number of challenges faced, to reiterate the achievements to date by the United Nations community, and to provide an outlook on how to address these issues within the United Nations.

In this regard, the European Union and its member States welcome the meaningful reports agreed by consensus of the recent Open-ended working group on Developments in the Field of information and communications technologies in the Context of International Security (Open-ended Working Group) and United Nations Group of Governmental Expert to advance responsible State behaviour in cyberspace.

The reports significantly contribute to increasing awareness, and allow enhancing the ability to prevent, respond to and recover from cyberthreats and malicious cyberactivities. This is much needed, as a lack of awareness and capacities constitute a threat in and of itself, as all countries are increasingly reliant on ICT.

Increasing global cyberresilience is therefore essential, as it reduces the ability of potential perpetrators to misuse ICT for malicious purposes. It also allows States to exercise due diligence and 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 United Nations Groups of Governmental Experts (UNGGEs) in the field of Information and Telecommunications in the Context of International Security.

* The Republic of North Macedonia, Montenegro, Serbia and Albania continue to be part of the Stabilization and Association Process.

The reports of the consecutive UNGGEs and the Open-ended Working Group offer a baseline for conflict prevention, cooperation and stability in cyberspace, i.e. reaffirming the application of international law, addressing norms of responsible State behaviour, confidence-building measures in cyberspace, and cybercapacity-building.

The European Union and its member States reaffirm that a framework for conflict prevention, cooperation and stability in cyberspace can only be grounded in existing international law, which includes the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law, as endorsed by the General Assembly since 2013.

Deepening understanding on how international law applies in cyberspace is to further reduce misunderstanding and increase accountability in cyberspace and the United Nations membership should continue to advance and implement this framework in view of international security and stability in cyberspace.

For instance, the European Union and its member States are of the view that international humanitarian law is fully applicable in cyberspace in the context of armed conflict. We reiterate that its application in cyberspace should not be misunderstood as legitimizing any use of force inconsistent with the Charter of the United Nations. International humanitarian law sets out essential protections for those who do not, or do not any longer participate in hostilities, inter alia to protect civilians against the effects of hostilities and combatants against unnecessary suffering, among others. It also imposes limits on permissible means and methods of warfare, including new ones.

Secondly, the adherence to norms of responsible State behaviour is of utmost importance. The set of agreed norms reflects the shared expectations of international community, which set standards for responsible State behaviour. It allows the international community to assess the activities and intentions of States in order to prevent conflict and increase stability and security in cyberspace.

Thirdly, cyberrelated confidence-building measures constitute a practical means of preventing conflict. Through cooperation and information sharing, regional confidence-building measures have proven to reduce the risk of misinterpretation, escalation and conflict that may stem from ICT incidents.

Lastly, the framework includes the important issue of capacity-building. We actively support the call for better coordination for enhancing coherence in capacity-building efforts in the use of ICT to close the digital divide, including by our numerous efforts with partners around the world.

The European Union supports cybercapacity-building work through its External Financing Instruments, which encompass a range of programmes with a global reach including actions implemented in Africa, Asia and Latin America, as well as the European Union’s Neighbourhood and the Western Balkans. Concretely, the European Union is currently investing in activities worldwide, to support the implementation in cooperation with its implementing partners, though projects such as European Union’s Cyber Resilience for Development, Glacy+, EU Cyber Direct and Enhanced Security In and With Asia Initiative.

In order to underline the framework for conflict prevention, cooperation and stability in cyberspace, the European Union will continue to promote responsible behaviour in cyberspace. In this light, the European Union and its Member States are committed to the settlement of international disputes by peaceful means also when such disputes arise in cyberspace.

The framework for a joint European Union diplomatic response is therefore part of the European Union's approach to cyberdiplomacy, contributing to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. In order to promote and protect an open, free, stable and secure cyberspace, the European Union will continue to use its cyberdiplomacy toolbox, and to cooperate with international partners to this end.

From the outset, and given the complex nature of cyberspace, it is of utmost importance for States as well as the multi-stakeholder community to tackle the challenges that cyberspace brings, improve cooperation and strengthen their capacities. We also have a primary responsibility to enable all stakeholders to seize their responsibility to advance an open, free, secure and stable cyberspace, grounded in human rights, fundamental freedoms, democracy and the rule of law, and support their efforts. The European Union's approach to cyberdiplomacy also take into account the prominence of gender perspectives in reducing the "gender digital divide" and promoting an effective and meaningful participation of women in the decision-making processes related to the use of ICT in the context of international security.

To strengthen the cooperation, we see a central role for the United Nations to advance the implementation of achievements to date. To promote an effective multilateral multi-stakeholder debate to advance peace and security in cyberspace, there is a clear need to take forward the United Nations framework for responsible State behaviour in cyberspace. Together with 53 Member States, the European Union propose to establish a programme of action to advance responsible State behaviour in cyberspace.

Building on the existing acquis as endorsed by the General Assembly, the programme of action offers a permanent platform for cooperation and exchange of best practices within the United Nations. The programme of action offers the opportunity to foster capacity-building programmes tailored to the needs identified by beneficiary States. It also provides an institutional mechanism within the United Nations to improve cooperation with other stakeholders such as the private sector, academia and civil society on their respective responsibilities to maintain an open, free, secure, stable, accessible and peaceful ICT environment.

Because of the permanent and action-oriented character of this platform, we think the programme of action proposal is timely and merits further exploration by the international community. It constitutes a solid and action-oriented basis for further work on the framework for conflict prevention, cooperation and stability in cyberspace and to ensure that States are able to reap the benefits of a global, open, stable and secure cyberspace.

Annex XXXI

Statement by the Permanent Mission of Georgia to the United Nations

We would like to express our gratitude to the Estonian presidency for convening today's high-level debate on this important issue and thank the distinguished speakers.

Georgia has been long committed to developing responsible and ethical cyberspace, including cybersecurity and resilience, to enable comprehensive frameworks for safe, reliable, trusted digital environment for the benefit of the whole nation. In last decade, we established necessary legal base of information and cybersecurity and identified critical information system subjects; adopted and implemented two cybersecurity strategies with relevant action plans; and the process for adoption is under way for the 3rd national cybersecurity strategy.

However, as we all know, together with major economic and social opportunities, innovation and development, cyberspace brings new kinds of security threats. In recent years we witnessed cyberspace being used not only for the purposes of terrorism, fraud and crime but also as a powerful tool for hybrid warfare and interference into internal affairs of States.

Unfortunately, Hybrid warfare also became a powerful instrument in the hands of for some States to further their national interests, and as this body is well informed, Georgia has a long and painful experience of dealing with hybrid threats emanating from one of its permanent members. Russian Federation has been waging the hybrid warfare against Georgia since early 90s and it has never seized trying to undermine the sovereignty, territorial integrity, European and Euro-Atlantic aspirations of our country.

The list of the incidents is extensive. In August 2008, during the Russia's full-scale military aggression against Georgia, we witnessed the first precedent of a massive cyberattack undertaken in parallel to on-going aggression. In 2019 a large-scale cyberattack was launched against websites, servers and other operating systems of the Administration of the President of Georgia, the Courts, municipal assemblies, State bodies, private sector organizations and media outlets. The investigation conducted by the Georgian authorities, in cooperation with our partners, concluded that this cyberattack was planned and executed by the Main Division of the General Staff of the Armed Forces of the Russian Federation.

Regrettably, even when the international community is in a fight against the coronavirus disease (COVID-19) pandemic, Russian Federation is still trying to gain political dividends by intensifying propaganda war against Georgia's one of the most successful institution in the fight against spread of the Coronavirus – Richard Lugar Center for Public Health Research. Russia's accusations represent a typical piece of misinformation and propaganda campaign against this unique laboratory that was established to identify and address outbreaks just like the pandemic.

Today we all witness aggressive application of hybrid toolkit by Russia not only in our region, but on a global scale as well. The most prominent instruments within the Russian hybrid toolkit are military presence, information operations, cyberattacks, support of proxy political groups, interference into domestic affairs and economic influence.

In conclusion, we must underline that cyberattacks and hybrid warfare against sovereign States represent grave violations of international law, its norms and principles and undermine international peace and security. And while reaffirming our commitment to continue strengthening the cybersecurity at national and international level, we also call on the international community to increase its attention towards malicious information and communications technology activities of the Russian Federation in Georgia and elsewhere.

Annex XXXII

Statement by the Permanent Mission of Germany to the United Nations

One and a half years ago, the coronavirus disease (COVID-19) pandemic hit the world and made us aware – with dramatic suddenness – of the extent to which digital technologies shape both our everyday lives and our economic resilience. At the same time, it has mercilessly exposed our vulnerabilities. Cyberattacks, including those conducted against critical infrastructures, can constitute a threat to international peace and security, and Germany remains convinced that this is an important topic for the Security Council.

International peace and security is coming under pressure from different sides: first of all, cybercriminal activities undermine the reliability and trustworthiness of technologies that are by now crucial for the functioning of our economies, governments and modern societies as a whole. To name just a few examples, there has been a sharp increase in denial-of-service attacks, phishing and the spread of malware since the outbreak of the COVID-19 pandemic. Attacks on critical infrastructure in Europe and North America and cyberattacks used as a vehicle for extortion, too, are on the rise.

Second, State-sponsored malicious cyberactivities for the purpose of espionage, sabotage, disinformation and destabilization or financial gain are damaging both international trust and cooperative mechanisms of conflict mitigation, and thereby threatening security worldwide.

Third, civil society as a whole and Human Rights Defenders in particular are under increasing pressure in cyberspace. Room for the freedom of expression, transparency and genuine communication – which the Internet is designed to provide – keeps shrinking.

In order to cope with these growing threats, a multi-pillar approach needs to be pursued: One pillar is to strengthen our resilience nationally and internationally. This includes improving technical infrastructure, political and legal capacities, as well as an increased international cooperation.

A second pillar is to further advance and define our common understanding of responsible State behaviour in cyberspace and to set red lines that must not be crossed. We must therefore defend the existing acquis achieved by the Open-ended Working Group and the Group of Governmental Experts and further advance the development of norms of responsible State behaviour.

It is Germany’s position that international law, including the Charter of the United Nations and international humanitarian law, applies online as it does offline. States should strictly refrain from supporting information and communications technology (ICT) activity contrary to their obligations under international law – not least in the light of the potential to create and escalate inter-State tensions. ICT activity must not intentionally damage critical infrastructure or otherwise impair the use and operation of critical infrastructure. In particular, no actor should jeopardize the general availability or integrity of the public core of the Internet, which is vital to the stability of cyberspace. We call on all States to adhere strictly to their due diligence obligations and to take swift action against actors conducting malicious cyberactivity from their territory – in accordance with international law.

In order to stimulate ongoing discussions on international law in cyberspace, Germany has published a policy paper on the applicability of international law in cyberspace, and we encourage others to do the same.

Agreeing on a common acquis is not enough, however. It is equally important for there to be a firm response to unacceptable behaviour. Various instruments can be considered, ranging from dialogue and exchange to political declarations by States or groups of States exposing and denouncing irresponsible behaviour, or imposing sanctions against the respective persons and entities. Together with our partners in the European Union, we have put in place a cyberrelated sanctions regime that allows us to respond to cyberattacks in a firm, effective and targeted manner and in full consistency with international law. We have used this instrument in the past and we will not hesitate to use it again if our security is compromised. Additionally, a culture of attribution can strengthen the normative framework and foster accountability in cyberspace.

A continuous exchange with civil society, the private sector and academia is essential in order to increase our resilience in cyberspace, and to advance the cause of Internet governance. The abundant expertise residing outside of public authorities has to be harnessed by, and included in, these efforts, with the aim being to maintain international peace and security in cyberspace.

Annex XXXIII

Statement by the Permanent Mission of Greece to the United Nations

Digital technologies deeply contribute to the current transformation of economies and societies, offering significant opportunities for economic growth, as well as sustainable and inclusive development. Cyberspace, in particular, has become one of the backbones of our societies. At the same time, the rise of malicious behaviour in cyberspace, including the abuse of information and communications technologies (ICT) by both State and non-State actors for malicious purposes, has become the source of new risks and challenges. Such behaviour threatens economic growth and can lead to destabilizing and cascading effects with enhanced risks of conflict.

We therefore strongly support the strategic framework for conflict prevention, cooperation and stability in cyberspace, endorsed by the General Assembly and we stress the need to focus our collective efforts on developing the skills and capacity to adequately address cyberthreats. The need for global cyberresilience is highlighted by the current global health crisis, in which we have observed cyberthreats and malicious cyberactivities targeting the health-care sector.

Global cyberresilience reduces the ability of potential perpetrators to misuse ICT and strengthens the ability of States to effectively respond to and recover from cyberincidents. As part of our latest efforts in strengthening global resilience and developing practical cooperative measures, we are currently in the process of organizing a regional cybersecurity seminar, with participants from the Western Balkans.

Through our active participation in international organizations such as the United Nations, NATO and the Organization for Security and Cooperation in Europe, we seek to cooperate, exchange experiences and best practices, and contribute to the highest extent possible in developing appropriate means to address cyberthreats. Furthermore, as a member of the European Union, we implement an inclusive and multifaceted strategic framework for conflict prevention and stability in cyberspace. Within the European Union, cybersecurity is a coordinated and collective effort between Member States that sets a unique and valuable precedent of multilateral cooperation.

We are highly committed towards a global, peaceful, secure, open and independent cyberspace governed by international law, where human rights, fundamental freedoms and the rule of law fully apply. We have been actively sharing our experiences in the implementation of norms, confidence-building measures, and capacity-building both bilaterally and multilaterally at all regional and international fora in which we participate. We are strongly committed to participate actively in further discussions at the United Nations on the issues of cybersecurity and we reaffirm our willingness to engage positively in an effort to make constructive progress.

Annex XXXIV

Statement by the Permanent Mission of Guatemala to the United Nations

Guatemala would like to express its gratitude to the Estonian delegation as President of the Security Council for convening this open debate on an issue that, without any doubt, is of utmost important for States to address. Cyberspace has become a central and indispensable domain of global activity, and its protection through responsible State behaviour is critical to ensuring the maintenance of international peace and security. We are confident that this kind of meetings are an excellent opportunity for our countries to exchange opinions and good practices on the different levels of implementation of an increasingly relevant topic.

The world is currently facing several security challenges that are exacerbated by the emergence of new threats, such as cybersecurity issues. Looking back at past cyberattacks, as well as their increase during the times of the coronavirus disease (COVID-19) pandemic, the need to address this topic is evident, especially if we take into account that it could affect the most vulnerable sectors of our society.

Cyberthreats and attacks arise and evolve derived from the various activities that are developed by the interconnection of digital media, which represents a complexity of conditions that require the participation and cooperation of all sectors of our countries, in order to develop the technical and legal frameworks that strengthen cybersecurity both domestically and globally.

As is the case in all countries, the increase in the use of information and communications technologies (ICT) has become widespread in all sectors of our society. This new scenario facilitates an unprecedented development of information exchange and communications, but at the same time, it involves new risks and threats that can affect the security of our populations.

Given this, my delegation would like to express its concern about these new technologies, especially given the civilian and dual-use nature of cyberspace and digital networks, which may be used by criminal and terrorist groups. It is extremely worrying that several States are developing information and communications technologies capabilities for military purposes and that the use of these technologies in future conflicts between States is becoming more and more probable.

Guatemala recognizes that the interconnected and complex nature of cyberspace requires joint efforts by governments, the private sector, civil society, and academia to address cybersecurity challenges in a comprehensive and balanced way. It is the responsibility of all these sectors to maintain an open, free, secure and stable cyberspace.

For this reason, my country promotes confidence-building and transparency measures and supports capacity-building activities, information exchange and the dissemination of best practices, both at the subregional, regional and international levels.

My delegation stresses that the applicability of international law to State behaviour in cyberspace, the voluntary non-binding norms of State behaviour applicable in peacetime and the implementation of confidence-building measures, remains crucial. Furthermore, after witnessing the existing gaps between countries on cybersecurity and defense, my country gives special interest to capacity-building efforts in order to find a more equitable playing field that would help maintain international peace and security.

Guatemala believes that regional organizations play an indispensable role in peacemaking on the ground. There is considerable potential in stepping up their presence in cyberspace, both regionally and globally, to innovatively advance the sustaining peace agenda. Regional and sub regional organizations have focused on improving States' security, which has made great strides in implementing practical confidence-building measures in the different regions to improve cyberstability. There's no doubt that, without these organizations' contributions, the efforts to conflict prevention and stability would be less.

Guatemala currently has a National Cyber Security Strategy whose main objective is to strengthen the capabilities of the country, creating the environment and conditions necessary to ensure the participation, development and exercise of the rights of people in cyberspace. Additionally, it has a Cyber Incident Response Center (CERT), which provides cybersecurity auditing, vulnerability scanning and alert classification services. Both of them were achieved with the accompaniment of the Organization of American States.

In addition to that, Guatemala is in the process of development of a law on cybercrime, clearly defining the lines of action and the types of crime with and in ICT in order to promote capacity-building through international cooperation, favouring due process by having well-defined protocols for the chain of custody and the handling of digital evidence. It is also necessary to mention that my country is honoured to be an observer country of the Budapest Convention, which seeks to tackle computer crimes and crimes on the Internet through the harmonization of laws between nations, the improvement of investigative techniques and the increased cooperation between nations.

My delegation considers the need to continue carrying out transformations and adjustments in the laws that govern each country in a harmonized way and to design systems that allow the detection, investigation and prosecution of probable crimes within a framework that safeguards the rights of individuals and at the same time reduces the risk of that computer networks are used against the confidentiality, integrity and availability of information. We hope that our discussion today will contribute positively and complement the process of cybernorm-making, taking place in the General Assembly, in particular through the meaningful works of the Group of Governmental Experts and the Open-ended Working Group 2021–2025.

At last we recall all States that ICT must be used peacefully and for the common good of humanity, promoting the sustainable development of all countries, regardless of their level of scientific and technological development.

Annex XXXV

Statement by the Chargé d'Affaires of Indonesia to the United Nations, Mohammad Kurniadi Koba

Allow me to thank Estonia for convening this meeting. I also would like to thank the briefer for her valuable briefing.

As people's dependence on digital connectivity increases, information and communications technologies (ICT) have become an integral part of our daily lives.

Moreover, during the coronavirus disease (COVID-19) pandemic, ICT has provided a lifeline for the public and private sectors in rendering essential services for the population.

In this regard, it is critical to stress that malicious cyberactivities by State and non-State actors, in particular those aimed at critical infrastructure, could jeopardize national stability as well as international peace and security.

In that context, Indonesia wishes to underscore the following:

First, the primacy of the rule of law to guide our conduct regarding the use of ICT as well as its implication for international peace and security.

The principles of international law and the Charter of the United Nations provide the fundamental legal rules guiding States on their use of ICT, including in responding to any malicious attacks.

All States must be guided by the same set of rules and laws. No one should be exempted.

Furthermore, Indonesia supports the norms of responsible State behaviour outlined in General Assembly resolution 70/237.

While continuing to address the growing need to identify and develop international legal framework on this matter, our endeavour should also be directed towards addressing gaps among countries and regions.

Apart from technical gaps, it is imperative to strengthen national policy frameworks as well as the implementation of existing international law and the voluntary and non-binding norms in cyberspace.

Second, the role of bilateral, regional and multilateral approaches in strengthening trust in cyberspace.

Cooperative measures at the bilateral, regional and multilateral levels are mutually reinforcing in advancing understanding and bolstering stability in cyberspace, in particular in the area of capacity and confidence-building.

ASEAN Confidence-building measures, through the establishment of Points of Contact, regular information exchanges, dialogue and sharing of best practices, have been contributing towards cyberstability in the Southeast Asian region and beyond, in particular through the ASEAN Regional Forum.

Furthermore, Indonesia underlines the merit of meaningful partnership with other multi-stakeholder entities to help States apply the framework of responsible behaviour in their use of ICT.

In this regard, we emphasize the need for developed countries to share ICT technologies with the developing countries. Just like all other global problems, ensuring that others have the right tools and capacities to address this threat, will contribute to overall stability in the ICT domain.

Third, the role of the United Nations in leading a coordinated effort in addressing conflicts that may stem from ICT incidents.

Today’s discussion is the first formal, dedicated Council debate on the impact of information and communications technologies on the maintenance of international peace and security.

It marks an important step forward on this issue in the United Nations.

In the future, the Council needs to anticipate rise in threats in the cybersphere, as well as possible significant incidents in the ICT environment which could lead to major war.

We underscore the importance of ensuring that United Nations actions remain coordinated and synergized. The Council should continue to respond to the international peace and security, as well as humanitarian implications of developments in the ICT domain.

At the same time, the Council must be guided by the norms and rules that are being deliberated upon and developed by the General Assembly.

Let me conclude by reiterating Indonesia’s commitment to advancing our common efforts to appropriately respond to the ever-growing challenges to the maintenance of peace and security relating to the use of ICT.

Annex XXXVI

Statement by the International Committee of the Red Cross

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to contribute to this Security Council open debate on “Maintaining International Peace and Security in Cyberspace”.

Over the past two decades, hostile cyberoperations have become an increasingly important concern for the maintenance of international peace and security. As societies are digitalizing, so are military capabilities of States and other actors. Today, the international community recognizes that “a number of States are developing ICT capabilities for military purposes” and that “the use of ICT in future conflicts between States is becoming more likely”.[10]

In light of this reality, the ICRC would like to recall the potential harm to humans that the use of cybertechnology can cause, and afterwards present how States can mitigate these adverse humanitarian consequences through action at the international and at the national level.

It is today well-known that cyberoperations against critical civilian infrastructure have caused significant economic harm, disruption in societies, and tension among States. In the final report of the “Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security”, all States recognized that cyberoperations against critical infrastructure risk having “potentially devastating humanitarian consequences”.[11] While the ICRC cannot confirm any cyberoperations with human casualties, we are concerned about the destructive effects of cyberoperations, such as the disruption of electricity supplies, water systems or medical services.[12] These kinds of operations pose acute risks to humans at all times. Our experience shows, however, that disrupting critical civilian infrastructure has particularly severe consequences in societies that are already weakened by armed conflict.

Adverse humanitarian consequences are *not* inevitable. States must take decisive steps to ensure that their use of cyberoperations during armed conflict complies with existing rules of international law. In the ICRC’s view, this requires action at the international and at the national level.

At the international level, States have affirmed that international law applies in the ICT environment. This comprises, first and foremost, States obligations under the Charter of the United Nations, in particular the prohibition against the use of force and the obligation to settle international disputes by peaceful means. Most recently, the Group of Government Experts also noted that “international humanitarian law applies only in situations of armed conflict”. The group recalled “the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report”, and it recognized “the need for further study on how and when these principles apply to the use of ICT by States and underscored that recalling these principles by no means legitimizes or encourages conflict”.[13] The ICRC fully supports this view: cyberoperations during armed conflict are not happening in a “legal void” or “grey

[10] Open-Ended Working Group, Final Report, 2021, para. 16; Group of Governmental Experts, Final Report, 2021, para. 7.

[11] Open-Ended Working Group, Final Report, 2021, para. 18.

[12] Available at www.icrc.org/en/document/potential-human-cost-cyber-operations.

[13] Group of Governmental Experts, Final Report, 2021, para. 71(f).

zone" – they are subject to the established principles and rules of international humanitarian law.

To ensure that international humanitarian law is understood and applied effectively, the ICRC welcomes further study of how and when this field of law applies. To avoid adverse humanitarian consequences and disruption of societies, we ask States to interpret and apply the rules and principles of international humanitarian law in a manner that takes into consideration the specific characteristics of the ICT environment. Essential questions on the protection of civilian life require further study and clear positioning by States. For instance, in an increasingly data-driven world, it should be a priority for States to agree that civilian data enjoys protection against attack, just as civilian paper files do. Moreover, States should affirm that cyberoperations that damage civilian objects by disrupting their functionality are subject to all international humanitarian law rules on the conduct of hostilities.[14]

While further study and agreement on how international law limits cyberoperations during armed conflict is important, these rules will only become effective through implementation at the national level. From discussions with military operators and experts, the ICRC identified a number of key steps on how States can, and should, avoid civilian harm from military operations during armed conflict.[15] Today, we would like to emphasize four of them:

– First, each State is responsible for all its organs involved in cyberoperations and other actors that act on that State's instructions, or under its direction or control. States must ensure that all of these actors respect international humanitarian law.

– Second, States should develop clear internal processes to ensure that if cyber-related means or methods of warfare are used, they comply with the applicable legal framework.

– Third, States have an obligation to take all feasible precautions to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber-related means and methods of warfare. In the ICT environment, this may include implementing technical measures such as "system-fencing", "geo-fencing", or "kill switches".[16]

– Four, States also have an obligation to put in place measures to protect the civilian population against the dangers resulting from military cyberoperations. Some of these measures may have to be implemented already in peacetime.

To conclude, the ICRC commends Member States for striving to advance international dialogue and agreement on the potential human cost of cyberoperations and measures to prevent and mitigate human harm. In our view, international humanitarian law must be part of such debates, and the ICRC remains available to lend its expertise to them.

[14] See also International Committee of the Red Cross (ICRC), International humanitarian law and cyberoperations during armed conflicts: ICRC position paper, 2019.

[15] ICRC, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021.

[16] "System-fencing" means preventing malware from executing itself unless there is a precise match with the target system, "geo-fencing" means limiting malware to only operate in a specific IP range, and "kill switches" signify a way to disable malware after a given time or when remotely activated.

Annex XXXVII

Statement by the Executive Director for Police Services of the International Criminal Police Organization (INTERPOL)

Introduction

Cybercrime is a global challenge in the digital era. Its impact goes far beyond what is being reported or detected, affecting the daily lives of over 4.5 billion people online. The recent increased reliance on the digital environment has created more criminal opportunities in cyberspace. Shifting its targets to governments, businesses, key infrastructure and even hospitals, cybercrime today poses a formidable challenge to security worldwide. Owing to its rapid growth both in scale and severity, the International Criminal Police Organization (INTERPOL) has put priority on combating cybercrime.

As a global and neutral inter-governmental organization, INTERPOL is cognizant of international law, norms, confidence-building measures and capacity-building efforts to maintain peace and security in cyberspace. In light of the objective of this open debate to better understand the growing risks stemming from malicious activities in cyberspace, INTERPOL presents this written statement to the Security Council to support their commitment to achieving a peaceful and secure cyberspace. The statement outlines the latest cybercrime trends and their impact as well as INTERPOL's global mechanisms and solutions that are available for its 194 member countries to address these pressing challenges.

Present and emerging cyberthreats

In the last year, INTERPOL has analysed a broad range of cyberthreats. Its recent assessment underlined that the coronavirus disease (COVID-19) pandemic has opened up new avenues for cybercriminals to carry out various forms of online criminality regardless of the region. The prominent threats include ransomware-based extortion, Business Email Compromise, illegal data-harvesting operations, misinformation and the re-emergence of older types of malware, repurposed to take advantage of the global pandemic.

The identified trends also involved a shift of targets to major corporations, governments and critical infrastructure.[17] Cybercriminals and fraudsters were exploiting fundamental social needs and anxieties. Since March 2020, INTERPOL has been receiving a number of requests from its member countries to address ransomware attacks against hospitals and other institutions on the front lines of the fight against the coronavirus.[18] By attacking these critical infrastructure which play a crucial role in responding to the outbreak, criminals were able to maximize the damage and financial gain.

While ransomware attacks are not new, it is the fastest growing form of cybercrime. Ransomware provides a highly enticing and lucrative business model for cybercriminals, with the use of double extortion and Ransomware-as-a-Service model. We also saw a pattern whereby such attacks were not geographically limited, suggesting that criminals were expanding their focus to target any institution across

[17] INTERPOL, Assessment Report of the Impact of COVID-19 on Cybercrime, retrieved from https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

[18] https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

the globe. For instance, the same ransomware strain which shut down a hospital in Europe was also used in Asia.

In addition, we have seen complex frauds hitting victims in Europe, and proceeds being routed as far as West Africa and South East Asia within hours. Massive data breaches also continue to occur causing significant financial losses to businesses worldwide. At the same time, cybercriminals are hiding in the Darknet that guaranties anonymous and untraceable access. This heightens the importance and relevance of INTERPOL's Notices, [19] in particular the Purple Notice, which is a tool for member countries to share information about the modus operandi of these fraudulent schemes. The goal is to disseminate this critical information faster than the next attack.

Furthermore, the convergence between cybercrime and financial crime is posing a complex challenge. This type of crime contains multiple phases from cyberattack to data exploitation, and then to money laundering phases of layering and eventual cashing-out. The use of cryptocurrency in this process also hinders an effective and timely response. Given the complexity, a joint operating model is required combining capabilities of different specialized units in law enforcement to better combat cyberenabled fraud and money laundering. To offer the full array of operational and analytical support in this regard, INTERPOL has launched the INTERPOL Global Financial Crime Task Force at the end of 2020.

Global mechanism to mitigate cyberthreats

Indeed, international police cooperation is vital in keeping the highly interconnected world safe and secure. As recognized in the UNODC's Comprehensive Study on Cybercrime, INTERPOL plays a unique role in facilitating police to police cooperation.[20] In support of 194 member countries, it is entrusted with the mandate of facilitating cross-border law enforcement cooperation and, as appropriate, supporting governmental and intergovernmental organizations, authorities and services whose mission is to prevent or combat crime – within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights.

Given its neutrality and global presence, INTERPOL is uniquely positioned to lead and coordinate the global law enforcement response to cybercrime. It also allows law enforcement worldwide to share information on cybercrime and threat actors, and offers a wide range of expertise, technical guidance and operational support. Based on this unique role, INTERPOL advocated and underlined the importance of international police cooperation in various United Nations policy processes such as the United Nations Expert Group to Conduct a Comprehensive Study on Cybercrime[21] and the United Nations Open-ended Working Group on ICT Security.

Taking the partnership to the next level, the second biannual review of the General Assembly resolution on the cooperation between United Nations and INTERPOL was unanimously adopted on 23 November 2020.[22] It was a meaningful achievement as it introduced new language on key areas of cooperation including cybercrime, thus providing greater legitimacy for further collaboration between the two organizations in this field.

[19] https://www.interpol.int/en/How-we-work/Notices/About-Notices.

[20] UNODC Comprehensive Study on Cybercrime, p.195.

[21] https://www.unodc.org/documents/Cybercrime/IEG_cyber_comments/INTERPOL.pdf and https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Statements/Item-3/INTERPOL_item_3.pdf.

[22] General Assembly resolution 75/10 on cooperation between the United Nations and the International Criminal Police Organization (INTERPOL).

In this era of digitalization, national solutions and even regional solutions are no longer sufficient. To help achieve international peace and security in cyberspace, INTERPOL is able to serve as a global mechanism to effectively combat cybercrime and provide its member countries with a variety of services and tools including:

- A secure global police communications system called the I-24/7 to share urgent police information securely and in real-time;
- 19 Databases[23] and Notices[24] that are instrumental in giving alerts to the international community and supporting transnational investigations;
- INTERPOL's Global Cybercrime Programme that delivers policing capabilities in preventing, detecting, investigating and disrupting cybercrime, with the aim to reduce to the global impact of cybercrime and protect communities for a safer world;
- INTERPOL Global Cybercrime Expert Group and Regional Working Groups with Heads of Cybercrime Units to discuss pressing issues pertaining to cybercrime and devise operational and strategic plans;
- Communications platforms such as Cybercrime Knowledge Exchange for sharing information securely within the wider law enforcement community and Cybercrime Collaborative Platform – Operations for closed operational discussions;
- Cyber Fusion Platform to aggregate cybercrime data and conduct in-depth analysis;
- INTERPOL's 24/7 Cybercrime Point of Contact to connect in real time cybercrime units from different countries for law enforcement cooperation;
- INTERPOL Global Cyber-Incident Response Team (I-CIRT) framework to coordinate global law-enforcement responses to major cyberincidents;
- INTERPOL Global Financial Crime Task Force to reduce the worldwide volume and impact of financial crime through enhanced international cooperation and innovation, with focus on cyberfraud and money laundering schemes.

A multi-stakeholder approach

Cybercrime investigations feature a number of challenges that are not experienced in the physical realm. For law enforcement, it is difficult to know first-hand that an attack has occurred, and even then reporting rates are low. Investigating cybercrime also takes specific skills and technology, which is not universally available. Cybercrime being inherently global is often detrimental to effective response with evidence and suspects located in multiple jurisdictions simultaneously.

To overcome these challenges, INTERPOL has placed partnership at the heart of its efforts in tacking cybercrime. At the 88th session of INTERPOL's General Assembly held in 2019, member countries have endorsed a legal framework titled "Gateway" that enables INTERPOL to share information with private sector companies.[25] This decision was based on the fact that law enforcement needs to work closely with the private sector where the majority of data and expertise lies in relation to cybercrime.

[23] https://www.interpol.int/en/How-we-work/Databases/Our-19-databases.

[24] https://www.interpol.int/en/How-we-work/Notices/About-Notices.

[25] https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-s-General-Assembly-sets-road map-for-global-policing.

INTERPOL’s Global Cybercrime Programme currently has 12 private partners under this framework which share up-to-date cybercrime information and expertise as well as provide technical assistance for law enforcement agencies. The access to data – from both the public and private sectors – allows INTERPOL to provide tailored operational support and technical guidance to member countries.

Furthermore, collaborating with various actors in the global ecosystem of cybersecurity is crucial as diverse datasets can help shape effective policies and operational responses to cybercrime. This also helps pool our wisdom to be resilient and agile especially in times of uncertainty. At the end of last year, INTERPOL supported the Nigerian Police, jointly with its private partner, in the arrest of members from an organized crime group responsible for phishing campaigns and Business Email Compromise scams affecting governments and private sector companies in more than 150 countries.[26]

INTERPOL also puts particular emphasis on prevention. To prevent cybercrime, INTERPOL works closely with its public and private partners to promote good cyberhygiene by running a series of global awareness campaigns. These efforts also support law enforcement organizations to overcome numerous challenges in tackling cybercrime by raising public awareness on the crime itself, ways to protect themselves and what to do when it occurs.

Conclusion

As the nexus of criminal actors, infrastructure and victims goes beyond national borders and jurisdictions, local law enforcement does not always have the capabilities or capacity to address these transitional elements in tackling cybercrime. Member countries should bear in mind that the gaps in law enforcement cybercapabilities or capacity across regions remain a fundamental enabler of crime networks to distribute their infrastructure and activities where risk is lower.

To mitigate these ever-evolving threats and risks concerning cyberspace, member countries should leverage and maximize the use of police-level cooperation for a timely and effective response. With a local footprint in each country, INTERPOL is able to connect the dots; to identify and disrupt the criminal actors in cyberspace, together with our member countries and partners.

It is evident that cybercrime can only be effectively combated through a globally coordinated – and importantly a rapid – response. We need to protect systems, prepare our leadership, share solutions and encourage the right response. In particular, law enforcement must be a trusted and effective partner, as the exchange of data is key – including between national police forces, the private sector, and global experts such as INTERPOL. Increasing trust within the global law enforcement community with “dare to share” attitude is crucial under the common goal of combating cybercrime.

At a time when the international community is put under exceptional pressure, ensuring our common security requires us to move towards more collaboration and inclusion. This is what INTERPOL stands for: assisting international law enforcement cooperation for a safer world. As we share the conviction that security and justice are key to achieving a peaceful and sustainable cyberspace, INTERPOL works at the side of the United Nations by facilitating international law enforcement cooperation. To make this endeavour a success, INTERPOL will continue to support its member countries in the fight against cybercrime.

[26] https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group.

Annex XXXVIII

Statement by the Permanent Representative of the Islamic Republic of Iran to the United Nations, Majid Takht Ravanchi

Cyberspace provides golden opportunities for mankind to constantly develop and promote all aspects of its life. Such an outstanding enabler must therefore not only be promoted throughout the world particularly in developing countries but also be protected against all threats.

Cyberspace can also be used to commit acts of aggression, breaches of the peace, “the threat or use of force”, “to intervene in matters which are essentially within the domestic jurisdiction of any State”, to violate the sovereignty of States or to coerce other States. These must also be effectively prevented.

As a guiding principle, the existing “applicable” principles and norms of international law, of course without misinterpretation or arbitrary interpretation, must govern the rights, duties and conducts of States with regard to cyberspace.

Yet, when there is no consensus about the applicability of international law, or even there is lack of international norms related to cyberspace, the international community must work towards developing required norms.

To that end, and given that the General Assembly is mandated by the Charter for the “progressive development of international law and its codification”, the Assembly must continue its ongoing efforts to develop and codify international principles and norms required for cyberspace, including in the form of an international legally binding instrument.

Parallel to such efforts, States must make every effort to promote the widest possible use of cyberspace for their development and in so doing, act responsibly and in accordance with applicable international law, in particular the Purposes and Principles of the United Nations.

The primary responsibility for maintaining a secure, safe and trustable cyberspace rests with individual States. Therefore, given the current complex situation of cyberspace governance, the prominent role and serious involvement of States in cyberspace environment governance at global level, in particular in policy and decision-making, must be promoted and ensured.

At the same time, the envisaged cyberspace governance must be developed in a manner that does not adversely affect the rights of States in making their choices of development, governance and legislation with respect to cyberspace environment.

The right of States to have “free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations” as well as “the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news”, which has also been reaffirmed by General Assembly in the 1981 “Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States”, must be fully observed.

In discharging their responsibilities for maintaining a secure, safe and trustable cyberspace, States must adopt a cooperative rather than confrontational approach.

As the General Assembly, in the 1965 “Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty” has reaffirmed, “No State has the right to intervene directly or indirectly for any reason whatever in the internal or external affairs of any other State". All States must therefore prevent and refrain from such acts, inter alia, against political, economic and cultural elements or cyberrelated critical infrastructure of States, including through cyberrelated ways and means.

Moreover, the Assembly, through the 1981 "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States" has reaffirmed the duty of a State "to ensure that its territory is not used in any manner which would violate the sovereignty, political independence, territorial integrity and national unity or disrupt the political, economic and social stability of another State"; "to refrain from any action or attempt in whatever form or under whatever pretext to destabilize or to undermine the stability of another State or of any of its institutions", as well as "to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States". These rules must also be observed by States with respect to cyberspace.

According to one of the principles reaffirmed by the General Assembly in the 1970 "Declaration on Principles of international law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations", States must not use any "type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind". Accordingly, States shall not use cyberspace-related advances as tools for economic, political or any other type of coercive measures, including by limiting or blocking measures against other States.

Likewise, States must refrain from the threat or use of force within or through the cyberspace environment. They must also refrain from, and prevent, abusing cyberspace-related supply chains developed under their control and jurisdiction, to create or assist development of vulnerability in products, services and maintenance compromising sovereignty and data protection of other States.

States must also exercise due control over cyberspace-related companies and platforms under their jurisdiction, and take appropriate measures to make them accountable for their behaviour in the ITC environment, including for violating national sovereignty, security and public order of other States. At any rate, States are responsible for their internationally wrongful acts within or through cyberspace.

Furthermore, all cyberspace-related international disputes must be settled exclusively by peaceful means and based on "the sovereign equality of States and in accordance with the principle of free choice of means" as stated in the 1970 "Manila Declaration on the Peaceful Settlement of International Disputes".

It is worth recalling in this context that, during the recent years, we have been witnessing an alarming trend of systematic accusations by certain States against other States of launching cyberattacks or similar activities in cyberspace. Given the existing challenges associated with attribution in the cyberspace environment as well as the absence of a set of internationally developed and agreed standards on genuine, reliable and adequate proof for substantiating the attribution, such accusations must be considered merely politically motivated.

All in all, cyberspace and its related means, technics and technologies must be used exclusively for peaceful purposes, and to that end, States must act cooperatively, responsibly and in full accordance with applicable international law.

Finally, we share the views that consideration of cyberspace-related issues must be continued in the General Assembly. For its part, the Islamic Republic of Iran, as one of the victims of cyberattacks, through the Stuxnet malicious computer worm – believed to be built jointly by the United States and the Israeli regime to cause damage to the Iranian peaceful nuclear installations – stands ready to contribute to Assembly's efforts in developing principles and norms required for cyberspace.

Annex XXXIX

Statement by the Permanent Mission of Italy to the United Nations

Italy commends Estonia for bringing the issue of cybersecurity to the attention of the Security Council and is pleased to participate in today's open debate.

We also appreciate the support and dedication of the High Representative for Disarmament Affairs, Ms. Nakamitsu, and her readiness to brief the Security Council at a moment when there is concern among Member States for the rising number of cybersecurity incidents.

Italy aligns itself with the European Union statement and wishes to add the following remarks in its national capacity.

The timing of this debate could not have been more appropriate. The General Assembly has recognized the work of the past two years carried out by the First Committee on developments in the field of information and communications technologies on international security and on the advancement of responsible State behaviour in cyberspace. The two reports adopted by the Open-ended Working Group and the Group of Governmental Experts during this semester represent important achievements that should contribute to building trust among Member States. The also gave visibility to a domain which for several years has been considered eminently technical.

The pace of digitalization is picking up at a global level and, along with the benefits associated with this development, comes the challenge to maintain cyberspace as a global, open, and stable domain. The surge in incidents in recent months, at times targeting critical infrastructures and imposing high costs to world economies, is deplorable. Some of the attacks offered a glimpse into the loss of human life that these actions can cause, especially during a pandemic. The destructive potential of the misuse of new technologies is becoming more and more evident and so is the need to keep them in check. Italy believes that the United Nations are the best positioned for this task and for promoting cyberpeace and stability.

Italy would like to echo the European Union statement with regard to the applicability of international law in cyberspace, including international humanitarian law and human rights law, the importance of adhering to norms of responsible State behaviour, and the usefulness of confidence-building measures as a practical means to prevent conflict. We also wish to highlight the important role that regional organizations can exert in the field of cybersecurity. As staunch supporters of multilateralism, we encourage the dialogue between the United Nations and regional organizations and, in this regard, we welcome the recent discussions between the United Nations Secretary General and the European Council, as a worthwhile opportunity to exchange views on the challenges we are facing. We also appreciate the efforts of the Swedish presidency of the Organization for Security and Cooperation in Europe, which is bringing to the fore the interlinkages between human rights, gender issues and cybersecurity.

In an increasingly interconnected world, dialogue becomes even more essential to promote shared understandings and increase opportunities for cooperation. In this spirit, we support the dialogue of the European Union with the United Nations and with regional organizations, notably the African Union, the Regional Forum of the Association of Southeast Asian Nations and the Office of the Special Adviser.

Through regional organizations, Member States can maximize their own bilateral contacts, sharing best practices and lessons learned, thus ensuring that regional approaches do not diverge. Further efforts should be dedicated to mechanisms for the peaceful settlement of disputes, as well as to initiatives to develop cyberdiplomacy and cybermediation.

We believe that the cyberdomain should stay open, free, secure and stable, as a means for States to implement policies that will enable societies to thrive and guarantee sustainable development for all, contributing to the attainment of the SDGs. The importance of capacity-building cannot be underestimated, as it guarantees homogeneous resilience of States, increases awareness and stimulates the development of capabilities. Much more needs to be done in this sector, and we believe that the programme of action to Advance Responsible State Behaviour in Cyberspace, promoted together with other 52 Member States, can represent the priority platform from which to coordinate and promote this endeavour. We have already flagged our availability to exchange further on this initiative in the context of the First Committee discussions and wish to reiterate our resolve today. The programme of action can also be the forum where the multi-stakeholder approach is shaped and Public-Private Partnerships are developed.

The pandemic has been a dramatic setback in 2020 and 2021. Our joint efforts need to focus on relaunching sustainable development and the cyberdomain is an essential ingredient for that. Italy is working toward this goal as a member of the G7 and is promoting this vision in the context of its current G20 presidency. Today's debate is a vital step toward increasing awareness and ensuring that developments linked to digitalization occur in a safe and stable cyberdomain, while safeguarding every effort from being undermined.

This debate takes place as the G20 Foreign Ministers are meeting in Matera to discuss the issues of recovery and sustainable development, with the aim of leaving no one behind. It is our hope that these efforts are mutually reinforcing and that the Security Council will remain focused on cyberissues, monitor progress and be ready to call non-compliant States to their obligations. Hopefully such instances will be very few as Member States converge on the need to dedicate time and effort to a positive cybersecurity agenda – one which develops trust, transparency and inclusiveness.

Annex XL

Statement by the Ambassador for United Nations Affairs and Cyber Policy of the Ministry of Foreign Affairs of Japan, Akahori Takeshi

Japan would like to express its sincere appreciation to Kaja Kallas, the Prime Minister of the Republic of Estonia, for organizing this open debate on cybersecurity. Japan thanks Estonia for recognizing in its concept note the open debate on complex contemporary challenges to international peace and security organized in 2017 under Japan's presidency.

Japan welcomes the adoption of the Open-ended Working Group report in March and the adoption of the report of the sixth Group of Governmental Experts in May, both by consensus.

The greatest value of the Open-ended Working Group report was that it was adopted by consensus in a process where all Member States could participate fully. The Member States affirmed the acquis directly, including that international law, in particular the Charter of the United Nations in its entirety, is applicable in cyberspace.

The Group of Governmental Experts report has additional value. For each of the 11 norms included in the 2015 Group of Governmental Experts report, the new report provides guidance and examples of implementation. Japan hopes that this content will further promote cooperation between States in advancing responsible State behaviour. In addition, it is clearer now that internationally wrongful acts attributable to a State entail State responsibility. The applicability of international humanitarian law is expressed in a clear manner. The Group noted again the inherent right of States to take measures recognized in the Charter.

We look forward to deepening concrete discussions on the application of international law in cyberspace in various fora in the future. Japan hopes that the position paper which it provided to the Group of Governmental Experts compendium of national positions will contribute to such discussions. Here, I would like to share the most essential points in Japan's position.

Japan takes the view that a State must not violate the sovereignty of another by cyberoperations. Moreover, a State must not intervene in matters within domestic jurisdiction of another State by cyberoperations. Internationally wrongful acts committed by a State in cyberspace entail State responsibility.

States have a due diligence obligation regarding cyberoperations under international law. Norms 13(c) and (f) and the second sentence of paragraph 71(g) of the 2021 Group of Governmental Experts report are related to this obligation. Regarding the recent Colonial Pipeline incident, the U.S. President mentioned efforts toward "sort of an international standard that governments knowing that criminal activities are happening from their territory move on those criminal enterprises". We recognize the difficulty of attributing cyberoperations to a State. The due diligence obligation may provide grounds for invoking the responsibility of the State from the territory of which a cyberoperation not attributable to any State originated.

Any international dispute involving cyberoperations must be settled through peaceful means pursuant to article 2(3) of the Charter of the United Nations. In order to ensure the peaceful settlement of disputes, the powers of the Security Council based on Chapters VI and VII of the Charter of the United Nations and the functions of the other United Nations organs should be used in disputes stemming from cyberoperations. Japan has reservations to the idea of establishing a new international mechanism for attribution.

Japan's view is that when a cyberoperation constitutes an armed attack under article 51 of the Charter of the United Nations, States may exercise the inherent right of individual or collective self-defense recognized under the same article.

International humanitarian law is applicable to cyberoperations. This affirmation contributes to the regulation of methods and means of warfare. The argument that the affirmation will lead to the militarization of cyberspace is groundless.

International human rights law is also applicable to cyberoperations. Individuals enjoy the same human rights with respect to cyberoperations that they otherwise enjoy.

On the relationship between international law and voluntary norms, for the stabilization of cyberspace, it is essential that international law and norms work together to prevent internationally wrongful acts using ICT and to promote responsible State behaviour in cyberspace. As clearly expressed in the Open-ended Working Group report, norms do not replace or alter States' obligations under international law.

Japan hopes that a large number of Member States will voluntarily publish their national positions on how international law applies.

Japan believes that it is time to prioritize implementation of the agreed voluntary norms and obligations under international law, together with confidence-building measures and capacity-building measures.

In the context of implementation, Japan would like to invite Governments to proactively announce their legal assessment when a malicious cyberoperation occurs, including, inter alia, on whether it constitutes a violation of international law. Such practice will promote shared understanding on how international law applies to cyberoperations. Application of international law by international and domestic courts and tribunals to cyberincidents would have similar effect. It is Japan's hope that malicious activities in cyberspace will be deterred by accumulating such practice.

Japan strongly supports the programme of action. We believe that the programme of action will be an effective mechanism to secure and monitor implementation of agreed norms, obligations under international law, confidence-building measures and capacity-building. We look forward to deepening discussions on the programme of action. We will also continue to participate proactively in the new Open-ended Working Group.

Japan is committed to safeguarding a free, fair and secure cyberspace and will continue to actively contribute to discussions and efforts to promote rule of law in cyberspace, including at the United Nations.

Annex XLI

Statement by Permanent Representative of Kazakhstan to the United Nations, Magzhan Ilyassov

We express our gratitude to the Estonian Chairmanship for organizing and conducting the debate entitled "Maintenance of international peace and security: cybersecurity".

In conditions of global threats, ensuring security requires the coordination of the international community and the settlement of many aspects of a political and economic nature. In this context, it should be noted that a new and at the same time complicated component has appeared in the world – cybersecurity.

It should be clear that information and communications technologies having enormous potential for the development of States. At the same time, they create new opportunities for perpetrators and may contribute to a rise in the levels and complexity of crime, the potential risk of the misuse of emerging technologies, including artificial intelligence. In this regard, the prevention and suppression of the use of information and communications technologies for criminal purposes should be a priority for the work of States at the present stage.

In this regard we welcome the established an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, foreseen by resolution 74/247 adopted by the General Assembly on 27 December 2019.

We believe that the work of the United Nations in this area will be further influenced by the final substantive report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security adopted in March 2021 and consensus by resolution 75/240, which established an Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, as well as by the consensus report adopted by the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of international security in May 2021.

States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to this sphere.

In this regard, we welcome cybersecurity negotiation process in the United Nations and understanding of the participants and Member States that all decisions on this specified agenda must be taken by consensus.

Annex XLII

Statement by the Permanent Mission of Latvia to the United Nations

Developments in information and communications technologies (ICT) have provided States and societies with myriad of benefits in the sphere of economy, services, education and communication. Alongside vastly positive effects of the application of ICT, Latvia is increasingly concerned about the implications of the malicious and disruptive use of ICT with the implications for both international peace, security, stability and human rights.

More often States suffer from such offenses, including those affecting democratic institutions and critical infrastructure. It is even more alarming that malicious cyberactivities are exploiting the coronavirus pandemic targeting medical care systems essential for maintaining human health, vaccine research as well as information space.

Broad participation and the very discussion displayed at the United Nations (UN) Security Council Arria-formula meeting last year confirmed the increasing relevance of the cybersecurity for the international peace and stability agenda. Therefore, it is only timely and appropriate to bring the issue of cybersecurity on the formal agenda of the Security Council. Latvia fully supports the efforts of Estonia to properly reflect upon mitigation of irresponsible behaviour in cyberspace on the international peace and security.

The United Nations must remain a significant global player to promote peace, security and stability, including in the cyberspace. Active work of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of international security and of the Open-ended Working Group on Developments in the Field of Information and Communications in the Context of International Security over the past years have laid substantial groundwork for the discussion of today.

The two consensus-based final reports of the Group of Governmental Experts and the Open-ended Working Group are welcome stepping stones for further work with a view to forging common understanding on broad range of issues.

In this regard, the programme of action on responsible use of ICT by States in the context of international security is a valuable outcome of Group of Governmental Experts and Open-ended Working Group reports. The cyberrelated programme of action should serve as a solid and, most importantly, action-oriented basis for further work to make tangible progress in the implementation of the norms of responsible behaviour.

In this context, Latvia would like to emphasize the multi-stakeholder nature of cyberspace, which requires the engagement in discussions of a range of non-State actors from the private sector, civil society and academia. Considering their commanding stakes in the ICT ecosystem those stakeholders can contribute significantly in many different ways, sharing their perspectives, knowledge and experience.

States should continue to work actively and be ready for in-depth discussions within future United Nations processes to advance responsible State behaviour in cyberspace in the context of international security. While we all have to work tirelessly to strengthen the protection and security of our own ICT, States should not permit another State or non-State actor to use ICT within its territory to commit internationally wrongful acts. We call on all States to refrain from conducting, enabling or tolerating such activities that are not in conformity with the international law, including the Charter of the United Nations, to avoid impeding security associated with the use of ICT. Responsibility, building trust and predictability must be the key elements of international cooperation in the field of cybersecurity.

In order to prevent misunderstandings and misperceptions on one hand and to establish practice of communication on ICT incidents on the other – we must establish open communication channels among Member States. The creation of a points-of-contact network at the policy and technical levels at the United Nations can make a meaningful contribution to a more effective communication on the global level. The network of points of contact has already proven to be effective on the regional level in the Organization for Security and Co-operation in Europe.

At last, Latvia would like to commend all Member States for demonstrating commitment to cooperate and work together in order to reach consensus on the reports in Group of Governmental Experts and Open-ended Working Group processes. This is the right path and excellent opportunity to further strengthen international cooperation towards a global, open, stable, peaceful and secure cyberspace where human rights, fundamental freedoms and the rule of law fully apply.

Annex XLIII

Statement by the Chargé d'affaires a.i. and Deputy Permanent Representative of Liechtenstein to the United Nations, Georg Sparber

Cyberoperations have served as the equalizer in modern warfare by providing new avenues for both offensive and defensive operations to all actors, including those with fewer resources. As a result, the frequency and severity of cyberoperations have intensified in recent years, threatening international peace and security. It is alarming that such attacks have the potential to cause grave suffering to the civilian population, including the loss of lives and the disruption of essential services. In this context, we recall that States increasingly agree that international law, specifically the Charter of the United Nations in its entirety and rules of customary international law derived from the Charter's principles, as well as the Rome Statute of the International Criminal Court and international humanitarian law, apply to cyberspace.

The Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security institutionalized discussions on international peace and security in the cybercontext within the United Nations. Furthermore, the final report released by the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Group of Governmental Experts) reaffirms the applicability and necessity of international law in cyberspace. Liechtenstein takes note of the combined contributions of the Open-ended Working Group and the Group of Governmental Experts in furthering the discussion on how international law, in particular the Charter of the United Nations, applies to cyberspace.

One of the landmark achievements of the Charter of the United Nations is the prohibition on the use of force. The use of force is prohibited except when authorized by the Security Council under Chapter VII or carried out in self-defence under article 51 of the Charter. However, article 51 is increasingly invoked as the legal basis for the use of force without necessary legal justifications. There is a substantive risk of this trend extending to cyberspace with the development of new technologies and State capabilities. We should ensure that cyberspace does not facilitate unjustified self-defense operations. And, we recall that invoking article 51 preemptively requires evidence of the imminence of an armed attack, and it always requires proof of necessity and the proportionality of measures taken in response.

The Charter of the United Nations foresees an enforcement role for the Security Council concerning the most serious violations of the relevant rules under international law that amount to acts of aggression. In addition to the tools contained in the Charter, the Council now also has the option of initiating individual criminal responsibility for perpetrators of the crime of aggression by referring relevant situations to the ICC. In this context, Liechtenstein believes that having a clear understanding of how the Rome Statute applies to cyberoperations will help to inform the work of the Council.

In an effort to elucidate the Rome Statute's application to cyberoperations, Liechtenstein, together with ten other ICC States Parties, created a Council of Advisers to explore the role of the ICC in the regulation of cyberwarfare. Composed of 16 eminent international lawyers, the Council of Advisers convened three times across 2019 and 2020 to discuss the extent to which the Rome Statute's core provisions apply to cyberoperations. A final report is scheduled to be presented this year. We are hopeful that this will contribute to shared understandings of accountability in the context of cyberoperations as well as deterring such crimes in the first place.

Liechtenstein underscores the need for a robust legal framework to regulate cyberspace for international peace and security. We are pleased to contribute to global efforts to combat malicious cyberoperations through our upcoming Rome Statute-focused report, and we will continue to strive for international peace and security with our unwavering commitment to international law.

Annex XLIV

Statement by the Permanent Mission of Malta to the United Nations

Malta thanks Estonia for organizing this timely debate on an issue which we believe should feature on the Security Council's agenda. Although cybersecurity issues have been alluded to in a number of Security Council debates, we believe that these issues should be given more prominence, considering that they represent one of the most important and constantly-evolving challenges to international peace and security.

Malta aligns itself with the statement delivered by the European Union and would like to highlight a few points in its national capacity. The evolution in cyberspace has brought with it a number of opportunities for Member States and citizens around the globe and has led to increased prosperity, connectivity and economic growth. However, the cyberdomain has also opened the door to malicious activities aimed at disrupting and exploiting vulnerabilities in societies and conduct attacks which can have considerable impact on Member States and its citizens, such as in terms of sensitive data and critical infrastructure. In fact, the more we shift towards the virtual and interconnected world, the more susceptible we are to these kind of malign activities.

Malta believes that the United Nations has a central role to play in the regulation of State behaviour in cyberspace, specifically because of the extensive body of international law that already exists. We are also very encouraged by the results achieved by the Group of Governmental Experts (Group of Governmental Experts) and the United Nations Open Ended Working Group (Open-ended Working Group) which have adopted consensus reports on *inter alia* advancing State behaviour in cyberspace. We need these processes to continue feeding in the United Nations system and elaborate on the application of international law in cyberspace, the importance of confidence-building measures and offering additional guidance and norms. We value the participation and contribution of Member States to these processes and we urge these discussions to move forward and keep up with the fast moving developments in this domain.

We have witnessed the devastating impact cyberattacks can have on sensitive data and infrastructure. It is vital that norms and regulations for the conduct of State behaviour in the cyberdomain are well outlined. This will lead to increased predictability and avoid any miscalculation when assessing cyberthreats. The malicious use of cyberspace has such a lasting impact that cooperation at the international level is also needed to avoid any potential conflicts which may arise.

Confidence-building measures between States through the application of good practices and established norms is a vital component moving forward. This will reduce any potential misunderstandings and enable better assessments of malicious behaviour.

The international community must also reach out to the myriad of other stakeholders on this file including civil society and the private sector to ensure a level playing field and an equitable set of rules. All the potential users of cyberspace need to recognize the role they play in increasing cyberresilience and in preventing the malicious use of the tools which are at our disposal.

Malta believes that the Security Council has an important role to play when it comes to new technologies which could have an impact on international peace and security. The Security Council must ensure that all the relevant actors in cyberspace respect international law and the established rules and guidelines with a view to avoid potential conflict arising from cyberattacks. We urge the Council to remain seized of this matter and to ensure that we foster together increased understanding and mutual trust.

Annex XLV

Statement by the Permanent Mission of Morocco to the United Nations

[Original: French]

First of all, the Kingdom of Morocco wishes to thank Estonia for organizing this first open debate of the Security Council on the relevant and timely question of the maintenance of international peace and security in cyberspace. Morocco welcomes the detailed statement by the Prime Minister of the Republic of Estonia, Ms. Kaja Kallas, as well as that country's excellent leadership on cyber matters and the security of cyberspace. Morocco also wishes to thank the High Representative for Disarmament Affairs, Ms. Izumi Nakamitsu, for her informative briefing on current challenges to the maintenance of international peace and security in cyberspace.

As a developing country with a high level of connectivity, the Kingdom of Morocco very quickly showed particular interest in the development of information and communications technologies (ITCs) and their advantages as engines of sustainable development. However, although we are unanimous in recognizing the benefits and advantages of progress in those technologies for the day-to-day well-being of humanity, we are beginning to become aware of the threats that can arise, from the simple circulation of "fake news" to actual attacks on peace and security, both at the national and international levels.

At a time when such terms as the Internet of things, the digital revolution or cyberwarfare are in common use, however, our ability to combat cyber threats remains much lower than our high level of dependence on these indispensable tools. On top of that, it is important to note that the current context marked by the COVID-19 pandemic has brought us even more into the cyber era, and at the same time exponentially and irreversibly increasing our exposure and vulnerability to cyberattacks and threats, including ones targeted at critical infrastructure.

Such malicious operations, beyond threatening State sovereignty, have the unfortunate potential of heightening the risk of conflicts in cyberspace, but also of causing considerable human and material damage. This is likely to undermine the structure of international peace and security and present cyberattacks as a major emerging threat.

"We are living in dangerous times", as the Secretary-General stated at the launch of his Agenda for Disarmament in 2018.

Indeed, now more than ever, the potential and real risks related to threats in cyberspace are confronting the international community and United Nations Member States. It is only through their efforts, both collectively and individually, to prevent malicious use of ICTs that we can guarantee that cyberspace will continue to serve as an engine for peace, security, stability and development.

In that regard, Morocco believes that the need to secure and protect cyberspace remains a shared responsibility of States as the leaders. Therefore Morocco, in accordance with Royal Directives, has undertaken immediately the following major actions at the legislative, organizational and preventive levels:

- The definition of a cybersecurity strategy centred around four strategic factors: evaluation of risks to information systems within administrations, public agencies and critically important infrastructure; protection and defense of these information systems; strengthening the foundations of security (legal framework, raising awareness, training and research and development); and the promotion and development of national, regional and international cooperation.

- Promulgation of Act No. 05-20 on cybersecurity on 25 July 2020, with the aim of establishing a legal framework requiring entities to have a basic minimum set of security measures and rules in order to ensure the reliability and resilience of their information systems. It also has the objective of the development of digital trust, the digitalization of the economy and, more generally, to assure the continuity of economic and social activity in Morocco in order to facilitate the development of a national cybersecurity ecosystem.

- The establishment, over the course of this decade, of several organizations aimed at ensuring state governance of cybersecurity, such as the Strategic Committee for Information System Security in 2011, the General Directorate of Information System Security, the Nation Agency for the Regulation of Telecommunications, the National Commission for the Monitoring and Protection of Personal Data, and the Moroccan Centre for Polytechnic Research and Innovation that conducts the national campaign to combat cybercrime.

On the eve of this open debate, on 28 June 2021, Morocco also approved a draft decree having to do with cybersecurity that set the rules applicable to information system security, as well as the African Union Convention on Cybersecurity and Personal Data.

However, in view of the global nature of cyber threats, major internationally agreed measures should be able to work in concert with regulations put into effect at the national level. Morocco has thus ratified the Council of Europe Convention on Cybercrime, also known as the Budapest Convention and in 2018 joined the Paris Call for Trust and Security in Cyberspace. Under United Nations auspices, it participates in the Open-Ended Working Group on development in information and telecommunications in the context of international security and the Group of Government Experts to promote responsible behaviour by States in cyberspace in the context of international security, the new Open-Ended Working Group on security of and in the use of information and communications technologies (2021–2025) and the elaboration of the forthcoming Programme of Action to promote responsible behaviour by States in cyberspace. Morocco is also a member of the Group of Friends on e-governance and cybersecurity of which Estonia is the excellent co-chair, along with Singapore.

In conclusion, the Kingdom of Morocco stresses that it is the shared responsibility of States to show proof of their common and firm will to protect cyberspace, mainly due to the fact that the facets of prevention and security of cyberspace are corollaries of the use of information and communications technologies.

The Security Council in particular is called on to play a key role, especially when cyberattacks constituting a direct threat to international peace and security occur, but also as a pioneer in the area of prevention.

Morocco reiterates its warm thanks to Estonia for organizing this necessary and timely open debate, as we need greater awareness and discussion on the question of the maintenance of international peace and security in cyberspace, and for having introduced this question on the agenda of the Security Council.

Annex XLVI

Statement by the Permanent Representative of the Netherlands to the United Nations, Yoka Brandt

The Kingdom of the Netherlands would like to thank Estonia and Prime Minister Kallas for organizing this open debate on maintaining international peace and security in cyberspace.

A timely meeting – seen the steep rise in cyberattacks, by State and non-State actors alike. These malicious cyberactivities can lead to potentially vast disruption in our societies, through relatively limited resources. With the result of destabilizing international relations.

Therefore, the time is now, to work together in securing an open, free and secure cyberspace by advancing responsible State behaviour, call out irresponsible behaviour and impose consequences.

While acknowledging that there are many other relevant angles in this issue, the Netherlands will limit itself to three specific elements that remain imperative to increasing stability in cyberspace:

- Adherence to the acquis
- Attribution
- Capacity-building

Adherence to the acquis

Over the years, cyberoperations against critical and civil infrastructure have shown to be a real and credible threat. Even more so over the past year where we have witnessed cyberattacks evolving in scope, scale, severity and sophistication.. As societies, we have increasingly shifted almost all aspects of our life to a digital world and must realize that it is the Internet that facilitates these connections throughout the world. It should therefor come as no surprise that the harmful effects of malicious cyberoperations against critical infrastructure, governments or societies, will be felt immediately and widely. Posing a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals.

With the recent consensus reached on the reports of both the Open-ended working group on Developments in the Field of information and communications technologies in the Context of International Security and United Nations Group of Governmental Expert to advance responsible State behaviour in cyberspace (Group of Governmental Experts), States are now equipped with a framework of responsible State behaviour in cyberspace. Allowing States to have a better understanding of the applicability of international law and the agreed 11 voluntary non-binding norms. The Netherlands recalls that existing international law, in particular the Charter of the United Nations is applicable to cyberspace and essential to maintaining peace and stability and to promoting a free, open and secure cyberspace including respect for human rights and fundamental freedoms in cyberspace.

States agreed that malicious cyberoperations against infrastructure and information infrastructure supporting essential services to the public infrastructures are off-limits, confirm Group of Governmental Experts norm 13(f). It is each State’s prerogative to determine which infrastructures it designates as critical may include: medical facilities, financial services, energy, water, transportation and sanitation. The Netherlands has consistently focused on three (non-exhaustive) infrastructures:

1. The technical infrastructure essential to the general availability or integrity of the Internet;

The technical infrastructure essential to elections;

The health-care sector.

In that vein, we encourage States to publicly define and share what they consider to be critical infrastructure by issuing national declaratory statements, detailing Member States positions' on the adherence to the framework for responsible State behaviour. This is the only way, we can increase transparency, develop common understanding, create predictability and build confidence. Continuing efforts on the implementation of the agreed framework are needed to reduce the risk of escalation as well as adherence to the acquis by all States.

Attribution

We all seem to agree on the rules and norms in cyberspace. Yet, we continue to witness an increase in cyberthreats. The Netherlands is appalled by the abuse of the coronavirus disease (COVID-19) pandemic for malicious cyberoperations against critical infrastructure; the health sector, technical infrastructure essential to the general availability or integrity of the Internet as well as the technical infrastructure for elections.

Let us be clear – we will work together on a voluntary basis to hold States accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behaviour in cyberspace.

Capacity-building

Digital resilience is key to manage cyberrisks and mitigate their impact. However, different levels of capacity of cybersecurity among different States amplify the vulnerability of our interconnected world. Therefore, it is in our common interest to engage in targeted capacity-building efforts to ensure that all responsible States can implement this framework and better protect their networks from significant disruptive, destructive, or otherwise destabilizing cyberactivity. Moreover, effective cybercapacity-building requires cooperation between both State and non-State actors. In that light, the Netherlands established the Global Forum on Cyber Expertise, which has matured into a strong public-private capacity-building platform that harnesses and consolidates the more than 700 existing cybercapacity-building efforts providing assistance in building technical resilience, help in drafting legislation that ensures safety, security, and respect for human rights.

We commend Estonia for laying the groundwork for future cyberdiscussions in the Security Council and welcome today's first official debate on cybersecurity.

Annex XLVII

Statement by the Permanent Mission of New Zealand to the United Nations

New Zealand would like to note our appreciation to Estonia for bringing the important issue of maintaining international peace and security in cyberspace to the Security Council agenda.

Cyber threats are a pressing and pervasive issue for all Member States. Cyber threats pose significant risks to New Zealand's prosperity and security, as well as to international peace and security.

We must work together to build a stable and secure online environment in order for us all to enjoy the benefits of digital connectivity, which is an important enabler for economic, social, and cultural development.

We value the opportunity to share New Zealand's perspectives on the international efforts to maintain peace and security in cyberspace. To that end we reiterate the critical importance of the agreed framework of responsible State behaviour online:

- We must abide by our obligations under existing international law, which we have all agreed applies online as it does offline;
- We must implement the norms of responsible State behaviour online, which we have each endorsed through General Assembly resolution 70/237;
- We must ensure that Confidence-Building Measures are widely adopted and utilized; and
- We must redouble our capacity-building efforts to ensure we are all cyberresilient.

This framework provides what we need to encourage responsible behaviour online, but it needs to be lived if it is to be effective. We need to continue to implement the framework in practical, meaningful and concrete ways. New Zealand is committed to continuing to work with you all to this end.

International law

As a small State, New Zealand is a steadfast supporter of the international rules-based order. This is especially true with respect to trans-boundary threats. Our geographical isolation does not protect us from cyberthreats.

Ensuring that this system promotes an open, secure, stable, accessible and peaceful online environment and encourages responsible State behaviour in cyberspace is a key New Zealand priority.

Reaching consensus on precisely how international law applies online is a crucial contribution towards the maintenance of peace and stability. We are all in agreement that international law applies online as it does offline. Applicable international law includes: the Charter of the United Nations; the law of State responsibility; international humanitarian law; and international human rights law.

But we acknowledge that there remain some differences on these matters. To support understanding of *how* international law applies online, in December 2020, New Zealand released a national position statement. We encourage other Member States to share their national perspectives in order to develop and enhance our common understanding on these issues.

Norms of responsible State behaviour

New Zealand is committed to preventing, detecting, deterring and responding to malicious cyberactivity, and to upholding the norms of responsible State behaviour as endorsed in the 2021 United Nations Open-ended Working Group report. The norms we have all committed to are a central component of stability and security in cyberspace. We need to continue to be held accountable – and hold others to account – to the commitments we have made.

Among other things, we must promote cooperation between States, protect critical infrastructure, safeguard global supply chains, provide assistance when required, respect human rights and privacy, and prevent the malicious use of digital technologies on States' national territories.

We continue to reflect on the way in which the coronavirus disease (COVID-19) pandemic has underscored the importance of a safe and secure cyberspace. We have seen reports internationally of a range of different malicious activity online, from both State and non-State actors. This activity has targeted, among others, critical health-care infrastructure; officials working on the response; and members of the public. This is unacceptable and highlights that threats in cyberspace put lives at risk. New Zealand, along with a number of other States, has publicly condemned malicious cyberactivity undermining the response to the pandemic.

Confidence-building measures

We remain committed to constructive, practical and concrete outcomes to improve international and regional cybersecurity. Confidence-building measures provide an important avenue to achieve this, and we welcome practical initiatives that support mutual understanding, transparency, predictability, and stability in cyberspace.

For New Zealand, the Regional Forum of the Association of Southeast Asian Nations (ASEAN) is a key forum for regional cybersecurity discussions. We appreciate the cooperation we have with members within that forum and look forward to continuing to work with you all in the years ahead. New Zealand welcomes the opportunity to share lessons learned within and across regions to improve transparency, understanding and confidence among regional partners in cyberspace.

Capacity-building

New Zealand wants to help ensure that all States can lower the risks associated with increased connectivity, while still benefiting from it. That includes supporting broader and deeper understanding of and adherence to the framework of responsible State behaviour in cyberspace.

To achieve this, we need to ensure all of us have the tools and capacity needed to participate meaningfully in ongoing discussions and areas of debate, and to implement initiatives domestically and regionally that support stability internationally.

New Zealand remains committed to building regional cybersecurity capacity, with a particular focus on working with our Pacific and South-East Asian neighbours. We continue to deliver initiatives under New Zealand's NZ$10 million Cyber Security Support to the Pacific programme, and to support the ASEAN-Singapore Cybersecurity Centre of Excellence.

Conclusion

We have much work ahead but we are not starting from scratch. We once again welcome the outcomes of both the recent UN Group of Governmental Experts and the Open-ended Working Group processes. These processes, and the resulting reports, are significant complementary and mutually reinforcing achievements. We must continue building on the foundation created by this – and other – consensus agreements endorsed by the General Assembly.

It is important that that discussions involve a diverse range of views, including those from small States, and from non-governmental stakeholders. The breadth of interest in cybersecurity from Member States has heartened us – peace and security in cyberspace do affect us all – and it is encouraging to see such a wide range of States genuinely engaged in efforts to address these challenges. New Zealand stands ready to engage with you all on this challenge.

Annex XLVIII

Statement by Permanent Representative of Pakistan to the United Nations

I would like to express my deep appreciation and sincere thanks to the Permanent Mission of the Republic of Estonia for convening this important and timely open debate of the Security Council on the theme “Maintaining international peace and security in cyberspace”.

Information and communications technologies (ICT) provide vast opportunities and continue to grow in importance for the international community. At the same time, the complexity of the issues inherent in the use of ICT poses serious risks for international peace and security.

The hostile use of cybertechnologies is fast approaching the stage where it can constitute a breach of peace or a threat to international peace and security.

Misuse and un-regulated use of ICT could lead to serious implications for international peace and security in the event of a cyberattack launched on critical infrastructure. Recent incidents of suspected cyberattacks are illustrative.

There is a need to address the growing prospect of cybersecurity on urgent basis as part of broader United Nations efforts to prevent conflicts.

In this regard, the adoption of consensus report by the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security in March this year was of historic significance in supporting the global efforts towards the common goal of creating a safe, secure, stable and peaceful ICT environment.

It was also a strong reaffirmation of the international community’s ability to come together to address key global challenges in the most difficult circumstances, such as the pandemic.

While we understand that the report did not address the concerns of all Member States, we consider it important to consolidate the progress that has been achieved thus far and to maintain the momentum for continuing this inclusive and transparent process.

Pakistan remained positively and constructively engaged in the work of the Open-ended Working Group and welcomes the establishment of the new Open-ended Working Group on Security of and in the use of information and Communication technologies (2021–2025) established pursuant to the General Assembly resolution 75/240.

It (the new Open-ended Working Group) provides extremely useful forums for achieving meaningful progress, building on the previous recommendations in order to strengthen rules for responsible behaviour in cyberspace and to achieve meaningful international cooperation to minimize threats posed on international security by the malicious uses of ICT.

The 2015 Group of Governmental Experts and the recent report of Open-ended Working Group agreed on a set of important findings that contributed to generating a broad consensus among Member States that international law, and in particular the Charter of the United Nations is applicable and essential to maintain peace and stability in the ICT environment.

The Charter of the United Nations is unequivocal in its categorical upholding the principles of sovereignty, territorial integrity and non-interference in internal affairs of other States. These principles should serve as guiding star as we navigate the complexities of cybergovernance.

At the same time, the extent, scope and nature of the applicability of international law and its interpretation in the conduct of States and their use of ICT require careful consideration.

A simple assertion of the applicability of existing international law to cyberspace is not sufficient in addressing the multifaceted legal challenges arising from the ICT. It needs to be adapted according to the unique characteristic of the cybersphere.

Pakistan recognizes the importance of developing a legally binding international instrument, specifically tailored the unique attributes of ICT, to provide a regulatory course that seeks to create stability and safety in cyberspace. Such legal framework should address the concerns and interests of all States, be based on consensus, and pursued within the United Nations with equal participation of all States.

Voluntary, non-binding norms of responsible State use of ICT can contribute to reducing risks to international peace and security. However, given the unprecedented threats in ICT environment and the rapid pace of technological developments, there is a need to strengthen international efforts to develop binding rules that can help in maintaining peace and stability and promote open, secure, stable accessible and peaceful ICT environment.

We should ensure that cyberspace is not misused to perpetuate State sponsored disinformation campaigns, incitement to violence, hate speech and other related form of intolerance, including Islamophobia.

The United Nations has a central role in promoting dialogue and international cooperation among Member States to develop common understanding on key aspects, including, on the application of international law and norms, rules and principles for responsible State behaviour, promoting confidence-building and transparency measures and supporting capacity-building and the dissemination of best practices.

With a population of over 200 million people, and a flourishing digital landscape marked by growing number of online users, Pakistan attaches immense importance to leveraging digital technologies for enabling socio-economic development and facilitating more effective and efficient governance and public service delivery.

Pakistan is committed to promoting international cooperation in ICT and cybersecurity as a means of bridging the digital divide. All countries are equal stakeholders in the development of rules governing digital economy and security of cyberspace and ICT.

Annex XLIX

Statement by the Permanent Mission of Peru to the United Nations

[Original: Spanish]

Peru welcomes the initiative by the Estonian Presidency to convene this high-level open debate of the Security Council on a matter of growing and primary importance for the maintenance of international peace and security. We also welcome the briefings by the other speakers.

We are aware of the relevance of the use of information and communications technologies (ITC) in the context of international security, their rapid evolution and the benefits they generate. The health crisis stemming from the coronavirus disease (COVID-19) pandemic has highlighted our dependence on them, the urgency of reducing the digital divide and the importance of protecting critical infrastructure.

In the same way, we are also aware of the dangers that can arise from the malicious use of ITC, thereby increasing the risk of conflict in cyberspace. Their malicious use by terrorist groups, criminal organizations, armed groups and other agents constitutes a grave and systematic threat to international peace and security.

Considering that the threats do not arise from the technologies themselves, but from the use that is made of them, we must deepen our understanding of their appropriate use and how to avoid deliberate malicious uses, by promoting open, free, stable and secure cyberspace.

To that end, we recognize the primacy of the Charter of the United Nations as a firm basis for security, and we support the application of international law and international humanitarian law in cyberspace. Furthermore, we believe that it is of primary importance that international norms in this area be developed through the establishment of legally binding obligations.

We appreciate the notable efforts and progress made in the United Nations for the formulation of elements to promote the application of international law and the implementation of norms for responsible behaviour of States in cyberspace in the context of international security. We commend the substantive reports adopted by the Open-ended Working Group and the Group of Governmental Experts, and we hope that by harmonizing the work of both processes we will be able to have a single coherent statement and course of action on cybersecurity.

In addition to international efforts, we believe that regional and national actions are essential, in particular in the promotion of confidence building measures, capacity building, exchange of information and sharing of best practices to guarantee cybersecurity. For countries with lower technological development, to us it seems essential that they specify understandings and agreements that avoid making cyberspace into an arena for conflict because of the potential effects resulting from their lack of capacity to avoid it.

Taking into account the interconnected and complex nature of cyberspace, continual innovations in information and communications technologies and the growing incorporation of emerging technologies, we support the participation of the private sector, in particular the information industry, civil society and academia, in confronting those challenges. We are convinced that their contributions will continue to enrich the multilateral deliberations on the matter.

We will conclude by underlining the need for coordinated work by the international community as a whole and the adoption of new actions to study existing threats and possible cooperation measures to address them. The role of the Security

Council in the prevention of conflict and promotion of peace and security will be essential in order to guarantee cyberspace that is open, peaceful, secure and beneficial, and that promotes sustainable development and well-being of peoples.

Annex L

Statement by the Permanent Mission of Poland to the United Nations

The first ever open debate in the Security Council on cybersecurity constitutes an important landmark of our perception of contemporary challenges to international peace and security.

We thank and commend the Estonian Chairmanship for enabling us to address cybersecurity issues at this very timely moment.

In 2019, during our membership, Poland has drawn attention of the Security Council to the problems of cyberincidents in the Middle East.

Now, it is the time to raise awareness of the international community as a whole of steadily raising malicious activities in cyberspace. For two decades, in parallel with unprecedented development of digital technologies, we have been observing all over the world more and more sophisticated cyberattacks and cyberincidents. Poland is experiencing them on a daily basis.

They are of course of a different nature. Some have purely criminal background, others are motivated by economic goals and – more and more often – political ones. However, there is one common denominator of these activities – all of them are illegal. Malicious cyberactivities cannot be, in no way, justified or defended.

As you, Madam Chair, rightly pointed out in your concept note: “Existing international law, in particular the Charter of the United Nations, provides sufficient guidance for States on conducting cyberactivities”. It is a great task of the international community to work out commonly acceptable paradigm of activities in cyberspace.

Poland strongly supports achievements of the Groups of Governmental Experts (Group of Governmental Experts) and actively participated in the work of the Open-ended Working Group, which in its report, has reaffirmed the application of international law in cyberspace. We hope that the 2nd Open-ended Working Group will contribute to better common understanding of the importance of peaceful use of cyberspace. We also attach a great importance to the work of Ad Hoc Committee within the Third Committee of General Assembly.

Apart from the common assessment of the situation even more important is common and well-orchestrated action. Poland, therefore, supports broad participation of multi-stakeholders, NGOs, private sectors and academia in international debate on cybersecurity.

We also strongly believe that the crucial work should be conducted within regions. With engagement of regional organizations, individual States and representatives of civil society, we can develop useful instruments for capacity-building or confidence-building measures.

In order to stimulate international efforts both on the global and regional levels we need to pool our resources and diplomatic energy. This is why we firmly support and promote the establishment of the programme of action as an ultimate format of international cooperation on cyberspace activities.

With this open debate, we hope that cybersecurity will take up its permanent place on the Security Council agenda. The political and economic costs of malicious activities in cyberspace are too high to be overlooked by this important United Nations body.

Please be assured that Poland will spare no efforts to contribute to all global and regional processes, which will lead to strengthening the cyberorder on the basis of respect for international law and commonly agreed norms.

Annex LI

Statement by the Permanent Mission of Qatar to the United Nations

[Original: Arabic]

Allow me to thank the High Representative for Disarmament Affairs, Izumi Nakamitsu, for her briefing. The work of the Office for Disarmament Affairs helps to give cybersecurity its rightful place on the United Nations disarmament agenda.

Every day we see the transformative impact of the world's heavy reliance on cyberspace. However, digital technologies and global connectivity also facilitate misuse of cyberspace, which is particularly worrying given the reliance of vital public infrastructure and services on the digital sphere. Misuse of cyberspace and information and communications technology (ICT) by governmental and non-governmental actors poses a threat to national security and affects regional and international peace and security and international relations. In addition, terrorist groups are using emerging digital technologies to enhance their capabilities to commit crimes.

Clearly, no country is immune from the threat of the misuse of cyberspace. Collective action is therefore necessary to meet this global challenge. Fortunately, cyberspace itself could provide an excellent tool for coordinating such efforts. As we have seen over the past year, digital platforms have proven an indispensable means of continuing the work of United Nations bodies and other forums for international cooperation.

We must assess potential threats and the impact of cyberpiracy and misuse of cyberspace on peace and security. Collective efforts are needed to strengthen the regional and international security environment in the face of such threats and to promote the peaceful use of cyberspace and the relevant advanced digital technologies.

In that regard, due consideration must be given to the application of international law to the use of ICT by States and to promoting responsible conduct relating to States' electronic space in the context of international security.

At the same time, the free flow of information and respect for human rights and fundamental freedoms must be maintained in an open and secure digital environment accessible to all.

In addition to international frameworks, national strategies are important for guiding action and coordination among relevant stakeholders. That includes the private sector, which plays a pivotal role in digital technology.

Protecting information security and information infrastructure is one of the priorities of Qatar. It is taking comprehensive measures and developing its resources in this regard, with a focus on promoting international cooperation and capacity-building.

Information security and cybersecurity have been on the United Nations agenda for several years. However, steps must be taken to keep pace with rapid developments in this area. We therefore welcome the attention devoted to this issue by the Secretary-General, who has made promoting a peaceful ICT environment one of his main priorities. We are also pleased to see that consensus has again been reached again within the Group of Government Experts. We also look forward to the next session of the open-ended working group, with a view to contributing to expanding the international consensus in this regard.

In closing, I should like to reiterate that the State of Qatar will continue to strive at all levels to contribute to global efforts to promote peace, security and stability in cyberspace.

Annex LII

Statement by the Permanent Representative of the Republic of Korea to the United Nations, Cho Hyun

I would like to first thank you for convening today’s timely open debate on “Maintaining international peace and security in cyberspace”. My appreciation also goes to the High Representative for Disarmament Affairs, Ms. Nakamitsu, for her in-depth briefing.

Over the past couple of decades, the human race has witnessed technological advancement in the field of digital technology like never before. The concept of cyberspace, which was once only in the imagination of science fiction, has since become an everyday reality to us all; with the virtual and physical space surrounding us being integrated into one ecosystem. And, as much as this advancement has brought us unprecedented economic and social benefits, we have also become ever more vulnerable against malicious cyberactivities. Over the past year, in the midst of the global pandemic, our lives have become even more susceptible to cyberthreats as more people have been online. At the same time, the increasing number of cyberattacks against critical infrastructure, including medical infrastructure and facilities around the world, is increasingly concerning.

Against this backdrop, I would like to highlight the following four points that are of particular importance to my delegation.

First, the Republic of Korea supports the United Nations’ central role in ongoing discussions on how to address the challenges at hand and advance responsible State behaviour in cyberspace. In this regard, my delegation welcomes the adoption of the consensus report earlier this year of the United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, as well as the fourth consensus report of the Groups of Governmental Experts (Group of Governmental Experts) which was adopted last month. These achievements reflect the progress that has been made in the cumulative and evolving framework for responsible State behaviour in their use of ICT, and, through these exercises, has enhanced the understanding of the international community as a whole in this critical area.

As all Member States agreed by consensus in the previous Open-ended Working Group report, international law applies to State use of ICT, and States should be guided by the framework for responsible State behaviour in the use of ICT, as outlined in the Group of Governmental Experts reports. The primacy of international law and the rules-based order must be equally applied to cyberspace in order to ensure peace and security.

Second, my delegation highly appreciates the recent Group of Governmental Experts consensus report presenting an additional layer of understanding on the norms of responsible State behaviour, confidence-building measures, capacity-building, and how international law applies to the use of ICT by States. The report reaffirmed the applicability of international law including the Charter of the United Nations, and notably, international humanitarian law in situations of armed conflict. We also strongly support the recommendation of the Group of Governmental Experts that States party to any international dispute, including those involving the use of ICT, shall first seek a solution by peaceful means, as described in article 33 of the Charter of the United Nations.

Specifically, my delegation is happy to see the report further elaborating on the norm that States should not knowingly allow their territory to be used for internationally wrongful acts with the use of ICT. This principle of “due diligence”, which was suggested by the ROK and first reflected in the 2015 Group of Governmental Experts report, points out that each State should take appropriate and reasonable steps to address the situation if it is aware of or if notified of an internationally wrongful act.

Third, we must further elevate our efforts towards building confidence and promoting common understanding. The Republic of Korea, as a responsible Member State and a leading nation in the digital and technological sector, has been actively participating in and contributing to various regional and multilateral fora. Just last week on June 22nd, the ROK, in close cooperation with the Organization for Security and Cooperation in Europe, successfully hosted "The Third Inter-Regional Conferences on Cyber/ICT Security" to discuss current trends in cybersecurity and promote cybersecurity cooperation between regional organizations. We also hosted the 19th ROK-United Nations Joint Conference on Disarmament and Non-proliferation focusing on the development and impact of emerging technologies in 2020, and will be co-chairing the ARF Inter-sessional Meeting on ICT security for 2021–23. Moreover, this coming November, the ROK will launch an international forum to further invigorate discussions to address emerging security threats including cyberattacks and malicious use of emerging technologies in the context of international peace and security. Under the principles of inclusivity, transparency, and openness, the Forum will provide a welcoming international platform that is accessible to various stakeholders.

Fourth, we cannot emphasize enough that cybersecurity requires a multi-stakeholder approach, as international security dimension of cyberspace cuts across multiple domains and disciplines. While governments remain at the centre, we can only be truly effective when we involve other key stakeholders such as the private sector, academia, civil society, and the technical community in the process. We should also keep in mind that engagement with other stakeholders can contribute significantly to promoting common understandings and implementation of the framework of responsible behaviours in cyberspace.

In closing, I would like to take this opportunity to reaffirm the Republic of Korea's commitment to working with the United Nations and all Member States in further promoting an open, secure, stable, accessible, and peaceful cyberspace.

Annex LIII

Statement by the Permanent Mission of Romania to the United Nations

1. We commend Estonia for its initiative of organizing the first open debate on cybersecurity as a formal specific issue on the agenda of the Security Council. This represents a timely initiative to further enhance the rule-based international order, as well as our multilateral cooperation on a subject of utmost importance for the maintenance of international peace and security.

2. Today's debate reinforces the remarkable progress made by Member States within the last UNGGE and Open-ended Working Group consensus reports in consolidating the normative framework for responsible State behaviour in cyberspace – premised on existing international law, norms, confidence-building measures and capacity-building.

3. In an international security environment that is constantly evolving, information and telecommunications technologies (ICT) present both outstanding benefits as well as some of today's most prominent and acute threats. Such threats originate from both State and non-State actors, and target a variety of key sectors, such as energy, transport, finance and health, which rely on both physical and digital key infrastructures for providing services domestically, regionally or globally. Digital technologies can also be misused to attempt to weaken our democratic institutions and erode public trust in democratic principles. In addition, they can be used to exploit systemic vulnerabilities for geopolitical purposes. The coronavirus disease (COVID-19) pandemic stands as a dire recent example of the destructive impact of cyberoperations aiming to compromise or alter strategic information on vaccine research and distribution.

4. In this environment, the value of multilateral cooperation between responsible States cannot be overestimated, nor can that of strengthened partnerships between public administration, the private sector, civil society and academia. We need to work together to share reliable, accurate, timely and trustworthy information on threats and credible responses, and to coordinate our efforts and strengthen relevant preventive mechanisms at the global, regional and national levels. Most importantly, we need to concentrate our efforts towards developing the resilience of our societies to the impact of threats to our critical infrastructures – whether they are physical, digital or institutional.

5. With this in mind, it is worth noting that within its current presidency of the Community of Democracies, Romania actively promotes the link between technology and democratic processes as one of its main priorities; as the host of the newly created European Cybersecurity Industrial, Technology and Research Competence Centre in Bucharest, Romania welcomes and actively promotes the planned co-managed partnership investments between European Union member States and industry; as the initiator and host of the newly-established Euro-Atlantic Centre for Resilience, Romania will work for generating new ideas and strategies for adaptation of societies to new challenges to peace, security and democratic stability.

6. As an European Union member State, Romania is working for promoting and implementing the main dimensions of the new European Union Cybersecurity Strategy for the Digital Decade, especially the Cyber Diplomacy Toolbox, including European Union Cyber Deterrence and Strategic Communication tools against malicious cyberactivities. The European Union Cyber Diplomacy Toolbox has an important role to prevent, deter and respond to cyberincidents that affect the security of European Union and Member States.

7. Romania approaches cybersecurity as a key dimension of national security, undertaking efforts to ensure the development and adaptation of a proper national legal framework in order to facilitate cooperation and the efficient exchange of information between competent authorities, and meet its international obligations. Responsible State behaviour involves key positive obligations: of having in place modern and effective national legislation, cyberstrategies and institutions, of promoting and participating in substantial international cooperation, and, very importantly, of transparency, upholding agreed norms, promoting democratic principles and fully respecting human dignity.

8. The security of cyberspace represents for Romania one of its highest political and diplomatic priorities, pursued through advancing responsible State behaviour and consolidating preventive and normative mechanisms at global, regional and national level. We are committed to supporting a global, open, safe and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply. We are also of the view that an open, secure, stable, accessible and peaceful online environment cannot be imagined outside an international rules-based system, primarily founded on international law.

9. Romania was actively involved in both United Nations processes aiming to consolidate the cybersecurity framework (UNGGE and Open-ended Working Group), which successfully concluded their work through agreeing on important recommendations for preventing conflict in cyberspace (from consolidating understanding on the application of international law in cyberspace, to non-binding voluntary norms for responsible State behaviour, as well as to proposals for a future institutionalized dialogue).

10. Going forward, Romania is of the view that establishing a United Nations programme of action for advancing responsible State behaviour in cyberspace would foster the adoption of concrete practical measures for capacity and confidence-building, as well as facilitate access to financing sources, in an open, inclusive and transparent, permanent manner, thus assisting all Member States in their efforts to prevent conflict, develop common perceptions of threats and increase their cyberresilience.

11. Within all future United Nations processes, Romania will actively promote its position that international law applies to cyberspace. It is our firm conviction that there is no reason to consider that the existing international law could not appropriately govern inter-States relations carried out in cyberspace/ or through the medium of cyberspace. This includes international humanitarian law in the context of cyberoperations carried out as part of an armed conflict (whether international or non-international). In such circumstances, the planning of and carrying on of cyberoperations must be done in conformity with the principles governing the conduct of hostilities, namely distinction, proportionality, necessity and precaution.

12. Nevertheless, increased dialogue and exchanges among States can help clarify some of the specific circumstances of the applicability of the international law to cyberspace. With this in mind, we note that Romania’s preliminary view on this topic has been issued for the purpose of contributing to the work of the Group of Governmental Experts pursuant to General Assembly resolution 73/266.

Annex LIV

Statement by the Permanent Mission of Senegal to the United Nations

[Original: French]

First, I would like to thank Ms. Kaja Kallas, Prime Minister of the Republic of Estonia for presiding over this important high-level virtual public debate on cybersecurity, a subject of increasing importance within the United Nations system given the growing security threats noted in cyberspace. I also wish to thank the High Representative for Disarmament Affairs, Ms. Izumi Nakamitsu, whose briefing my delegation followed with great interest.

The fact is clear: the proliferation of malicious acts in cyberspace represents a real threat to international peace and security which calls for the Security Council to act. The debate that brings us together today shows that the Council is aware of this threat and is part of the ongoing and unfailing efforts on cybersecurity for over a decade by the General Assembly.

In this spirit, the various deliberations conducted by the four Groups of Governmental Experts and the Open-ended Working Group, respectively, on responsible behaviour by States in cyberspace and development in information and telecommunications in the context of international security, are positive and represent a clear signal of the will of States to find consensus on the modalities for regulation of cyberspace.

In recognizing the applicability of several principles and norms of existing international law and declaring State responsibility for internationally illicit acts they might commit in cyberspace, the conclusions of the reports of the Open-Ended Working Group and the latest Group of Governmental Experts, in March and May 2021, represent an additional contribution to the understanding of the exercise of international law in cyberspace.

Furthermore, like several countries, Senegal believes that confidence-building measures and transparency are essential to promote responsible behaviour by States in cyberspace, and should thus be strengthened.

Indeed, through regularly exchanging information on their cyber activities, States can help to avoid errors in perception and misunderstandings, to prevent and manage crises born out of the use of cyberspace, and as the case may be, lay the foundation for fruitful cooperation on digital matters.

Nevertheless, because of the huge changes in the sector and the emergence of new cyberthreats, Senegal believes that the rules of positive international law and confidence-building measures and transparency will not be enough in themselves to regulate cyberspace appropriately. They should be complemented by a binding international legal instrument.

Thus, a general approach joining voluntary confidence-building and transparency measures with a binding international convention would become necessary, not only to establish the rules of cyberspace, but also to take into account the positions and interests of all Member States. The deliberations of the new Open-ended Working Group on the security and use of information and communications technologies should tend toward that approach during the 2021–2025 period.

For its part, the Government of Senegal is firmly committed to making a positive contribution to the work in this area, which remains one of its priorities since the November 2017 adoption of the National Cybersecurity Strategy. This document, with the vision of instituting in Senegal in 2022 a cyberspace that is trustworthy, secure and resilient for all, contains an evaluation of the strategic context of cybersecurity in Senegal, taking into account current and future threats. It defines five strategic objectives: strengthening the legal and institutional framework of cybersecurity; protection of critical information infrastructure and State information systems; promotion of a culture of cybersecurity; building capacity and technical knowledge of cybersecurity in all sectors; and participation in regional and international cybersecurity efforts.

In accordance with the last objective, Senegal was the first country to become party to the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention). It also joined the Council of Europe Convention on Cybercrime (Budapest Convention) and Council of Europe Convention No. 108 for the protection of individuals with regard to automatic processing of personal data (STE no. 108) as well as its Additional Protocol regarding supervisory authorities and transborder data flows (STE No. 181). In addition, it adopted the Economic Community of West African States (ECOWAS) Directive of 19 August 2011 on fighting cybercrime and endorsed the Paris Call for Trust and Security in Cyberspace of 12 November 2018 and the Christchurch Call of 15 May 2019 to eliminate terrorist and violent extremist online content.

Domestically, the country has established a legal framework for digital regulation and utilization. In addition to Act No. 2008-08 of 25 January 2008 on electronic transactions, we can mention Guidance Act No. 2008-10 of 25 January 2008 on the information society, Acts Nos. 2008-11 and 2008-12 of 25 January 2008 on cybercrime and on protection of personal data, and Act No. 2018-28 of 28 November 2018 on a code of electronic communications. Along the same lines, the Code of Criminal Procedure was revised to take into account procedure in the area of offenses committed using information and communications technologies.

In parallel, the institutional structure was reinforced by the establishment of a central technical service for data and information system security, the Special Division to combat cybercrime, and the Data Protection Commission. This structure will soon be further enriched by the establishment of a national cybersecurity advisory committee and a national cybersecurity agency to implement the 2022 National Cybersecurity Strategy.

Building cybercapacity presents another challenge, especially for developing countries. Senegal has thus made multiple efforts to provide training in information security. Currently the country has several training establishments in the field, of which the most noted are the National and Regional Cybersecurity School of Dakar, opened in November 2018, and the Professional Institute for Information Security, established in October 2015.

Cybersecurity should not inhibit the innovation and development opportunities offered by new information and communications technologies or be used for the purpose of restricting the development of those technologies.

As a means of prevention and combating the malicious use of cyberspace, cybersecurity initiatives should have the ultimate goal of promoting a digital environment that is accessible, safe, peaceful and prosperous and which leaves no one out, in accordance with target 9.c of Goal 9 of Agenda 2030.

With this ambition in mind, the Government of Senegal has developed the Digital Senegal Strategy 2016–2025, in accordance with the Emerging Senegal Plan. This document, which embodies the ambition of Senegal to maintain a position as the lead country in Africa for digital innovation, is centred on the slogan “digital for all and for all uses by 2025 in Senegal, with a dynamic and innovative private sector in an effective ecosystem”.

Annex LV

Statement by the Permanent Representative of Singapore to the United Nations, Burhan Gafoor

Thank you for convening this important meeting, which marks the first time that the Security Council will address cybersecurity formally.

It is a timely topic. The accelerated speed of digitalization brought on by the coronavirus disease (COVID-19) pandemic has benefited our lives in new ways. It has also opened us up to new vulnerabilities. Cyber threats and malicious cyberactivities are becoming more frequent and sophisticated with more severe consequences. In 2020, malicious cyberactivities were estimated to have cost losses of nearly $1 trillion. The recent spate of such activities is a stark reminder that the international community must continue to guard against and be prepared to respond to these global and transboundary threats. I would like to highlight five points in this regard.

First, we must recognize that cyberspace is fundamentally an issue of managing the global commons. As a small State, Singapore has always supported a rules-based multilateral system rooted in respect for international law. Our approach is no different regarding cyberspace. To maintain a cyberspace that is secure, trusted, open, and interoperable, we must adopt a global approach, based on global rules and norms and adherence to international law. To do so will be challenging, given the backdrop of a volatile and fractious global landscape caused by growing geopolitical tensions. However, we have no option but to continue to advocate and support the applicability of international law and norms in order to encourage responsible State behaviour in cyberspace. We need to double down on international collaboration for greater cyberresilience and stability.

Singapore is committed to the role of the United Nations, as the only universal, inclusive, and multilateral forum, in developing rules that govern cyberspace. We are encouraged by the maturing cybersecurity discussions at the United Nations. Since the first time information and communications technology (ICT) security was included in the agenda of the United Nations in 1998, six Groups of Governmental Experts (Group of Governmental Experts) have studied the threats posed by the misuse of ICT in the context of international security and how these threats should be addressed. Four of these Groups have agreed on substantive reports, including the latest iteration which has just completed its work.

The cybersecurity discussions were brought to the wider membership for the first time at the s session of the General Assembly. This was done through the establishment of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security. We are encouraged by the successful recent adoption of the consensus report of the Open-ended Working Group. The report contributes to our common understanding on many issues and identifies areas where more discussions are needed.

Singapore participated actively in both the Open-ended Working Group and the most recent Group of Governmental Experts. Singapore is also honoured to be elected as Chair of the new Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025. As Chair of this body, Singapore is strongly committed to continuing the open, inclusive, and transparent discussions on cybersecurity at the United Nations. We are hopeful that the work of the new Open-ended Working Group will contribute to a rules-based multilateral order in cyberspace, and give all States, big or small, the confidence, predictability, and stability that are essential for economic progress, job creation, and technology adoption. We look forward to working closely with all Member States in this regard.

Second, all States are vulnerable to malicious cyberactivity which is growing in scale and sophistication. But small States are particularly vulnerable, especially developing countries and least developed countries. If we are serious about a global approach to cybersecurity, we must maintain a strong focus on capacity-building for countries that need help. This is one area where the United Nations can help to coordinate efforts. Singapore partnered with the United Nations Office for Disarmament Affairs to develop an online training course open to all Member States to promote a greater understanding of the use of ICT and their implications for international security. We remain committed to working with and supporting the United Nations to offer further capacity-building programmes.

Third, Singapore believes that more can be done to promote greater awareness and implementation of the existing 11 voluntary, non-binding norms of responsible State behaviour in the use of ICT. We support the exchange of best practices and experiences on the implementation of norms. This will help to identify challenges which we should tackle and gaps where additional norms may be needed. Singapore supports further work to elaborate the existing norms. For example, malicious cyberactivity against any cross-border Critical Information Infrastructure (CII), such as clouds and banking systems, can cause wide-ranging disruptions to essential services in multiple States, including those related to international trade, transport, and communications. States should consider how to improve cross-border cooperation with the relevant infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure.

This brings me to my fourth point on greater engagement with other stakeholders, in particular the private sector. With a significant portion of CII owned by the private sector, the international community must find ways to cooperate closely with the private sector to prevent and mitigate the impact of such disruptions. Singapore supports a collaborative approach between the public and private sectors to exchange best practices to support a strong cybersecurity framework.

Fifth, Singapore believes that regional organizations play an essential role to support United Nations discussions and to assist in the implementation of rules and norms developed at the United Nations. Cybersecurity was a priority for Singapore’s Chairmanship of the Association of Southeast Asian Nations (ASEAN) in 2018. That year, ASEAN became the first regional organization to subscribe in-principle to the 11 voluntary, non-binding norms of responsible State behaviour in the use of ICTS. ASEAN is now developing an action plan to implement these norms. Within ASEAN, Singapore has also been supporting capacity-building programmes. The ASEAN-Singapore Cybersecurity Centre of Excellence was established in 2019 as a multidisciplinary centre for capacity-building on areas such as confidence-building measures, policy, strategy, legislation, and operations. We look forward to working together with Member States to enhance our collective cybercapacity-building efforts.

Let me conclude by saying that a safe and secure digital infrastructure must undergird our ambitions for the digital economy. It is more important than ever for Member States to tackle the challenge of cybersecurity together, in a sustained, holistic, and coordinated manner. Singapore stands ready to work with all countries to build partnerships and cooperation towards a secure, trusted, open, and interoperable cyberspace.

Annex LVI

Statement by the Permanent Representative of the Slovakia to the United Nations, Michal Mlynár

Slovakia associates itself with the statement delivered by the European Union. We would like to make some additional remarks in national capacity.

I would like to thank the President for organizing this timely discussion that provides an opportunity for reflection on the growing risks stemming from malicious activities in cyberspace and their impact on international peace and security as well as to address the global efforts to promote peace and stability in cyberspace.

The coronavirus disease (COVID-19) crisis has made the need to bolster the security and stability of cyberspace even more topical and pressing. The crisis has shown that digital capabilities have become crucial for the provision of essential services as well as for the continuation of effective governance. The disruption of the functioning of critical infrastructure can cause serious consequences. Malicious cyberactivities against vital sectors and services have destabilizing effects and may ultimately threaten international peace and security.

Since cyberthreats are largely transnational in nature, it is important to maintain international cooperation and dialogue between States as well as between States and the multi-stakeholder community. It is through our shared responsibility and joint efforts of the governments, private sector and civil society that we can effectively support the maintenance of international peace and security in cyberspace, and protect human rights.

The United Nations plays an important role in driving international debates to raise awareness of cyberchallenges to international peace and security, and to make progress on advancing responsible State behaviour in cyberspace.

Slovakia strongly supports multilateralism which helps to manage and tackle current and future challenges in cyberspace. We are convinced that the stability in cyberspace should be based on existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law. Slovakia fully supports the applicability of existing international law to State conduct in cyberspace as recognized by three consensus reports of Groups of Governmental Experts endorsed by the General Assembly in 2010, 2013 and 2015. Our best efforts shall go towards holding transparent and constructive discussions, so that we can mutually benefit from each other´s experience, good practice and expertise.

Slovakia is also a co-sponsor of the programme of action to advance responsible State behaviour in cyberspace within the Open-ended Working Group. We believe in an inclusive and constructive institutional dialogue focused on results, regularity and consensus-based approach. In our view, the programme of action proposal offers grounds for such dialogue across the whole United Nations membership.

When it comes to confidence-building measures and capacity-building in cyberspace, Slovakia is of the opinion that these two are the most important measures in order to keep stability in cyberspace. Regional organizations such as the Organization for Security and Cooperation in Europe are being very useful tools in conflict prevention and strengthening cooperation between States. Regular communication and interaction between States in cyberspace help to avoid conflict and to deescalate potential rising tensions and, at the same time, they create a platform for dialogue.

The international law is one of the main pillars of stability and predictability in relations between States. Slovakia strongly stands with those reaffirming that existing international law – notably the Charter of the United Nations in its entirety and international humanitarian and human rights law – do apply to actions of States in cyberspace. The Charter of the United Nations sets out the rules and principles of international law of particular importance for the maintenance of peace and stability. There is no doubt that human rights apply online as they do offline and States must respect and defend those rights.

Thank you, Madam President.

Annex LVII

Statement by the Permanent Mission of Slovenia to the United Nations

Slovenia welcomes the first open debate of the Security Council, dedicated to a specific thematic issue of the cybersecurity. Addressing cybersecurity is timely and beneficial for all Member States. An open debate in the Security Council on this topic is contributing to raising awareness in the framework of international peace and security. In this regard, Slovenia welcomes the recent reports agreed by consensus of the Open-ended working group on Developments in the Field of information and communications technologies in the Context of International Security (Open-ended Working Group) and United Nations Group of governmental Expert to advance responsible State behaviour in cyberspace.

Slovenia aligns with the statement of the European Union and we would like to make additional remarks in the national capacity.

We live in an interconnected and rapidly changing world. A global, open, free, stable and secure cyberspace contributes to economic and social benefits. However, there are also malicious cyberactivities. Misuse of cyberspace can affect vital economic sectors and essential services to the public, such as health-care and energy, and other basic infrastructure. Malicious purposes in the use of ICT by State or non-State actors can undermine trust between governments with negative implications leading to destabilization of international peace and security.

To mitigate existing and emerging threats Slovenia firmly believes that cyberspace should be governed in full respect of existing international law, in particular the Charter of the United Nations in its entirety, international humanitarian law and human rights, as well as the implementation of norms and rules for responsible State behaviour. To this end, our first objective should be to promote the application of existing international law and to focus our collective efforts on advancing the implementation of existing norms of responsible State behaviour, including criminal prosecution of private entities operating from a country jurisdiction.

The norms of responsible State behaviour go hand in hand with the policy of confidence-building and capacity-building measures. This is where we can make a real difference. Slovenia firmly supports – within the framework of the 53 Member States – the proposal to establish a programme of action to advance responsible State behaviour in cyberspace. The programme of action will build on the existing acquis of the General Assembly. The programme of action will provide an opportunity to foster capacity-building programs and will provide an institutional mechanism within the United Nations for cooperation and exchange of best practice and cooperation with other stakeholders.

Moreover, in implementing norms of responsible State behaviour, Slovenia will continue to promote and support the prominence of a gender perspective in reducing the "digital gender divide" and effective and meaningful participation of women in decision-making processes related to the use of ICT in the context of international security.

Slovenia, as the incoming presidency of the Council of the European Union starting on the 1st of July 2021, will strengthen cooperation in the field of cybersecurity and streamline cyberissues between the European Union and Western Balkans region. Bringing Western Balkans closer to the European cyberecosystem is an important element in building trustful and secure environment for digital development, better connectivity and better access to the digital economy and society. It is also a contribution to global stability in cyberspace.

To this end, Slovenia plans to organize the informal European Union and Western Balkans Summit in early October 2021. Slovenia will also organize a Cyber Security Conference – the event on the Western Balkans in cooperation with the EUISS. Additionally, we will contribute to a review and progress of cooperation with Western Balkans States in the field of prevention and investigation of sexual abuse and exploitation of children.

Slovenia, as the incoming presidency of the Council of the European Union will also promote European regulatory efforts to strengthen cyberresilience and cybercrisis management, with the review of the Directive on Security of Network and Information Systems (NIS 2 Directive) outlining measures for high common level of cybersecurity across the Union, as well as the efforts to actively promote the implementation of European Union Cyber Diplomacy Toolbox as a means of contributing to conflict prevention, mitigation of cybersecurity threats and greater stability in international relations. We are going to strive for increased international cooperation, and reducing risk of misperception, escalation and conflict.

Let me conclude by reiterating that Security Council plays a central role in supporting efforts in the field of cybersecurity which are crucial to maintaining international peace and security. By organizing this open debate, you have already actively encouraged to foster an environment that leads to the promotion of cooperation, building confidence related to ICT and to global, open, free, stable and secure cyberspace.

Annex LVIII

Statement by the Permanent Mission of South Africa to the United Nations

South Africa has noted with interest the convening of this open debate of the Security Council to consider, for the first time as a dedicated thematic matter, the maintenance of international peace and security in cyberspace. We also thank the High Representative for Disarmament Affairs, Ms. Nakamitsu, for her briefing.

We have further noted the guiding questions provided for the discussion today, which we will endeavour to respond to in our statement.

At the outset, South Africa would like to emphasise that the issue of peace and security in cyberspace is a pervasive and complex matter that requires the full engagement of all Member States of the United Nations. It is for this reason that we believe that the proper place for this matter to be addressed is within the proceedings of the First Committee of the General Assembly, which has already been engaging on this matter.

In this regard, Member States have been engaged through the work of a number of Groups of Government Experts, the latest of which focused on advancing responsible State behaviour in cyberspace, producing its consensus report at the end of May 2021 under the able leadership of Ambassador Guilherme de Aguiar Patriota of Brazil.

Furthermore, the broad engagement of all Member States have taken place in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security from 2019, which adopted its consensus Report at the end of March 2021; and the newly established the Open-ended Working Group on Security of and in the use of information and communications technologies 2021–2025 that will be guided by Ambassador Burhan Gafoor, the Permanent Representative of the Republic of Singapore as its Chair.

The United Nations membership has therefore come a long way in discussing emerging threats to international peace and security in cyberspace; the international law frameworks that govern this aspect of international peace and security; the norms, rules and principles that guide Member States; the required confidence-building measures; capacity-building requirements; as well as ways to continue dialogue in this regard.

Allow me to make the following brief points in this context.

South Africa believes that the multitude of emerging threats necessitates the engagement of all relevant actors including civil society and the private sector. This will be necessary both to understand the nature of these threats and to cooperate across all of society to on the threats posed by both State and non-State actors in cyberspace and adequately address them.

South Africa would like to emphasise the need to bridge the digital and gender divides, as well as the transformation of the digital divide into digital opportunities, which will be key to building resilience while at the same time fostering greater development. The increasing sophistication of harmful ICT incidents, however, are a concern for developing countries such as South Africa.

South Africa remains concerned by the growing threat of cyberattacks on critical infrastructure and critical information infrastructure. While we believe we should confront these threats through greater cooperation and the development of best practice mechanisms, these efforts should support national priorities and efforts to identify and designate such infrastructure. We are also aware that despite the exposure to threats the positive economic and social opportunities that can be derived from ICT should not be overshadowed by the malicious use of these technologies. Therefore, it is not the technologies themselves, that are of concern, but the misuse of such technologies.

In order to govern the use of cyberspace and especially the threats posed to international peace and security, South Africa supports the applicability of international law and specifically the Charter of the United Nations in its entirety.

In view of the significant work already done, we believe that we should focus on implementing existing norms, rules and principles. It is a fundamental principle shared by developing countries that we must also recognize the fact that we are all at varying positions of risk, given the varying capacities of States to guard against the threats posed by malicious acts in cyberspace. Therefore, my delegation would like to emphasise the need for capacity-building programmes from both State and other stakeholders to assist countries in combating the destabilising threats from malicious actors in the cyberrealm. South Africa believes that capacity-building is critical in bringing States on par for the betterment of the security of global cyberspace, as this is truly a global challenge that requires global solutions.

Finally, South Africa remains committed to continuing the engagement to address these matters, especially within the context of the Open-ended Working Group on Security of and in the use of information and communications technologies, which will begin its substantive work in December. This will serve as an all-inclusive, single-track for discussing how we can all address the emerging, complex and pervasive threats to international peace and security in cyberspace.

Annex LIX

Statement by the Permanent Mission of Switzerland to the United Nations

[Original: French]

I would like to thank Estonia for organizing this open debate and the High Representative for her briefing. Cyberspace has become an integral part of our societies and creates tremendous opportunities for social and economic development. At the same time, malicious cyber operations pose a risk of instability and have become a threat to international peace and security. We are concerned that cyberspace is being instrumentalized for projection of power and is becoming increasingly fragmented and destabilized.

An open, secure, stable, accessible and peaceful cyberspace is beneficial to all. The United Nations plays a crucial role in this respect. Switzerland welcomes the recent adoption by consensus of the reports of the Group of Governmental Experts and the Open-ended Working Group. These reports represent essential steps towards responsible behaviour of States in cyberspace.

To promote peace and stability in cyberspace, I would like to highlight several points.

First, international law applies in cyberspace. Respect for international law is an essential condition for conflict prevention and the maintenance of international peace and security. The obligation to resolve disputes by peaceful means also applies to the activities of States in cyberspace. Furthermore, international humanitarian law is applicable when an armed conflict, whether international or not, exists de facto. Switzerland welcomes the fact that the latest Group of Governmental Experts report clearly states this. This is a significant milestone. International humanitarian law and its fundamental principles place important limits on the execution of cyber operations in the context of armed conflict.

Second, Switzerland is concerned about the humanitarian impact of malicious cyber operations, which have been on the rise since the pandemic and frequently concern medical infrastructure. Switzerland stresses that such infrastructure is protected, as demonstrated in the open debate in April. The Group of Governmental Experts reports provide a framework to protect critical infrastructure from malicious cyber activities. In addition, data collected for humanitarian purposes must be protected. We also encourage States to comply with the voluntary norms of responsible behaviour in cyberspace and additional Group of Governmental Experts guidance for their implementation, to avoid damage to critical infrastructure, mitigate humanitarian impacts and ensure the protection of civilians.

Third, confidence-building measures are important to prevent a climate of mistrust in cyberspace. At the regional level, Switzerland is committed to advancing the role of the Organization for Security and Cooperation in Europe in promoting cyber stability. It is developing, together with Germany, a proposal for the implementation of a confidence-building measure that provides for consultations in the context of a serious cyber incident. Switzerland is also committed to transparency and capacity building. Our National Cyber Security Centre provides technical support to other States in the event of an incident and shares data and information on possible threats. The Security Council and United Nations organizations should take into account regional initiatives and confidence-building measures that have proven useful in promoting peace and stability in cyberspace.

Lastly, civil society organizations, academia and the technical community as well as the private sector play an important role in supporting international cyber stability, especially with regard to the respect for human rights and fundamental freedoms online and offline. Switzerland, as a member of the Freedom Online Coalition, engages with over 30 Governments and a network of stakeholders to promote freedom of expression on the internet. We encourage the Security Council and Member States to involve the different actors in the implementation of the Framework for Responsible State Behaviour in Cyberspace.

Multilateral cooperation and adherence to international law, including human rights and international humanitarian law, are essential for peace and security in cyberspace. Switzerland encourages further work on these topics, including in the new Open-ended Working Group and the future programme of action for the promotion of responsible State behaviour in cyberspace. As a candidate for the Security Council, Switzerland looks forward to pursuing a multi-stakeholder and constructive dialogue, building on the existing achievements.

Annex LX

Statement by the Permanent Mission of Thailand to the United Nations

Thailand appreciates Estonia's efforts in organizing the Security Council High-Level open debate: "Maintaining international peace and security in cyberspace" at this relevant and timely juncture. We also commend Estonia's leadership, being the first to hold a formal Council meeting on cybersecurity. We hope that securing and preventing the misuse of cyberspace and information and communications technologies (ICT) will remain high on the Council's agenda, while continuing to welcome the participation of the wider United Nations membership on these important discussions.

Thailand is of the view that cyberspace has benefitted humanity, as evident during the pandemic, by keeping people connected to basic social services and most importantly, to each other, as well as a contributor to the achievement of the 2030 Agenda for Sustainable Development. Nonetheless, the uses of ICT by States and non-State actors, including terrorists for malicious purposes such as attacks on critical civilian infrastructure, not only undermine international peace and security, but also affect the safety of our people. It is therefore the responsibility of States, in line with relevant international laws and norms, to address these issues.

Thailand believes that the United Nations can play a significant role in supporting efforts towards the creation of a stable and secure cyberspace. Indeed, the security of cyberspace has been on the agenda of Member States for more than two decades. The most evident successes have been the recent historic adoptions, by consensus, of the report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (2019–2021) and the report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (Group of Governmental Experts) (2019–2021).

Thailand welcomes the new Open-ended Working Group on security of and in the use of information and communications technologies (2021–2025). We are confident that, under the able leadership of Mr. Burhan Gafoor, Permanent Representative of Singapore and Chair of the Open-ended Working Group, States will engage in fruitful discussions, including on enhancing confidence, cooperation and transparency among States and the further elaboration of norms on responsible State behaviour in cyberspace.

At the new Open-ended Working Group, Thailand hopes that the following issues may be resolved or clarified: further developing guidance and recommendations on how to operationalize norms of responsible State behaviour; reaching a common understanding on how international law applies in cyberspace and whether gaps exist; creating sustainable, demand-driven confidence-building measures, and adopting a "Regular Institutional Dialogue".

Thailand also takes note of the good efforts by other intergovernmental bodies, private sector, and civil society organizations and processes that have contributed to our collective endeavour towards a safe and secured cyberspace. Thailand supports multi-stakeholder approach in our work to ensure meaningful engagement of relevant stakeholders and partners in the society, including that of women and youth.

To this end, Thailand supports the strengthening of normative foundations by enhancing practical implementation of agreed norms, bridging existing divergences and capacity needs, and ensuring that existing multilateral and bilateral channels are kept open for continued dialogue. All States must continue working together to safeguard our shared vision of an open, secure, accessible, and peaceful cyberspace and ICT environment for all.

Annex LXI

Statement by the Permanent Mission of Turkey to the United Nations

I would like to thank Estonia for organizing this open debate, which focuses on a critical topic particularly under current circumstances due to the pandemic. I also thank Madame Nakamitsu, High Representative for Disarmament Affairs, for her briefing.

The use of information and communications technologies (ICT) impacts economy and development around the world. The pandemic has underlined how heavily reliant we are on digital technologies. Ensuring free, open and secure access to ICT is certainly crucial.

Turkey is concerned with the growing number of cyberattacks. Malicious cyberactivities targeting critical infrastructure, terrorism, digital espionage, fraud, online child abuse and exploitation, and misuse of personal data are among current threats that also pose risk to international peace and security.

Due to technological developments, cyberattacks have become easier to carry out, while the negative effects and the cost for the victims are rapidly increasing. Cyber-attacks are also getting more “target-oriented”. The annual cost of cyberattacks is increasing exponentially. Defense against these attacks requires new and up-to-date methods and instruments.

Turkey welcomes the consensus reports of the Open-ended Working Group on Developments in the Field of information and communications technologies in the Context of International Security and, more recently, the United Nations Group of Governmental Experts to Advance Responsible State Behaviour in Cyberspace. These reports are valuable contributions to the existing body of work on cybersecurity under the United Nations umbrella. It is equally important that both Open-ended Working Group and Group of Governmental Experts reports are compatible and complementary in order to increase stability, resilience and international cooperation in cyberspace. We hope to see more cohesion in such endeavours in the future.

With its fast rate of digitalization, Turkey has been focusing on taking necessary measures in order to improve its national cybersecurity. Currently, National Cyber Security Strategy and Action Plan, which covers the term 2020–2023 is being implemented. Main strategic objectives of this Action Plan are critical infrastructure protection and increasing resilience, capacity-building, organic cybersecurity network, security of new generation technologies (i.e. IoT, 5G, cloud computing etc.), fight against cybercrime, developing and fostering domestic and national technologies, integration of cybersecurity into national security, and improving international cooperation.

In addition, the National Cyber Emergency Response Team of Turkey plays a vital role in the implementation and coordination of preventive measures against cyberthreats.

Training programs as well as national and international cybersecurity exercises complement our efforts. Turkey’s information and communications technologies Authority (BTK) provides online public trainings on cybersecurity and other related areas. More than 5.000 people have been trained in different areas of cybersecurity in the last 4 years.

Annually organized “Safer Internet Day” is among the awareness raising activities of BTK, aiming at increasing awareness on conscious and safe use of the Internet. Additionally, Turkey takes steps to counter heightened digital security risks to cybersecurity and has taken measures in cooperation with relevant stakeholders, in order to guarantee business continuity, accessibility and protection of consumers during the pandemic.

We have also taken steps to strengthen our national legislative framework.

Given the transborder nature of cyberrisks, increased international cooperation is crucial. With this understanding, Turkey engages in cyberthreat intelligence sharing and contributes to policies and cooperation strategies within regional and international organizations, including the Organization for Security and Cooperation in Europe, G20 and OECD. Turkey also participates in international exercises, including those within ITU and NATO.

The United Nations has a central role for a more strategic and effective cooperation in the use of ICT by States. Turkey supports the applicability of international law in cyberspace. It is high time we built on the previous work undertaken within the United Nations system and find meaningful ways to operationalize rules, norms, principles and recommendations for responsible State behaviour in cyberspace.

A priority area for our future work is forging a common understanding on how international law applies in cyberspace. This is indeed necessary to decrease misunderstandings and promote accountability in cyberspace.

There is also need for establishing communication channels among Member States for emergency situations and sharing information and resources through those channels. This would highly contribute to confidence-building and accelerate our capacity-building efforts.

In addition, we also need to urgently review and strengthen existing international instruments in order to enhance cooperation within the framework of new technologies such as cloud computing, the Internet of Things, 5G and Artificial Intelligence.

Conducting a survey of national regulatory approaches towards ensuring the security of new technologies and preparing code of conducts to guide and inform the national frameworks can be useful tools. Also, we need to develop a common understanding and definitions of threats.

In the context of capacity-building, we believe that the United Nations as well as the regional organizations can promote exchange programs for cybersecurity experts and establish common training platforms. International exercises must be encouraged in order to enhance national cyberincident preparedness and response capacities.

Since cyberspace is a borderless field and cybersecurity is a multi-stakeholder issue, national authorities need to work with users, private sector, NGOs, and international counterparts in order to fight against cyberthreats. Global vendors, service providers and security companies should also cooperate more effectively with governments and international organizations in order to contribute to global cybersecurity.

Turkey is committed to continue its engagement and dialogue in order to promote regional and global cybersecurity.

Annex LXII

Statement by the Permanent Mission of Ukraine to the United Nations

We thank Estonia for initiating such an important meeting of the Security Council, as well as Ms. Nakamitsu, the High Representative for Disarmament Affairs, for her briefing.

Rapid development of information and communications technologies progressively led to the "re-formatting" of Internet space: nowadays it is no longer a comfortable platform for communication, but also real weapon, which becomes more and more dangerous in hands of hackers, criminals, some State actors and their proxies.

Unfortunately, despite existing legal norms and institutional mechanisms established to combat cybercrimes on national, regional and international levels, the advantages of modern digital world are too often been abused, with cyberattacks on the rise, having become a new method of hybrid warfare.

International policy is progressively becoming vulnerable to cyberthreats. Over the last few years, a number of States in the world have become lucrative targets of cyberattacks.

Ukraine is the State where cyberattacks since 2014 became one of the major elements of the external attempt to undermine our sovereignty. In 2014-2021 Ukraine has faced an unprecedented number of cyberoperations against vital objects of our critical infrastructure. Most of those attacks were carried out by hacker groups being controlled from the Russian Federation.

Cyberoperations against major critical infrastructure facilities, energy, transport, oil and gas sectors are challenges and threats to international peace and security. Recently, the Colonial Pipeline has been an object of cyberattack that seriously impacted computerized equipment managing the pipeline leading to serious consequences.

In times of the coronavirus disease (COVID-19) pandemic, the devastating impact of malicious cyberoperations is evident. Some State and non-State actors abuse the global crisis to launch cyberoperations, including against the health sector, which is a matter of an urgent concern for the international community.

Yet not only critical infrastructure, but international politics are becoming progressively vulnerable to malicious use of ever more complex and sophisticated ICT capabilities that was confirmed by headline-making cases of interference into major election campaigns and candidate's profiles committed by Kremlin's hackers.

Therefore, cyberstability has become a crucial component of ensuring wider peace and security that requires strict adherence to international law, the application of which in cyberspace has been recently reaffirmed in the Open-ended Working Group and Group of Governmental Experts reports, appropriate implementation of norms, rules and principles of responsible behaviour, as well as strengthening international cooperation to preserve a free, open, stable and secure cyberspace.

We emphasize that a particular attention should be placed on elaboration of unified standards in combating cyberthreats, sharing best practices, building mutual trust in the field of cybersecurity, preventing the use of cyberspace for political, terrorist and military purposes, as well as providing financial and technical assistance to enhance national capacities to withstand cyberthreats, mitigate the risks and strengthening resilience.

As of today, cyberoperations against critical infrastructure and governmental agencies, as well as disinformation campaigns, that may incite terrorism, is a widely used method of interference into internal affairs of sovereign States, including Ukraine.

No doubt, Russia uses high technologies to get its own political and geopolitical objectives, namely by supporting and exacerbating conflicts in neighbouring States, conducting aggressive information wars.

We strongly encourage the international community to thoroughly consider the issue of accountability in cases of identification of a particular State or State actors behind preparation or exercising targeted malicious use of ICT or dissemination of lies for hostile purposes.

After all, international efforts made in this domain are simply in vain if there are no reliable mechanisms to detect, punish and bring to justice individuals and relevant States, responsible for coordinating and financing illicit activities in the global cyberspace.

Annex LXIII

Statement by the Permanent Mission of the United Arab Emirates

The coronavirus disease (COVID-19) pandemic has highlighted the world's dependence on information and communications technologies which were essential in keeping us informed and connected to one another, even as we remained physically apart.

Over the course of the last eighteen months, we have witnessed an increased trend in malicious cyberoperations targeting medical facilities, including organizations dedicated to research and vaccine development to combat COVID-19. We live in a volatile region, and the Middle East is not immune to the risk posed by malicious cyberactivity—it is often the target of major cyberoperations and espionage. In the last few years, our region has witnessed severe incidents affecting the telecommunications, banking, and public sectors. Oil and natural gas installations have also been targeted, causing hundreds of millions in damages. Such malicious cyberactivity on the region's critical infrastructure has the potential to spark a conflict in an already tense environment, and pose a threat to international peace and security.

The United Arab Emirates is committed to creating the necessary infrastructure and mechanisms to enhance its cybersecurity capabilities, both to protect itself against cyberthreats and better work with others to address shared challenges. In November 2020, we established the United Arab Emirates Cybersecurity Council, which will develop a comprehensive national cybersecurity strategy and a national cyberincident response plan. We host the largest cybersecurity and digital transformation conferences including GITEX, GISEC and Cybertech to build domestic capacity, and we have developed a platform for public-private partnership to facilitate information sharing. We also collaborate with States, international organizations, and private sector entities to share information both at a policy and technical level. For example, the United Arab Emirates contributes to the work of regional organizations, such as the Gulf Cooperation Council's new joint malware analysis platform, and is an active member of the Organization for Islamic Cooperation's Computer Emergency Response Team (OIC-CERT). These cooperative and transparency confidence-building measures are some of the ways that the United Arab Emirates is doing its part to reduce cyberrisks to international peace and security.

The United Arab Emirates welcomes the recommendations in the reports of both the Open-ended Working Group on ICT and the Group of Governmental Experts. They underline the importance of supporting efforts to further the implementation of the voluntary norms of responsible State behaviour in cyberspace as well as the need to develop common understandings on the applicability of international law to online activity. More, however, needs to be done, both to encourage and support States in carrying out the recommendations as well as to provide further guidance in a rapidly evolving environment. The programme of action for responsible State behaviour in cyberspace provides an ideal road map for future work, and will contribute to addressing cyberrisks to international peace and security.

Minimizing cyberrisk to international peace and security will remain a challenge. The United Arab Emirates proposes two recommendations that can assist with this task.

First, States should provide training and capacity-building at the bilateral, regional and international levels, including through training programmes and the development of guidance to assist with implementing the norms for responsible State behaviour. These actions can act as confidence-building measures, responding to the mistrust and misunderstandings between States in cyberspace that can pose a risk to international peace and security.

Second, States should continue to share their views and assessments with the Secretary-General and actively participate in cyberrelated international fora and cross-regional formats. The sharing of best practice and exchanges of experience can help States adapt to evolving norms and become responsible actors in cyberspace.

All States have a responsibility of promoting international peace and security, both online and offline. Abiding by norms of responsible State behaviour in tandem with obligations under international law is the best place to start.