United Nations S/PV.9662 (Resumption 1)

Security Council

Seventy-ninth year

Provisional

9662nd meeting
Thursday, 20 June 2024, 3 p.m.
New York

President:	Mr. Hyunwoo Cho	(Republic of Korea)
Members:	Algeria	Mr. Louafi
	China	Mr. Wang Zhenjiang
	Ecuador	Mr. Durán Medina
	France	Mr. Strehaiano
	Guyana	Ms. Parmanand
	Japan	Mr. Suzuki
	Malta	Mr. Ciscaldi
	Mozambique	Mr. Irachande Gouveia
	Russian Federation	Mr. Dergachev
	Sierra Leone	Mr. Schenks
	Slovenia	Mr. Burkeljc
	Switzerland	Mr. Stritt
	United Kingdom of Great Britain and Northern Ireland	Ms. Page
	United States of America	Ms. Wu

Agenda

Maintenance of international peace and security

Addressing evolving threats in cyberspace

Letter dated 7 June 2024 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the President of the Security Council (S/2024/446)

The meeting resumed at 3.05 p.m.

The President: I wish to remind all speakers to limit their statements to no more than three minutes in order to enable the Council to carry out its work expeditiously. Flashing lights on the collars of the microphones will prompt speakers to bring their remarks to a close after three minutes.

I now give the floor to the representative of Cuba.

Mr. Gala López (Cuba) (*spoke in Spanish*): The use of information and communication technologies must be preserved for exclusively peaceful purposes, in order to benefit cooperation among and the development of peoples.

Cuba firmly opposes the militarization of cyberspace and any use of information and communications technologies as instruments for the threat or use of force, or for actions aimed at interfering in the internal affairs of States. Article 51 of the Charter of the United Nations is not applicable and cannot be invoked in the context of cyberspace. It is therefore worrisome that some States include, in their national security strategies, the use of cyberweapons and the possibility of cyberattacks, supposedly to deter adversaries.

All necessary measures must be taken to prevent the misuse of information and communication technologies and media platforms, including social networks and radio and electronic broadcasts, as tools for the promotion of hate speech, incitement to violence, subversion, destabilization, the dissemination of false news and the misrepresentation of the reality of States for subversive and interfering aims, in contravention of international law. The covert and illegal use of nations' information technology systems by individuals, organizations and States to carry out cyberattacks against third countries is also unacceptable.

Cuba advocates for the negotiation, within the framework of the United Nations, and the adoption, as soon as possible, of a legally binding international instrument to fill the significant legal gaps in cybersecurity and effectively address the growing challenges and threats in that domain, including through international cooperation. There is a need to overcome the colossal technology gap and obstacles imposed on developing countries in order to invest in the security of their information and communications technology infrastructure, which limit the ability of those countries to cope with threats.

The Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, mandated by the First Committee of the General Assembly, is the appropriate mechanism for conducting exchanges and reaching agreement on the threats and challenges that we face as States and that involve the malicious use of information and communications technologies. The Group is an inclusive, democratic and transparent forum in which all Member States can contribute on an equal footing to finding consensus-based solutions in this domain.

The President: I now give the floor to the representative of Bahrain.

Ms. Salman (Bahrain) (*spoke in Arabic*): At the outset, I would like to welcome His Excellency Mr. Cho Tae-yul, Minister for Foreign Affairs of the Republic of Korea, presiding over this morning's session of the open debate, and to thank the Permanent Mission of the Republic of Korea to the United Nations for convening this meeting on a topic that is increasingly important, given the major developments in cyberspace. I would also like to thank His Excellency Mr. António Guterres, Secretary-General of the United Nations, and other briefers for their valuable statements.

The growing risks posed by malicious activities in cyberspace, such as ransomware attacks, cryptocurrency theft and the theft of sensitive information and assets, not only jeopardize the safety of critical infrastructure, but also exacerbate existing challenges to global stability. Those activities act as powerful threat multipliers, amplifying traditional security concerns and creating new vulnerabilities. The interconnected nature of digital systems means that cyberincidents can quickly escalate into international crises, undermining trust and stability among States.

The Kingdom of Bahrain emphasizes the importance of a multifaceted approach, which includes leveraging existing and innovative tools, platforms, frameworks and strategies to mitigate the risks associated with cyberthreats, in addition to engaging all stakeholders, given that cybertools and cybertechnologies are no longer the exclusive domain of governments. The Kingdom of Bahrain also emphasizes the importance of capacity-building and sharing technologies, knowledge and best practices to enhance the capabilities of States to prevent and respond to cyberincidents.

In that context, the Kingdom of Bahrain has supported various General Assembly initiatives

on strengthening cooperation for maintaining cybersecurity, including the groups of governmental experts, the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, and the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

At the national level, the Kingdom of Bahrain attaches great importance to cybersecurity, based on a clear cybersecurity governance system supported by a comprehensive national strategy. We have also established the National Cyber Security Centre to provide safe cyberspace in the Kingdom of Bahrain through establishing effective governance standards, providing the means of defence from, monitoring of and responding to electronic attacks, as well as raising awareness among individuals and institutions.

The national cybersecurity strategy is strengthening regional and international partnerships. Five fundamental pillars have been identified in this strategy, and each pillar is an essential and necessary component in realizing the Kingdom of Bahrain's cybersecurity vision. Taken together, they form a comprehensive and cohesive framework for maintaining a secure and reliable cyberspace. Those pillars are, first, strong and resilient cyberprotection; secondly, effective cybersecurity governance and standards; thirdly, building a cybersecurity-aware society; fourthly, enhancing protection through partnerships and cooperation; and fifthly, developing national cadres.

In conclusion, the Kingdom of Bahrain looks forward to further fruitful dialogues on cybersecurity within the United Nations, in particular in the Security Council, given the rapidly evolving nature of the threats arising from developments related to information and communications technology.

The President: I now give the floor to the representative of Poland.

Mr. Szczerski (Poland): The worldwide spread of digital technologies, including the development and implementation of e-government and the electronic administration of critical infrastructure resources, results in growing dependence on cyberspace. It poses serious challenges to the security and sovereignty of States. Every day, we are witnessing a growing number of malicious activities in cyberspace, carried out by both non-State and State actors, targeting the stability and security of countries and societies.

Poland adopted a national position on the application of international law in cyberspace as a primary measure to guarantee international peace and security. In that regard, there are two points that are of the utmost importance to my country. The first one is that, in certain circumstances, actions in cyberspace may constitute a violation of the prohibition of the use of force. The second one is that a cyberattack may be qualified as an armed attack. For us, the right to self-defence applies in cyberspace.

A challenge we often face involves the attribution of cyberattacks. Regardless, we shall not abandon efforts to bring responsible States and cybercriminals to justice. It is important to recognize that some States, instead of fighting cybercriminals operating from their territories, groom and protect them for political or economic gain. In doing so, they undermine the stability and security of others. They attempt to blur the lines between State-sponsored and criminally motivated actors and create ambiguity for the targeted entities when those entities try to defend themselves and hold the perpetrators accountable.

At the same time, there is a large group of States that have the political will to implement international law and voluntary norms, but that may lack the necessary capabilities to do so. It is in our common interest to work closely with them in order to assist them and to offer adequately measured and targeted capacity-building. That will not happen overnight. Therefore, we need a permanent platform for such cooperation within the United Nations framework. In that context, and in line with the statement delivered on behalf of the European Union, Poland strongly supports the establishment of the programme of action. We encourage all United Nations Members to support it and to actively contribute to its operationalization.

Cyberattacks and malicious activities seek to undermine international peace and security. Therefore, we call on the Security Council to step up efforts to stop and prevent malicious activities in cyberspace. We also want to call on one Member State of the Council — the Russian Federation — to respect international law and to stop its illegal aggression against Ukraine not only on the ground, but also in cyberspace and against its neighbours.

The President: I now give the floor to the representative of Romania.

Mr. Feruță (Romania): I would like to thank the Republic of Korea for organizing a debate on such an important topic.

I would like to make a few points in addition to the statement delivered on behalf of the European Union.

Threats in cyberspace are persistent, complex, destructive and have become more frequent. Romania is alarmed by the number of malicious cyberactivities targeting government institutions and democratic processes. That is a serious threat — cyberoperations, often in combination with disinformation, could undermine the integrity of democratic processes and the overall resilience of our societies.

We are also worried about cyberattacks against critical infrastructure and essential services, with possible disruptive and destructive effects. We strongly condemn malicious cyberactivities intended to undermine our democratic institutions, national security and free society. Irresponsible conduct in cyberspace creates risks to international peace and security and cannot be tolerated. The Security Council is entitled to address such issues and to encourage increased accountabilty.

International law applies in cyberspace. In cyberspace, States have the same obligation to act in a responsible manner, in line with international law, including the Charter of the United Nations, and we encourage the Security Council to condemn malicious behaviour in cyberspace. Any use of information and communications technologies (ICTs) by States in a manner inconsistent with international law and their obligations under the United Nations framework of responsible State behaviour in the use of ICTs undermines international peace and security.

Enhancing the Security Council's role in addressing cyberthreats in a manner complementary to other United Nations processes on ICTs is both timely and crucial for the maintenance of international peace and security in cyberspace. This open debate and previous Arria formula meetings in May 2023 and April 2024 confirm the important contribution that the Security Council can make.

Romania places great emphasis on the need to strengthen resilience in the cyberdomain. We need to enhance the protection of critical national infrastructure, as malign actors attempt to severely disrupt the functioning of our societies. We remain committed to the International Counter Ransomware Initiative and look forward to its consolidation as a coordinated international response to this set of threats. Moreover, the nature of cyberspace itself calls for a forward-looking discussion of the potential of artificial intelligence technologies to increase the magnitude and complexity of cyberattacks but at the same time to prevent and more rapidly counter cyberattacks and even mitigate their effects.

In conclusion, we call on all States to respect their international obligations and commitments to uphold international law and to act within the agreed framework for responsible State behaviour in cyberspace. We must indeed stay true to our core values and principles and act in a responsible manner.

The President: I now give the floor to the representative of Austria.

Mr. Pretterhofer (Austria): Austria wishes to thank the Republic of Korea for convening this timely open debate.

Austria aligns itself with the statement made on behalf of the European Union. Allow me to add the following points in our national capacity.

To answer your guiding questions on the role of the Security Council, Mr. President, we believe that it adds conceptual clarity to approach this debate through the common language on which we all agree: international law. All Member States have agreed by consensus that international law, and in particular the Charter of the United Nations, applies in its entirety to cyberactivities. And the Charter is clear: it gives the Security Council a mandate to respond to threats to international peace and security. In order to discharge its mandate, it is essential that the Security Council continue to respond to contemporary threats to international peace and security. It is equally important to highlight the role of the Security Council in the pacific settlement of disputes, as laid out in Chapter VI of the Charter. Cyberactivities do not take place in a separate virtual cyberspace, but in the real world. Therefore, cyberactivities do not constitute a new domain that requires its own new rules or a distinct application of international law. In the end, the Council addresses State behaviour. It is only logical that the Council not shy away from one form of State behaviour — cyberactivities — whenever it becomes relevant for its mandate. For example, regarding

sanctions, all activities, including cyberactivities, aimed at breaching binding sanctions decided by the Council merit its attention. In that regard, mainstreaming cybersecurity in the Security Council's files is crucial.

Austria is committed to the rule of law both in and outside the cybercontext and has recently published its position paper on cyberactivities and international law. Austria welcomes today's debate, which underlines the Security Council's important role in fulfilling its mandate, set out by the Charter of the United Nations, to address threats to international peace and security.

The President: I now give the floor to the representative of Kazakhstan.

Mr. Umarov (Kazakhstan): I would like to express our gratitude to the Republic of Korea for organizing today's very important meeting.

The pace of digitalization is faster than any other innovation in human history. In just two decades, digital technologies have transformed societies and affected approximately 50 per cent of the population of developing countries. The use of technology to improve connectivity and access to financial, business and government services can significantly reduce population inequality. The health-care industry is utilizing advanced technologies that use artificial intelligence to save lives, diagnose illnesses and increase life expectancy. The availability of virtual learning environments and distance learning in education has made it possible for students to participate in programmes that were previously unattainable.

At the same time, information and communications technologies (ICTs) are being used by numerous non-State actors, including criminal groups and terrorists, for identity theft, fraud and cyberattacks. They are also being used to sow discord and spread misinformation that can destabilize States and undermine trust among countries. Malicious acts in cyberspace can disrupt critical infrastructure, such as energy, transportation and communications, and could therefore serve as a threat multiplier in existing conflicts, requiring the involvement of the Security Council. That confirms the trend that cyberthreats are becoming a geopolitical challenge.

In that regard, Kazakhstan supports a global and responsible approach to the use of ICTs and artificial intelligence through the development of generally accepted standards for their use. Experts from our country are taking an active part in the work of the Open-ended Working Group on Security of and in the Use of Information and Communication Technologies and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. We support the global intergovernmental points of contact directory, which was launched in May. Like many Member States, Kazakhstan is currently in the process of appointing diplomatic and technical points of contact for the directory.

Finally, I would like to emphasize that in conditions of geopolitical instability, it is important to avoid the politicization of the issue and instead seek common ground. The Security Council could play a key role in coordinating international efforts and implementing specific measures to counter cyberthreats, including: supporting capacity-building initiatives for States, especially in developing regions; enhancing their ability to prevent and respond to cyberincidents; involving non-State actors, including tech companies and civil society organizations; strengthening collective efforts against cyberrisks; and of course, raising awareness about cybersecurity issues and organizing regular reviews of the changing cyberthreat landscape.

The President: I now give the floor to the representative of the Islamic Republic of Iran.

Mr. Iravani (Islamic Republic of Iran): I thank you, Mr. President, for convening this open debate.

Addressing evolving threats in the information and communications technology (ICT) environment requires a multifaceted approach encompassing technological, legal and cooperative strategies.

Iran has been the primary target and the main victim of numerous cyberattacks on its infrastructure, which have significantly disrupted public services and governmental functions. Clear examples include the Stuxnet and Duqu attacks on Iran's peaceful nuclear facilities, as well as cyberattacks on critical industrial infrastructure, such as the steel and petrochemical industries and gas stations. Those malicious activities highlighted the potential for ICT environments to be weaponized to inflict damage on the infrastructure of States.

Given the complex nature of ICT governance, I would like to highlight the following points.

First, the primary responsibility for maintaining secure, safe and trustworthy ICT rests with individual States. The prominent role and active involvement of States in the ICT environment governance at the global level, especially in policy and decision-making, must be enhanced and ensured. ICT governance should be developed in a manner that does not adversely affect the rights of States to determine their own development, governance and legislation concerning the ICT environment. States must act responsibly and in accordance with the fundamental principles of international law, in particular the purposes and principles of the United Nations.

Secondly, the absence of universally legally binding norms for ICT remains a challenge. Current international law often lags behind the rapid pace of technological change, creating gaps that malicious actors exploit. Developing and enforcing international legally binding norms that address the specific features of the ICT environment is therefore essential.

Thirdly, States must refrain from using ICT advances as tools for economic, political or other coercive measures, including limiting or blocking measures against other States. They must also prevent and avoid abusing ICT-related supply chains under their control and jurisdiction, ensuring that those supply chains do not develop vulnerabilities that compromise the sovereignty and data protection of other States. States must ensure appropriate measures for ICT companies and platforms with extraterritorial impacts within their jurisdiction and to hold them accountable for their behaviour in the ICT environment, especially if they violate the national sovereignty, security or public order of other States.

Fourthly, we strongly believe that the ICT environment must be used exclusively for peaceful purposes. To that end, the United Nations must continue its central role through the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies in order to develop legally binding obligations to prevent the use of ICTs for malicious purposes and maintain that domain for exclusively peaceful purposes.

The President: I now give the floor to the representative of Pakistan.

Mr. Akram (Pakistan): We thank the delegation of the Republic of Korea for convening this important debate on addressing evolving threats in cyberspace. I also wish to thank the Secretary-General and the other briefers for their insightful remarks.

The technologies and applications of information and communication technologies (ICTs) have contributed immensely to socioeconomic development. However, those technologies have also expanded the scope of conflict. Cyberwarfare has emerged as a new and important domain of warfare, encompassing information warfare and actual cyberattacks by State and non-State actors. Pakistan recognizes the gravity of the evolving cyberthreat landscape and its impact on international peace and security. We also recognize the urgent need to address other malicious activities in cyberspace, including ransomware and the theft of sensitive information.

Several countries, including Pakistan, are victims of disinformation. In its 2019 and 2020 reports, the EU DisinfoLab, an organization based in Brussels, uncovered the conduct of anti-Pakistan propaganda and disinformation activities and cyberwarfare against Pakistan. The 2019 report provided proof of 15 years of massive operations against Pakistan, involving more than 10 so-called non-governmental organizations fraudulently accredited to the Human Rights Council, more than 750 fake media outlets and 550 fake websites going so far as to even resurrect dead people. This was a systematic State-led campaign carried out to spread disinformation and misuse the United Nations, as well as European institutions, with the aim of maligning Pakistan. The exposé on that disinformation campaign, revealed by the EU Disinfolab, requires global attention. We must develop modalities to prevent such illegal and blatant misuse of cybertools to promote the narratives and objectives of hostile States.

In December 2021, the General Assembly adopted the Pakistan-sponsored resolution 76/227, entitled "Countering disinformation for the promotion and protection of human rights and fundamental freedoms" by consensus. The resolution affirmed the responsibility of States to counter the dissemination of disinformation that undermines the promotion of peace and cooperation among States. As a victim of continuing hostile cyberpropaganda and other propaganda, Pakistan remains committed to countering the virus of disinformation. We will promote action on this through international cooperation, including in the Security Council.

While we acknowledge the Security Council's important role in addressing specific cyberthreats that challenge international peace and security, we believe that the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies is best placed to promote international cooperation and consensus-based responses to the challenges posed and opportunities offered by the rapid advances in ICTs.

The Charter of the United Nations unequivocally urges universal observance of the principles of sovereignty, territorial integrity, the non-use of force and non-interference in the internal affairs of States. Those principles should serve as a guiding framework for cybergovernance.

However, the simple assertion that international law applies to cyberspace is not sufficient. Pakistan shares the view that it is essential to develop a legally binding international instrument tailored to the unique attributes of ICTs in order to provide a regulatory framework and a governance mechanism essential to a stable and secure cyberspace. Such a legal and institutional framework should address the concerns and interests of all parties and be negotiated within the United Nations with the equal participation of all States.

Appropriate confidence-building measures, such as the voluntary exchange of information and best practices, can contribute to increasing transparency and predictability in cyberspace and reduce the likelihood of misunderstandings and thus reduce the risk of conflict. The inauguration, last month, of the global points of contact directory for ICT security was an important step to promote trust and cooperation among States in the area of ICT security. We must build on such mechanisms and cooperation in order to establish enhanced cybersecurity and ensure the full utilization of ICT capabilities for economic and social development.

The President: I now give the floor to the representative of Uruguay.

Mrs. González (Uruguay) (*spoke in Spanish*): We welcome the Secretary-General's participation this morning, as well as the contributions of Chief Executive Officer of the CyberPeace Institute and the Professor of Law and Technology at Leeds Beckett University and Vice-Chair of the African Union Cyber Security Expert Group.

We consider the convening of this open debate by the current presidency of the Council, the Republic of Korea, to be very timely. This debate highlights the issue and enriches the dialogue and discussion on an issue that is pivotal to the international peace and security agenda and germane to many other issues in the Organization's purview. Uruguay supports this and other types of initiatives that seek to generate positive actions in the face of the devastating impact of the malicious use of information and communication technologies (ICTs) on global peace, security and stability.

There is no region or country that is exempt from this danger, which knows no borders. Most Member States have experienced an attack of this nature, making cyberspace an insecure place and further aggravating the scourges that afflict our societies, such as terrorism, drug trafficking, human trafficking and attacks on critical infrastructure, to mention a few.

We listened carefully to the Secretary-General this morning and agree that the dangers of armed digital technology are increasing. We also condemn the use of artificial intelligence as a threat multiplier in cyberspace, as well as the similar use of quantum technologies, which further enhance the capacity for harm.

Uruguay promotes a free, open and secure use of cyberspace that allows the development of the positive aspects of technologies and the use of the Internet — a positive approach that enables us to achieve the Sustainable Development Goals, to promote international trade and to continue to make scientific and medical advances that improve the welfare of our populations.

To that end, we must have concrete tools and safe regulatory frameworks that provide that security. However, in reality, not all countries and regions are in the same position to respond or to protect themselves from these cyberthreats due to their varied levels of development in the technologies that comprise cybersecurity.

In that context, we are concerned about the lack of significant progress in capacity-building and international cooperation. More than ever, developing countries need the transfer of technology, knowledge, good practices and equipment necessary to efficiently meet the challenges arising from the malicious use of ICTs.

In the adverse context created in cyberspace, the United Nations plays a fundamental role in international peace and security, which is a precondition for any kind of prosperity.

In that context, we highlight the role of the General Assembly through the First Committee. We value and support the work of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, as we did the work of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security in the past. Their work, which has generated recommendations and standardized norms on the responsible behaviour of States, has generated a common basis of understanding that serves as a reference and has constituted the main forum for discussion and debate. It is also the responsibility of States to apply those generated norms and foundations.

As technologies advance, organizations too must be dynamic. They must evolve and improve their institutional framework and governance through a permanent mechanism that allows them to address the challenges posed by these evolving developments. They must avoid duplication and eventually move towards mandatory rules for all States. Cyberspace is not exempt from international law and regulations, which is what affords us legal certainty.

We take this opportunity to mention the importance of the upcoming session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, also known as the convention on cybercrime. We hope that it can be adopted as soon as possible, and that the States develop national standards accordingly. We believe that this is a positive step that the Organization can take in that regard.

Finally, I would like to reaffirm the importance of strengthening of cyberresilience and capacity-building, which is a common denominator for most of the Organization, in which regional organizations play a key role. We value and appreciate the support of various countries that have cooperation programmes and promote the training of technicians and professionals who can tackle the challenges related to cyberspace, and we urge them to continue along that path, which will undoubtedly lead to a cyberecosystem that is more beneficial for all — one based on international cooperation, rather than confrontation or the politicization of these issues.

As in other areas, synergy between the Security Council and the General Assembly in addressing cyberthreats is critical. Periodic briefings and debates, such as this, are necessary to establish effective actions to combat the misuse of technologies in the entire sphere of international security, including in conflicts, thus also promoting the protection of civilians in aspects linked to cyberspace.

I thank you, Mr. President, for including this item on today's agenda.

Mrs. Janina (Albania): In today's digitalized world, cybersecurity emerges as a matter of importance to all Member States. We would like to thank the Korean presidency for convening this important discussion in the Security Council, and the briefers for their useful inputs.

Many of us have had to face some form of cyberattack. We have seen these malicious activities not only affect the daily lives of our citizens, but also, more broadly, impact the international community as a whole and directly endanger international peace and security. The increasing number of cyberattacks has a significant effect in reducing countries' gross domestic product in various regions, with developing countries being the most vulnerable.

With cyberthreats becoming more complex and varied, our responses should be agile. We should be equipped to develop such responses and mitigate the cyberthreats we face, individually and collectively, by facilitating international cooperation and information-sharing. Two years ago, Albania became the target of an unprecedented heavy cyberattack by multiple hacker groups linked to the Islamic Republic of Iran, with the clear aim of destroying the governmental infrastructure, paralysing public services and sowing chaos and insecurity in the country. We continue to be the target of sophisticated cyberattacks.

In that context, Albania is investing in its national cyberresilience, while paying significant attention to regional and international approaches to cybersecurity. Our region, the Western Balkans, continue to face a growing number of cyberthreats that continue to evolve. We are working to build cybercapacity in the region through programmes in cybersecurity, cybercrime and

cyberdiplomacy. The regional summit on cybersecurity, which will be held in July in my country, Albania, will seek to foster greater cyberresilience in the Western Balkans.

We strongly believe that more could and should be done at the international level.

In that context, I would like to underline three elements.

First, the Security Council, as the main organ for maintaining international peace and security, could and should become more engaged. This is a valuable platform to discuss cyberthreats and ways to address them. The discussions should be inclusive and open to different actors. In that regard, we see added value in collaboration between governments and the private sector for stronger defence against cyberthreats.

Secondly, the accountability process towards maligned State and non-State actors should become more present in our joint efforts for a secure cyberspace. That goes hand in hand with respect for international norms of responsible behaviour in cyberspace.

Thirdly, there is a need to strengthen capacity-building. While developed countries have a robust and solid cyberposture, many developing countries lack the resources and expertise to address cyberthreats. That could lead to dangerous exposure of critical infrastructure, cyberattacks, cyberespionage and other destructive activities.

In conclusion, let me reiterate once again that a secure cyberspace is possible only by joining efforts at the global level, and this meeting is a step in the right direction.

The President: I now give the floor to the representative of Greece.

Mr. Sekeris (Greece): First of all, I would like to thank the Republic of Korea for organizing this very important high-level discussion, and I would like to thank our briefers for their very interesting remarks.

Greece fully aligns itself with the statement made earlier by the representative of the European Union delegation and would like to make the following remarks in its national capacity.

The digital evolution of our times has been a catalyst for human progress, transforming our societies and economies and expanding opportunities for cooperation. Emerging technologies provide humankind with significant opportunities for economic growth, as well as sustainable and inclusive development, affecting all three pillars of the Organization's work: peace and security, human rights and sustainable development.

And as our economies, democracies, and societies depend more than ever on secure, reliable and increasingly interconnected networks and information systems, cybersecurity has become essential for building a global, open, free, stable and secure cyberspace.

At the same time, the malicious exploitation of those technologies has become a source of new risks and challenges. Malicious behaviour in cyberspace has intensified in recent years, including a sharp and constant surge in cyberattacks targeting critical infrastructure, supply chains and intellectual property, as well as a rise in ransomware attacks against governments, organizations, businesses and citizens.

Moreover, what is even more alarming is that cyberattacks are becoming an integral part of operations during armed conflicts. Greece has expressed its deep concern about such activities, which undermine international peace and security and could lead to destabilizing and cascading effects, with enhanced risks of conflict.

Yet cyberspace is not a lawless domain. As part of what is known as the framework of responsible State behaviour in cyberspace, all States have agreed that existing international law and, in particular, the Charter of the United Nations, is applicable and essential for maintaining peace and stability. International law must be upheld and enforced in this domain in the same way that it applies to all other domains of international relations.

As the Security Council bears the primary responsibility for maintaining international peace and security, we hope that in future it will adopt a more active role in matters that involve emerging and contemporary threats. Such a role can include efforts to reinforce the aforementioned framework of responsible State behaviour and respond to cyberactivities inconsistent with the objectives of maintaining international peace, stability and security.

As a staunch supporter of the primacy of international law and the peaceful settlement of disputes, we reaffirm our aspiration to a peaceful and secure cyberspace, and we are fully committed to further discussions on this

very important topic, including during our tenure as a non-permanent member of the Security Council for the 2025-2026 term.

The President: I now give the floor to the representative of Spain.

Mr. Gómez Hernández (Spain) (*spoke in Spanish*): I welcome the convening of this open debate. As a strong advocate and active contributor to the maintenance of international peace and security, Spain reaffirms its commitment to combating cyberthreats and to promoting the responsible behaviour of States in cyberspace through regional and international collaboration within the framework of the responsible conduct of the States Members of the United Nations.

While the rapidly changing nature of threats forces us to adapt the approach and tools to address them in a joint and integrated manner, the key to global and national cyberresilience remains the implementation of more and better cybertools that ensure the protection of critical infrastructure around the world.

Some of the most worrisome trends are the proliferation of data hijacking, especially against critical infrastructure; the manipulation of information and perception through digital technologies; and attacks on international supply chains that exploit various vulnerabilities and result in economic losses.

The very concept of conflict has evolved with the emergence of hybrid strategies, grey zones and asymmetric warfare. The sharp distinctions between war and peace are, in some cases, no longer valid. The malicious use of information and communications technologies (ICTs) is now an integral part of a complex and changing landscape of tools used to gain advantage in conflict. There is an urgent need to adopt a broader perspective in order to address contemporary conflicts in a comprehensive manner.

Therefore, any possible international mechanism or commitment related to information and communication technologies should be based on consensual agreements on the framework for responsible conduct of States in relation to ICTs and be produced through an open, inclusive and transparent process.

The President: I now give the floor to the representative of Portugal.

Mr. Vinhas (Portugal): I would like to commend the Republic of Korea for today's debate and to align myself with the statement delivered by the representative of the European Union earlier today.

As the guarantor of international peace and security, the Security Council must be able to address current, emerging and future threats. The fact that we are debating the issue of threats in cyberspace shows that, when prompted, the Council can adapt in the face of new challenges.

Hostile cyberactivity and operations have proved to be the most serious challenge to the prosperity ushered in by digital transformation. They have also proved to be a serious challenge to the integrity of our institutions and to the trust our citizens place in them. More worrisome still is the fact that the impact of cyberinsecurity on the physical world cannot be underestimated.

The increasing offensive capabilities of hostile cyberactors has led to growing costs to prevent and recover from their attacks. The role of cybercriminal groups, in particular, has increased the complexity of the cyberthreat landscape. Following the disruptive attacks of alleged ransomware groups in 2022, Portugal joined the International Counter Ransomware Initiative. It is worth noting that ransomware is also increasingly used by State-sponsored actors as a cover for the pursuit of strategic objectives.

Artificial intelligence has emerged as a great leveller of capabilities across multiple threat actors, providing unsophisticated operators with a new degree of possibilities and potentially increasing the scope of attacks. In the face of that threat landscape, we trust that the future United Nations convention to combat cybercrime will soon be finalized and able to promote international law enforcement cooperation. Such cooperation against cybercrime perpetrated by State-sponsored actors will, in turn, facilitate the implementation of the United Nations framework of laws, norms and confidence-building measures for responsible State behaviour in cyberspace.

Capacity-building also plays an essential role, and Portugal intends to launch an annual digital capacity-building programme for developing countries, in partnership with the United Nations University. The future permanent institutional mechanism, or programme of action, to be implemented from 2026 onwards, is also expected to contribute to bridging the digital divide.

The Council has an important complementary role to play, while preserving the role of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies (ICTs) as the main platform for deepening our understanding of threats, norms and laws, but also for promoting capacity-building and confidence-building among States.

First, the Security Council could reaffirm the set of norms of responsible State behaviour agreed to by consensus in the Open-ended Working Group, for instance by issuing a presidential statement to that effect. That measure alone would provide an important recognition of the impacts that cyberthreats can have on international peace and security.

Secondly and lastly, the Security Council could also attempt to integrate ICT-related concerns into its relevant mandates, where appropriate. Building resilience of critical infrastructure against hostile cyberactivity can, in certain contexts, contribute decisively to increasing stability in the long term.

The President: I now give the floor to the representative of El Salvador.

Mrs. González López (El Salvador) (*spoke in Spanish*): I would like to thank the Republic of Korea for convening this relevant debate on the evolving threats we face in cyberspace.

As my delegation has noted on other occasions, the threats associated with the use of information and communication technologies (ICTs) in the context of international security continue to evolve in scale and intensity. Those threats, associated with the misuse of emerging technologies, such as artificial intelligence or quantum computing, can generate new attack vectors, resulting in the exploitation of vulnerabilities in ICT systems. Due to the increasing connectivity of digital infrastructure in all areas of governance — social, economic and political — we could see cascading effects whose impacts are difficult to predict.

Malicious activities in the ICT field can have disruptive effects that transcend the international threshold of peace and security. Likewise, they could cause direct harm to civilians, particularly when such attacks are carried out against critical infrastructure necessary for social functioning, such as public health systems or basic services like water and energy supplies and transportation systems, or when they disrupt or impair the functionality and availability of the Internet.

My country believes that this organ, the Security Council, should more systematically and proactively address cyberthreats to peace and security as part of its mandate and responsibility to maintain international peace and security. That could be done through specific discussions, with concrete results related to the protection of critical infrastructure and critical information infrastructure; detection of, response to, and recovery from cybersecurity incidents; and a cross-cutting vision of cybersecurity capacity-building, among other issues.

In addition, consideration could be given to the possibility of including an item on the Council's thematic agenda to address threats to peace and security arising from the digital domain, including ICTs and other emerging technologies, such as artificial intelligence, to complement the efforts being made in the framework of the General Assembly and other subsidiary bodies.

It is also important to point out the need to further address the impact of digital technologies on the protection of civilians and civilian objects in armed conflicts, including the application and full respect for the principles of international humanitarian law in the digital domain. We believe that the increase and impact of disinformation, the spread of misinformation and hate speech through digital platforms are issues that also deserve the Security Council's attention.

In the interest of time, the full statement will be available through the Secretariat.

The President: I now give the floor to the representative of Bulgaria.

Ms. Stoeva (Bulgaria): Bulgaria aligns itself with the statement made on behalf of the European Union. I would like to highlight a few points in my national capacity.

We commend the Republic of Korea for organizing today's high-level debate and for bringing this important topic to the attention of the Security Council. We would like to thank the briefers for their extremely informative and insightful presentations.

The issue of evolving threats in cyberspace is of growing importance for the security and stability of our societies. Today, cyberspace is increasingly exploited for political and ideological purposes, and increased

polarization at the international level is hindering effective multilateralism.

As illustrated by the briefers, some of the greater risks we face from malicious cyberuse are the empowered disinformation campaigns that attempt to exploit societal vulnerabilities, undermining democratic processes and institutions, sowing mistrust and ultimately weakening societies. In addition, the malicious targeting of critical infrastructure and essential services constitutes a major global threat as well. All those activities erode international security and stability and the benefits that cyberspace brings for economic, social and political development.

While national security, including cybersecurity, remains a national government prerogative, the potential cross-border impact of cyberincidents suggests a need for joint efforts. For that reason, it is important to enhance cooperation on cyberissues at the international level. And while the effective multilateral debate on international security in cyberspace is generally deteriorating owing to geopolitical tensions, there is a clear need for the Security Council to take a more proactive stance on the issue.

Bulgaria is of the view that international security and stability depend on a global, open, stable and secure cyberspace in which international law, in particular the Charter of the United Nations, is respected and the voluntary non-binding norms, rules and principles of responsible State behaviour are adhered to. To that end, international cooperation is essential. That is why enhancing the Security Council's role in addressing cyberthreats is critical. Proactive engagement on cybersecurity, aligned with its primary responsibility to maintain international peace and security, makes the Council well positioned to respond to malicious cyberactivities.

The interconnected nature of cyberspace requires all stakeholders to exchange information on and assume their specific responsibilities with regard to cyberspace in order to maintain a global, open, stable and secure cyberspace. A multi-stakeholder approach is thus vital to properly address the evolving threats in cyberspace. States and international institutions, including the Security Council, should seek to reinforce regular and structured exchanges with all stakeholders, including the private sector, academia and civil society. That is the way to also promote and advance prevention, preparedness, resilience and responsiveness in cyberspace.

Lastly, it is worth noting that the level of cyberresilience and the ability to detect and respond to malicious cyberactivities vary significantly across countries in terms of capacity and maturity. For that reason, it is necessary to improve the overall level of cybersecurity through capacity-building and establish common standards for cybersecurity, especially for critical infrastructure, as well as for the development and application of new technologies.

The President: I now give the floor to Ms. Andriani.

Ms. Andriani: It is my honour to address the Security Council today on a critical issue: the misuse of modern technologies and growing threats to cyberspace.

Cybercrime is a threat multiplier, enabling other forms of criminality, worsening global shocks and undermining sustainable development, peace and security.

INTERPOL supports this open debate and will make three points with regard to strengthening the global security architecture against cyberthreats posed by criminal non-State actors.

First, we must enhance our understanding of the modern cyberthreat landscape, which to this day remains fragmented across regions and sectors. In that regard, INTERPOL has developed a Gateway model to facilitate access to industry data as complementary to information-sharing among member countries. On our I-24/7 platform, we connect 196 member countries, enabling secure police information exchange globally. Additionally, we offer tailored cybercrime platforms for the exchange of best practices and analytical purposes. Furthermore, our 24/7 points-of-contact list and regional working groups facilitate rapid responses in urgent cases and build trust among agencies. By working together and leveraging existing and established mechanisms for information exchange, we can make significant strides in protecting cyberspace and ensuring global security.

Secondly, we must bridge gaps in capabilities. There remain significant disparities in cyberresilience. INTERPOL supports member States in overcoming the digital divide by providing technical assistance and capacity-building. We seek to equip law enforcement with the knowledge and skills needed to face today's cyberchallenges.

Thirdly, we must maximize synergies through regular institutional dialogue and multilateral mechanisms. Let us remember — collaboration, not duplication, is key. That is why INTERPOL actively participates in various cyberprocesses within and beyond the United Nations, including the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Cyberthreats know no borders, and neither should our defences. INTERPOL remains committed to ensuring a safer cyberworld for all through collaboration, innovation and endless dedication.

The President: I now give the floor to the representative of India.

Mr. Raguttahalli (India): I congratulate the Republic of Korea on its assumption of the presidency of the Security Council for the month of June. I welcome this initiative of an open debate on "Addressing evolving threats in cyberspace". I also thank the Secretary-General and the representatives of civil society for their insights.

Today's world is of a digital age. Digital transformation has transcended all conventional geographical, political and economic boundaries. With the rapid advancements and adoption of new and emerging technologies such as artificial intelligence, our lives have become increasingly intertwined with the digital realm. In the interconnected world, from personal communication to critical infrastructure, the reliance on cyberspace is profound.

The digital transformation has also exposed us to a myriad of cyberthreats. Cyberattacks against critical infrastructure, information and financial systems, and government networks are increasing in frequency and sophistication. Cryptocurrency heists, data hijacking, deep fakes, misinformation and incitement are commonplace now. Further, the potential of artificial intelligence to add scope and scale to cyberattacks is also notable.

The integrity and security of information and communications technology (ICT) products, which form the building blocks of cyberspace, are being compromised. Those acts are committed by both State-sponsored and non-State actors, as well as transnational crime networks. Such nefarious acts undermine trust and confidence in global ICT supply chains, compromise security and create potential flash points between States. According to World Bank estimates, cyberattacks could have caused losses of approximately $5.2 trillion to the world from 2019 to 2023.

Terrorists are also finding new ways through cyberspace to perpetrate violence; radicalize youth; undertake recruitment; conduct training and raise financial resources. New methods in the form of virtual assets and cryptocurrency are becoming a norm in financial transactions by terrorists. Terrorism is exploiting new channels and new funding methods from the cyberworld, making it a critical issue for the security and prosperity of every nation. India has been a victim of terrorism for several decades, and it is cognizant of the serious nature of the cyberterrorism challenge.

In that context, let me highlight four points.

The threats in cyberspace have the potential to not only jeopardize national security but also to undermine the very fabric of global stability and cooperation. No single country or organization can combat cyberthreats alone — it requires a united front.

There is a growing need for international instruments to address threats from cyberspace. Current international law is not well positioned to support responses to cyberattacks. Cyberattacks against critical infrastructure, information and financial systems and government networks should be treated as terror attacks. The applicability of existing anti-terrorism treaties to the cyberdomain should be considered. The international community should ensure uniformity in counter-terrorism crime laws. Global cooperation in that area will help to harmonize cybersecurity benchmarks, best practices and regulations.

India has been participating in United Nations-mandated cyberprocesses and consultations that support global, inclusive and transparent intergovernmental participation with the objective of realizing a safe and secure cyberspace. We believe multi-stakeholder collaboration is essential to be informed of and understand the emerging threats in cyberspace.

In conclusion, India is among the world's leaders in advancing digital technology, connectivity and resilience. India is committed to an open, secure, free,

accessible and stable cyberspace environment. India will continue to work with the global community to tackle cyberthreats and ensure that the digital revolution continues to benefit humankind without compromising its collective well-being and stability.

The President: I now give the floor to the representative of Cambodia.

Mr. Mao (Cambodia): At the outset, I wish to express my appreciation to you, Mr. President, for convening today's high-level open debate, which allows Member States to share their perspectives on cyberspace, as cyberthreats are becoming a growing concern for every country. I also thank His Excellency António Guterres, our briefers and the speakers for their insightful remarks.

There is no denying that our world is now deeply reliant on digital technologies. The rapid advancement of information and communication technology (ICT) has brought immense possibilities, but it also exposes us to new and evolving risks that threaten international peace and security. The recent rise in cyberattacks has demonstrated that ICT systems are more vulnerable than ever.

In that regard, Cambodia is committed to fostering a secure digital environment for all. We are leveraging our Association of Southeast Asian Nations (ASEAN) platform to facilitate capacity-building programmes and promote the exchange of best practices. We firmly believe in the power of international cooperation and urge the global community to provide technical assistance and knowledge-sharing to enhance cybersecurity, particularly in developing countries.

At the national level, Cambodia took decisive action by establishing the Digital Security Committee earlier this year. That Committee, comprised of relevant ministries, is leading our efforts in cybersecurity, cybercrime prevention, cyberdefence, and cyberdiplomacy. That coordinated approach allows us to assess our needs, address skill gaps and implement effective strategies to protect our digital infrastructure.

Cambodia values the importance of cybersecurity capacity-building. Last month, our Minister of Post and Telecommunications actively participated in the Global Round table on ICT Security Capacity-building. We commend the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, chaired by Singapore, for its tireless efforts in promoting international dialogue and cooperation on that critical issue.

Moreover, Cambodia advocates robust legal frameworks and international norms that promote responsible behaviour in cyberspace, uphold national sovereignty and prevent malicious actions. Collaboration between governments, businesses and civil society is vital for sharing information and developing innovative solutions. We also prioritize education and awareness initiatives to empower our citizens with the knowledge and skills needed to navigate the digital world safely.

In conclusion, Cambodia is dedicated to working with all nations to build a secure and resilient digital future. We reaffirm our commitment to cooperation and collaboration in pursuit of a stronger, safer and cyberresilient future for all. My delegation believes that together we can create a cyberspace that fosters innovation, economic growth and the well-being of all our citizens.

The President: I now give the floor to the representative of Brazil.

Mr. França Danese (Brazil): I thank the Republic of Korea for convening this meeting.

As we stated during the Arria formula meeting in April, organized by the Republic of Korea, Brazil shares with many other delegations the concern about the evolving cybersecurity threat landscape. We are also in agreement on the need for multilateral solutions that can improve cyberresilience for all.

We remain convinced, however, that the best way to achieve that goal is to keep our discussions inclusive, without duplicating existing work. While we appreciate the Republic of Korea`s genuine efforts in seeking broader formats for discussions in the Security Council, both through the Arria formula format and through this open debate, we believe that the right forum for these discussions continues to be the General Assembly.

This year, we saw the limitations of the Council`s ability to set rules for new domains when it twice failed to adopt a draft resolution on weapons in outer space (see S/PV.9616 and S/PV.9630). On both occasions, delegations raised concerns about bringing to the Council complex issues that are best addressed by the full United Nations membership. Those concerns are valid and apply here, too.

The ongoing Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies has a mandate to debate that very topic and has been productive in identifying cyberthreats. It has highlighted ransomware and cryptocurrency threats, as well as other vectors of attack, including upon critical infrastructure. It has debated the spillover effects of cyberattacks and discussed how to guard and differentiate systems that are of particular humanitarian importance. It has clarified the applicability of international law and international humanitarian law to cyberspace. It is currently discussing concrete measures for implementing the framework for responsible State behaviour in cyberspace. Those are significant achievements, which illustrate the viability and importance of holding these debates in the appropriate forum.

That is not to say that the Council has no role to play. Consistent with its powers and functions under the Charter of the United Nations, this organ may respond to specific and concrete cyberincidents that constitute a threat to international peace and security.

In an era when progress in disarmament has almost stalled, the area of cybersecurity stands out as a result of the significant progress achieved in the General Assembly. Let us work to sustain that momentum.

The President: I now give the floor to the representative of Guatemala.

Ms. Rodríguez Mancia (Guatemala) (*spoke in Spanish*): Guatemala would like to thank the Republic of Korea, in its capacity as President of the Security Council, for convening this important open debate.

My delegation recognizes that cyberspace has become a central and indispensable domain for global activity and, because of its civilian and dual-use nature, has been used by criminal and terrorist groups on more than one occasion. That has led to an increase in the exploitation of and cyberattacks on critical infrastructure, in which electricity grids, transportation systems, hospitals, schools, among others, are affected, which has a devastating impact on people's lives and the economy. Globally interconnected networks and the digitization of the global economy have opened a space in which cybersecurity breaches can pose significant economic and international security threats.

Malicious activities in cyberspace can be a conflict multiplier in a number of ways. They can intensify tensions between States by enabling covert attacks with plausible deniability, complicating attribution and fostering mistrust. In addition, State and non-State actors can use cyberspace for propaganda, disinformation and espionage, sowing internal divisions and fuelling internal and transnational conflicts.

Moreover, it is undeniable that artificial intelligence (AI) represents a very important opportunity to contribute to progress for humankind, ranging from preventing and addressing crises, to implementing health-care and education services, expanding the work of governments, civil society and the United Nations in all areas. However, the malicious use of AI can undermine trust in institutions, weaken social cohesion and threaten democracy. In the light of the aforementioned, my delegation sees the need to reinforce existing efforts, first, towards prevention and, secondly, to confront existing and potential threats.

Some steps have already been taken to integrate cybersecurity issues into the programmes of work of this Organization. However, it is necessary to reinforce, with forceful actions, the efforts to effectively add those issues to the agenda of the Security Council. Examples of such actions include establishing a mechanism for imposing sanctions to regulate behaviour in cyberspace; increasing assistance to States to strengthen their cybersecurity capabilities and continuing to work with the private sector and civil society to develop robust strategies to control information and communication technology.

The Security Council must exercise greater leadership in combating cyberthreats that undermine international peace and security.

The President: I now give the floor the representative of Belgium.

Mr. Kridelka (Belgium): At the outset, allow me to wholeheartedly thank the Republic of Korea for organizing this meeting.

I have the honour to deliver this statement on behalf of the Benelux countries — Luxemburg, the Kingdom of the Netherlands and my own country, Belgium. The Benelux countries align themselves with the statement made of behalf of the European Union. And we would like to underline four additional points.

First, on the threats, as previously noted in the Council, the Benelux countries remain deeply concerned over the increasing and evolving threat of malicious

cyberactivities. That threat continues to rise in scale and may be further exacerbated by emerging technologies, including artificial intelligence and advances in quantum computing. One worrisome trend we observe is the increase of ransomware attacks, the use of ransomware-as-a-service and malicious cyberthreats, targeting critical infrastructure, including the health and education sectors, and electoral processes. The effects of such incidents and the risk of spillover effects are a threat to international peace and security.

That brings me to my second point. Under the First Committee of the General Assembly, we all adopted by consensus the United Nations framework for responsible State behaviour in cyberspace. The framework confirms that international law, in particular the Charter of the United Nations, applies to cyberspace. The implementation of the framework remains fundamental to addressing existing and potential information and communications technology-related threats to international security. In that regard, the Benelux countries support the establishment of a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. Other relevant United Nations processes include the development of a United Nations convention to combat cybercrime.

In addition — and this is my third point — under Chapter VI of the Charter of the United Nations, the Security Council has a clear role in the peaceful settlement of disputes, including in the cyberdomain, by calling upon parties to settle any dispute likely to endanger the maintenance of international peace and security. As Benelux countries, we are of the view that the Council has an important role in promoting an open, free and secure cyberdomain. We therefore welcome the Council's increasing attention to cybersecurity, as witnessed by the rising number of meetings held on cyberissues since 2016. Ongoing conflicts demonstrate that the cyberissue is inherently part of broader threats to international peace and security. Therefore, the Benelux countries also endorse your suggestions, Mr. President, on mainstreaming cyberissues into existing work by the Council.

Finally — and this is my fourth point — the Benelux countries are calling for more attention to the victims of cyberoperations. While often viewed through a lens of geopolitical competition, malicious cyberactivities have devastating effects on people, severely curtailing their human rights. Therefore, in order to keep human well-being and dignity at the forefront of our discussions, we call for a victim-centred approach.

And let us not forget the significant protection risks posed by digital transformation, including in cyberspace, to people affected by humanitarian crises. We see the International Committee of the Red Cross, including through its Global Cyber Hub, based in Luxembourg, at the forefront of addressing some of those challenges, for instance, by developing and testing new tools for providing digital services to affected populations in a neutral, impartial and independent manner.

We, the Benelux countries, thank you, Mr. President, again for organizing this debate, and we applaud your efforts to raise awareness and address the importance of cyberthreats.

The President: I give the floor to the representative of Norway.

Mr. Løvold (Norway): I have the pleasure to speak on behalf of the Nordic countries: Denmark, Finland, Iceland, Sweden and my own country, Norway.

Let me start by thanking the Republic of Korea for taking the initiative to organize this timely meeting. It is only the second time the Council officially addresses the important topic of cybersecurity.

Developments in the cyberthreat landscape have been worrisome since the Council first discussed the issue under the Estonian presidency in 2021 (see S/2021/621).

Let me quickly highlight three kinds of threats.

First, the threat from State-sponsored cyberaction has continued, most notably in the context of Russia's illegal war of aggression against Ukraine. Russia's cybercapabilities have been weaponized in Ukraine in an attempt to undermine trust in authorities and to destroy critical infrastructure. We continue to place importance on Ukraine's cyberdefence, as well as on protecting our own societies from malicious actors. In that context, we would like to again underline that international law applies also in cyberspace.

Secondly, the blurring of lines among State-sponsored, non-State and criminal actors has continued to grow. Key concerns include the increasing number of ransomware attacks and the accessibility of advanced cybertools and techniques to a broader range of both State and non-State actors.

Finally, linked to all of those threats, a particular concern is the increasing targeting of critical sectors and infrastructure by malicious actors.

In responding to those threats, the Nordic countries would particularly like to highlight the importance of multi-stakeholder engagement on cybersecurity. We must strive for stronger coordination between governments and all relevant stakeholders, including civil society, academia and the private sector. With their access to information, the private sector plays an essential role in cyberspace, as the tech and cybersecurity companies have a key role in forecasting and responding to threats. It is important to better leverage relevant stakeholders' knowledge and capabilities in support of a free, open, peaceful and secure cyberspace.

In the light of the evolving threat landscape, the Nordic countries see increasing benefit in the Security Council discussing cybersecurity more regularly. Discussions in the Security Council on current and emerging cyberthreats during thematic and country-specific discussions can help raise awareness of the threats, share lessons learned and formulate appropriate responses.

The Council's work also complements discussions in other forums. With that in mind, and in conclusion, I would like to reiterate the support of the Nordic countries for the establishment of a programme of action on cybersecurity as a permanent, inclusive and action-oriented mechanism to advance responsible State behaviour in that domain.

The President: I now give the floor to the representative of Croatia.

Mr. Šimonović (Croatia): I thank you, Mr. President, for organizing this timely open debate, and I thank the briefers for their input.

Croatia aligns itself with the statement made by the representative of the European Union, and I would like to make a few remarks in my national capacity.

We face a rising number of increasingly sophisticated cyberthreats. Those include ransomware attacks targeting critical infrastructure, persistent campaigns and foreign interference in democratic processes, just to name a few. Each of these activities have the potential to destabilize governments, in particular, and peace and security, in general.

In conflict zones, cyberoperations can amplify the effects of conventional warfare, especially when targeting critical infrastructure, leading to escalated hostilities and greater civilian harm. In that regard, we commend the International Committee of the Red Cross for its work in highlighting that cyberspace is not a lawless domain, and we affirm that international humanitarian law applies equally in both physical and cyberrealms.

That is why the Security Council should consider further developing its understanding of this highly complex matter, not only through regular exchanges with multi-stakeholders in the field of cybersecurity, but also in peacebuilding, as well as in conflict prevention and mediation efforts. That could be achieved through regular briefings and reports on cyberthreats, ensuring that both the Council and Member States are informed of the latest developments and trends.

Furthermore, the role of the Security Council in addressing cyberthreats could develop in a mutually reinforcing and complementary manner, alongside the existing work of other United Nations bodies and multilateral initiatives. That involves the work of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies and other relevant and future frameworks, ensuring a coordinated and comprehensive system-wide approach. The Council could also explore its contribution to de-escalating tensions by promoting dialogue and confidence-building measures between States, reducing the risk of cyberconflicts escalating into armed confrontations.

By taking proactive steps to understand and mitigate cyberthreats, promote international cooperation and integrate cyberconsiderations into its broader mandate, the Council could assume an important role in the existing United Nations cybersecurity ecosystem and better safeguard international peace and security in the digital age.

The President: I now give the floor to the representative of Chile.

Mrs. Narváez Ojeda (Chile) (*spoke in Spanish*): We appreciate the opportunity to participate in this open debate. We take note of the presentations and contributions heard today by the speakers. We take this opportunity to congratulate the Republic of Korea on its presidency of the Security Council this month.

As we have stated on previous occasions, Chile believes that cyberattacks and malicious activities in cyberspace constitute a threat to international peace and security and can affect States in various ways, depending, in part, on their levels of digitization, capabilities, security, infrastructure and development. In particular, we highlight that these threats can also affect various groups and entities differently, especially women, girls, boys and adolescents.

Regarding emerging and evolving trends in malicious activities in cyberspace, we note the use of artificial intelligence and machine learning, the combination of various attack vector tactics, supply chain attacks that compromise the integrity of products and services and attacks on Internet of things devices, among others.

We also note the risk posed by malicious software such as ransomware, wipers and Trojans, along with techniques such as phishing and distributed denial-of-service attacks. In the hands of malicious actors, those threats can wreak great havoc on the functioning of countries and affect both their economies and their people's well-being.

We therefore believe that it is essential to strengthen joint work and cooperation among States. That includes the exchange of experiences and lessons learned, the implementation of existing norms of responsible behaviour of States in cyberspace, the application of international law and international humanitarian law, confidence-building measures and capacity-building, all of which help to reduce mistrust among States and contribute to stability in cyberspace. Chile promotes the aforementioned, and notes that all related debates and discussions should include all interested parties, such as civil society, academia, the private sector, the technical community, among other relevant actors.

We stress the importance of strengthening the role of the Security Council in addressing cyberthreats and believe that it can contribute significantly to the establishment of a secure, open and peaceful cyberspace for the benefit of all nations. Chile attaches great importance to this particular issue, since malicious actors take advantage of the vulnerabilities of countries that lack the necessary tools and training to deal with such threats.

In that sense, the Council could be an invaluable tool to generate spaces for dialogue and cooperation in terms of capacity-building and technical assistance, which could benefit the countries that need it most. We call for this organ to address the challenge of the evolving cyberspace threat landscape, together with international cooperation, which we believe should be a matter of consensus.

The President: I now give the floor to the representative of Nepal.

Mr. Thapa (Nepal): At the outset, I wish to thank the presidency of the Republic of Korea for convening this open debate. I would also like to commend the briefers for their insightful and invaluable contributions.

Rapid advancements in information and communication technologies and artificial intelligence have revolutionized our lives, providing unprecedented opportunities to accelerate social and economic development. Our reliance on technology has been ever growing. Yet, its misuse has created new and serious threats. We are concerned about the surge of cases of ransomware attacks, cybercrime, and the spread of misinformation and hate around the world.

No infrastructure or system is immune from cyberattacks — be it civilian infrastructure, such as financial institutions, hospitals, transportation, water or energy supply systems, or the military command-and-control system of nuclear weapons or autonomous weapon systems. That poses challenges to international peace, security, stability and development.

We in Nepal have also been facing the immense challenges of this menace, as banking institutions, government websites, and servers in Nepal have suffered cyberattacks and ransomware attacks from time to time.

In that context, let me highlight a few points.

First, we need to implement a robust set of rules based on the accepted norms of international laws, including the Charter of the United Nations, while ensuring cyberspace's openness, stability and security. We should develop a common understanding of the application of rules and promote confidence-building measures in cyberspace, as well as in advancing responsible State behaviour in cyberspace.

Secondly, we must hold regular briefings and assessments incorporating insights from technology-led companies, the private sector, civil society and academia, sharing their knowledge and best

practices on how to keep us prepared for the evolving cyberthreat landscape.

Thirdly, countries like Nepal are more vulnerable to such emerging threats. The lack of adequate legal and regulatory frameworks, limited human capacity and financial resources are among the challenges we face to prepare ourselves to prevent and respond to those threats. Sustained international support and assistance are therefore critical to enhancing the capacities of countries like Nepal so as to enable them to prevent and respond to cyberattacks. We need to advance multi-stakeholder partnerships in order to bridge institutional, skill, capacity, technology and resource gaps.

Fourthly, we should promote cybersecurity through inclusive development and prosperity for all by bridging digital divides among States.

In conclusion, the cyberthreats we face are significant. By taking proactive, comprehensive and coordinated actions, we can ensure a secure, open, and peaceful cyberspace for all. As we move ahead with our agenda of a sustainable and digital future for all, we must together build a resilient global community capable of withstanding and overcoming the threats of the digital age.

The President: I now give the floor to the representative of Bangladesh.

Mr. Muhith (Bangladesh): I thank the Republic of Korea, the current President of the Security Council, for convening this important open debate. I also thank the briefers for their insightful presentations.

In the evolving digital landscape, cyberthreats have become pervasive and often imminent, disrupting global financial, democratic, sociocultural and security structures. The Global Risks Report 2024 underscores cyberthreats as one of the most serious challenges of our time, estimating potential cybercrime costs of $24 trillion by 2027. Such an astounding figure demands our immediate and urgent action. But beyond the cost in economic terms, the appalling impact of cybercrime on individuals and societies cannot be underestimated.

To address the President's guiding questions, I would like to highlight several points.

First, the proliferation of cyberthreats, including ransomware attacks, cyberespionage, and misinformation and disinformation campaigns through deep fakes and other means, poses significant risks to global peace and stability. These threats target critical infrastructure and undermine democratic processes and societal harmony by spreading xenophobia, intolerance and stereotypes. Additionally, advancements in artificial intelligence and quantum computing have magnified the scope and complexity of cyberthreats. With billions relying on digital platforms for daily activities, the urgency to address those threats has reached an unprecedented level.

Secondly, we firmly believe that, in the face of such grave threats, we are only as strong as our weakest link. Enhanced international cooperation and coordination are therefore indispensable today. Strengthening cybersecurity measures, fostering information-sharing mechanisms and investing in capacity-building initiatives are imperative to bolster resilience against cyberthreats. In that regard, we emphasize the importance of upholding the principles of sovereign equality and international law in the digital domain. We must find ways to balance freedom of expression with the need to combat the harmful dissemination of misinformation.

Thirdly, in this rapidly evolving cyberlandscape, we commend the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies on facilitating vital international discourse and collaboration. The General Assembly, reflecting the global will and aspirations of the international community, remains the key platform for such critical discussions, enabling all States to actively participate in shaping our collective cyberfuture. We also hope that the ongoing Global Digital Compact will play a critical role in addressing this issue, and we advocate a collaborative approach between the General Assembly and the Security Council for the Compact's effective implementation.

Finally, turning to the issue of whether or not addressing evolving threats in cyberspace falls under the purview of the Council, since it is not a part of the traditional concept of security, we believe that, owing to the emerging threats this matter poses to peace and security, cybersecurity deserves the highest attention of the United Nations. The right platform to address this crucial issue needs to be determined through open and transparent dialogues, rather than having it become yet another area of divergence and polarization.

In the meantime, we think the Council could play a vital role in fostering confidence-building measures, including through effective information-sharing and exchange of views. We must work together, be it under the auspices of the Council or in any other appropriate forum in the United Nations including the Open-ended Working Group, to develop norms, standards and regulations that promote a safe, secure, non-discriminatory and stable digital environment for all. Bangladesh reaffirms its commitment to collaborating with the global community to address the evolving global cybersecurity threat landscape.

The President: I now give the floor to the representative of Viet Nam.

Mr. Dang (Viet Nam): Threats in cyberspace have continuously evolved both in scale and complexity, presenting substantial challenges to international peace and security. Those threats range from malicious cyberactivities, including espionage, attacks targeting critical infrastructure and data breaches; to misinformation, disinformation and cyberpsychological warfare. Such activities can pose significant risks to national security, cause substantial economic damages and undermine public trust in institutions.

No country is immune from these threats. Developing countries, in particular, which often lack robust cybersecurity capabilities, are undoubtedly the most vulnerable and, sometimes, used as testing grounds for nation-State cyberwarfare, as well as for cybercrime committed by non-State actors.

On a global scale, given the borderless nature of cyberspace and the challenges of attribution, cyberattacks can trigger conflicts and exacerbate geopolitical tensions. Addressing this complex issue therefore requires a multifaceted approach, in which the United Nations plays an important role.

First, it is essential that States adhere to and implement existing norms and rules of applicable international law, which constitute a comprehensive guide for State behaviour in cyberspace.

At the same time, to further promote peace, security and cooperation among nations in the digital sphere, we need to continue strengthening the international framework that governs cyberactivities, particularly by committing to the ongoing processes related to this field, including the Global Digital Compact and a convention on countering cybercrime.

Secondly, capacity-building is key to maintaining an open, secure, stable, resilient, and peaceful cyberspace, especially for those with limited cybercapabilities, in order to effectively prevent, prepare for and respond to the impacts of malicious cyberactivities. It is crucial that all States share a common goal of strengthening capabilities and narrowing the development gap in information and communication technologies among countries and regions.

Thirdly, given its mandate, the Council should give more attention to this issue and address the interlinkages between cyberthreats and other key issues on its agenda, such as conflict prevention, counter-terrorism and the protection of critical infrastructure. It is also imperative for the Council to foster collaboration with other United Nations bodies, regional organizations and the private sector in order to create a unified and holistic response to cyberthreats.

The Government of Viet Nam has embraced a comprehensive, society-wide approach to addressing cyberthreats with the enactment of its cybersecurity law in 2018. Viet Nam reiterates its support for a concerted global effort to establish robust frameworks and mechanisms aimed at upholding the principles of sovereignty, non-interference and responsible behaviour in cyberspace. Through constructive dialogue and cooperation, we can effectively address the challenges that come with the evolving technologies, while safeguarding the integrity of the global cyberspace and information ecosystem.

Ms. Oppong-Ntiri (Ghana): I begin by thanking you, Mr. President, for organizing today's open debate on such an important topic. We are also grateful to the briefers for their insightful perspectives.

As it embraces the ever-dominant influence of the information and communications technology (ICT) revolution, Ghana remains keenly aware of the risks that that revolution also poses to international peace and security. Closer to home, on the African continent, we have witnessed the modifying impact and effects of the exponential growth of ICT on a diverse array of national security challenges and threats. Whether it is phishing and identity theft, the recruitment of adherents by terrorists or the trade in small arms and ammunition on the dark web, the security risks from the digital realm have been unrelenting. Private businesses and critical public infrastructure have not been spared, posing serious risks to peace and stability in some

cases. Even in the area of democratic governance, the positive influence of ICT on empowering African citizens to advance their chosen political causes under the framework of freedom of association and assembly has suffered greatly from its misuse in spreading fake news, disinformation and misinformation — a high risk to national unity and cohesion.

While robust cyberdefence capabilities must be built to address those growing trends, which reduce public confidence and trust, we caution that a calibrated response is needed to avoid governmental overreach and actions that blunt the rights and freedom of citizens, which on their own can become a source of great discontent and instability. Indeed, in recognition of the challenge facing Africa, the leaders of our continent have been taking several measures to bolster its cyberdefences. During the thirty-seventh Ordinary Session of the Assembly of Heads of State and Government of the African Union, held this year, cybersecurity took centre stage, with key decisions taken to further the Digital Transformation Strategy for Africa agenda. In addition to the push to expedite the creation of a continental cybersecurity strategy, African leaders agreed on a common position on the application of international law in cyberspace. We would agree that much more remains to be done to establish a cyberspace that is trustworthy and capable of addressing the constantly evolving threats. We must make every effort to bridge the digital gap through capacity-building and technical assistance.

In responding to the question as to the role that the Security Council can play in addressing threats to international peace and security in cyberspace, Ghana would like to make the following three additional points.

First, to fully harness the enormous potential of cyberspace for growth and prosperity, there must be concerted global action to address the emerging risks and to create a reliable, safe and resilient cyberspace for all. That underscores the importance of the consensus reports of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, which leaves us in no doubt that international law and the Charter of the United Nations are applicable and essential to maintaining peace, security and stability in the ICT environment.

Secondly, today's open debate, one of only a few in recent times on the subject, is another important step in acknowledging the increasing dangers that malevolent actors in cyberspace pose to global peace and stability. The Council's actions should aim to supplement the General Assembly's role in developing and promoting norms of responsible behaviour in cyberspace. It could also consider encouraging a legally binding framework for the digital realm to regulate any actions of governmental or non-governmental entities that threaten international peace and security. Such a framework could leverage the expertise of key stakeholders in the ICT space to coordinate international efforts in responding to and attributing and assigning responsibility for cybercrimes to ensure accountability. A subsidiary body devoted to the matter could be a starting point.

Thirdly, given the rapid advancement of ICT, specifically artificial intelligence, and the potential dangers of its misuse, the Council could consider creating a specific agenda item focused on cybersecurity before eventually incorporating it into the various thematic and geographical agendas. Such an approach would afford the Council ample time to deliberate on its implications and fully grasp the issue, allowing it to develop comprehensive strategies to safeguard global peace and security against cyberthreats.

The President: I now give the floor to the representative of Panama.

Ms. Concepción Jaramillo (Panama) (*spoke in Spanish*): In the digital age, threats caused by malicious cyberactivities continue to grow. Panama recognizes the importance of building a global cybersecurity architecture to effectively combat those evolving cyberthreats. The Security Council, among other actors and in the context of its mandate, can play a critical role in addressing those challenges and strengthening international cooperation to safeguard our shared digital environment. It has the primary responsibility for the maintenance of international peace and security, and that responsibility is equally crucial in the field of cyberspace. By proactively engaging in cybersecurity efforts and staying on top of emerging threats, the Council can contribute significantly to establishing a secure and peaceful cyberspace for all nations. It is imperative that we explore ways to improve the Council's ability to respond to malicious cyberactivities, which can affect critical infrastructure, civilians and humanitarian efforts.

When navigating the complex landscape of those cyberthreats, it is essential to consider the discussions under way on elaborating a comprehensive international convention to counter the criminal use of information and communications technologies that will help to complement the Council of Europe Convention on Cybercrime. While that Convention and its Protocols have been instrumental in facilitating international cooperation in the fight against cybercrime, the evolving nature of cyberthreats calls for the adaptation and strengthening of our legal frameworks. By updating and improving those frameworks, we can better address new challenges in cyberspace and ensure a more resilient global cybersecurity architecture.

Considering the transnational nature of malicious cyberthreats, it is imperative that the Security Council work collaboratively with Member States, international organizations and other stakeholders to address those multifaceted challenges. By fostering cooperation, sharing best practices and promoting responsible State behaviour in cyberspace, we can collectively mitigate the risks and vulnerabilities associated with those threats. Panama believes that those efforts can be promoted in some of the Council's committees, such as the Committee established pursuant to resolution 1540 (2004). In general, the Security Council can take on specific roles and actions to address international peace and security challenges arising from cyberspace, including developing assessments and strategies on cyberthreats and integrating cybersecurity into its discussions on specific issues. Cyberthreats are interconnected with other issues on the Security Council's agenda, including the protection of civilians, peace and security in armed conflict, the fight against terrorism, counter-terrorism and the theme of women and peace and security. Evaluations and strategies should consider the gender perspective and women's participation in policymaking, bearing in mind their differentiated vulnerability.

To effectively integrate cyberspace-related concerns into its work, the Council can explore ways to strengthen cyberresilience, promote international cooperation and address cyberthreats holistically. By strengthening coordination and cooperation and improving cybersecurity capabilities, we can build a safer and more resilient digital environment for the benefit of all nations. Panama calls for the Security Council to take decisive action in that regard and for us to work together to ensure a safer and more peaceful cyberspace for current and future generations.

The President: I now give the floor to the representative of Italy.

Mr. Jovanovic (Italy): I would like to express my gratitude to you, Mr. President, for convening this timely open debate. As we navigate an era marked by rapid technological advancement, the need for a robust and unified approach to cybersecurity has never been more urgent.

Italy aligns itself with the statement made on behalf of the European Union and would like to add some considerations in its national capacity.

Italy is concerned about the increasing number of malicious cyberactivities and the development of information and communications technology (ICT) capabilities for military purposes. We are strongly committed to enhancing cooperation among all Member States in the field of new digital technologies. Italy's Group of Seven presidency seeks to build on the efforts of the international community in promoting an open, interoperable, safe, secure, resilient and human-rights-respecting cyberspace, governed by the principles and rules of international law. Italy calls for the respect of the Charter of the United Nations and existing international norms in order to preserve peace and stability and strengthen our common security.

With its primary responsibility to maintain international peace and security, the Security Council is uniquely positioned to respond to cybersecurity threats for the benefit of all nations. That engagement of the Council should indeed complement other ongoing United Nations processes, such as the proposed programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. Proposals put forward in previous meetings of the Security Council are aimed at optimizing collective initiatives that address the global security implications of ICTs. One such suggestion is to consider relevant cybersecurity concerns in specific national cases or in other broader thematic issues, such as peacekeeping and peacebuilding missions, non-proliferation and counter-terrorism.

Moreover, we should strengthen the capacity of the United Nations to respond to malicious uses of ICTs that jeopardize international peace and security. That

is especially relevant when it comes to safeguarding civilians, critical infrastructure and humanitarian operations. As we move forward, we must consider the key trends of malicious activities, sometimes amplified by new technologies such as artificial intelligence, as well as their potential as threat multipliers in existing conflicts, and what specific actions the Security Council and the United Nations as a whole can envision to address the mounting challenges ahead of us.

We are all aware of the potentially disproportionate impact that malicious cyberactivities can have on vulnerable segments of our populations. We are all at risk of cyberattacks targeting critical infrastructure, such as health care or energy, or private citizens and businesses. To stop the perpetrators of cyberattacks from reaping rewards for their wrongful conduct, capacity-building is essential. In that regard, Italy will host a national conference on 2 July on enhancing the ecosystem of public and private entities tasked with cybercapacity-building activities worldwide. That will serve to facilitate the implementation of future projects with an inclusive and multi-stakeholder approach.

Attesting to Italy's commitment to the success of that approach, let me reaffirm our readiness to work with all Member States to develop and strengthen the skills, processes and resources needed to adapt to a fast-evolving cyberspace and ultimately to ensure a safer future for all nations.

The President: I now give the floor to the representative of Israel.

Mr. Kalmar (Israel): Israel wishes to join others in congratulating the Republic of Korea for organizing and presiding over this very timely and important debate on cybersecurity threats and to add some remarks on the existing and evolving threats in cyberspace from our perspective.

Israel has been on the front lines of an unprecedented wave of cyberaggression. Our adversaries have not limited themselves to conventional warfare and terror but have sought to exploit the digital realm to undermine our security, spread discord among our population and disrupt our way of life. Cyberattacks have become a daily reality for Israel. Our critical infrastructure, be it governmental, financial or societal, faces relentless assaults from State and non-State actors alike. Those attacks seek to jeopardize the safety and well-being of our citizens, threaten our economic stability and challenge our democratic institutions. The threats that we confront in cyberspace are real and pervasive, and demand our collective vigilance and action.

Like many nations, Israel understands the profound implications of cyberthreats. Our experience has taught us that these threats are not theoretical. On Saturday, 7 October 2023, thousands of Hamas terrorists penetrated Israel's southern border and massacred, burned, raped and mutilated 1,200 innocent people — women, men, elderly persons, children and babies. In addition, thousands more were injured, and more than 240 innocent citizens were abducted and taken hostage by the terrorists. Since 7 October 2023, Israel has also been subjected to ongoing massive cyberattacks. Those attacks have been orchestrated by Iran with the active support and participation of its proxies, Hizbullah, Hamas and other terror groups, which have launched massive cyberattacks targeting our most critical and sensitive infrastructure, such as our water supply, and energy infrastructure and hospitals. Iran must be condemned for blatantly violating the norms of responsible State behaviour in cyberspace and for breaching basic humane and moral standards. In addition to cyberattacks, we are under a massive Iranian influence campaign aimed at terrorizing Israeli citizens and abusing our free and democratic society, as well as causing more suffering for the victims of the brutal Hamas attack and their families. The attackers are using cyberspace as a tool and a venue for their terrorist activities, attempting to harm the foundations of Israeli society.

Israeli and Jewish communities around the globe are experiencing a global wave of incitement, hate speech and anti-Semitism, which is greatly augmented by coordinated, inauthentic behaviour on social media. We note the evolving efforts by some big technology companies and their social media platforms to mitigate hate and violence, yet there is still much more to be done. We call on all social media platforms to demonstrate more responsibility in that regard. Hate speech of any kind, calls for destruction and calls that imply the annihilation of a population should not be allowed to echo around the world.

Hamas's use of cyberspace combines a large array of strategies and goals, as stated at the recent meeting in The Hague on 15 May of the international coalition countering Hamas incitement and financing, established by French President Macron in the aftermath of the 7 October 2023 attack. Various online platforms are utilized by Hamas operatives to radicalize, indoctrinate,

incite violence, spread hate and disinformation and raise funds, all for the organization's stated goal, which is to destroy the State of Israel through violence and jihad. Hamas's cyberspace messaging, which incorporates the sophisticated use of icons and symbols to overcome artificial intelligence language-monitoring systems, allows groups and individuals to identify with Hamas's violent world view and transfer those ideas from cyberspace to the real world. That transfer is manifested through the significant increases in donations and fundraising amounting to tens of millions of United States dollars being directed to Hamas accounts, the mass of protesters at hate-filled demonstrations and the stabbing attacks motivated by Hamas's anti-Israel and anti-Semitic rhetoric posted online. Cyberterror is not yet being addressed by the international community as such. Cyberterrorists have distinct motivations and are not affected by international norms. The world today still lacks the proper means to deal with cyberterror.

All peace-loving nations should consider addressing that gap sooner rather than later. What starts in the Middle East rarely remains solely in our region. In this interconnected world, no nation is immune. The recent surge in cyberincidents across the globe — from ransomware attacks crippling critical infrastructure to disinformation campaigns undermining public trust — underscores the urgency of our shared responsibility. Those threats not only jeopardize our technological advancements and affect our economies, but also threaten the very fabric of our democratic institutions and global stability. Israel emphasizes the importance of international cooperation. No single nation can confront those threats alone. We must strengthen our partnerships, enhance information-sharing mechanisms and demand that every country implement the norms and rules of responsible behaviour in cyberspace. That is essential to create a secure and stable digital environment in which innovation can thrive without fear of exploitation. The international community must stand united in condemning cyberaggression and ensure that there are consequences for those who seek to undermine our collective security through cybermeans.

In conclusion, let us seize this opportunity to reaffirm our commitment to safeguarding the integrity and security of cyberspace. Together, through dialogue, cooperation and decisive action, we can mitigate the threats that we face and harness the transformative potential of digital technologies for the benefit of all humankind.

The President: I now give the floor to the representative of Morocco.

Mr. Hilale (Morocco) (*spoke in French*): First, allow me to congratulate you, Mr. President, for the holding of this open debate in the Security Council on a topic that takes on vital importance in these difficult times our world is currently facing and given the changing and complex nature of the threats inherent to cyberspace. I welcome the participation of the Minister for Foreign Affairs of the Republic of Korea, Mr. Cho Tae-yul, of the Secretary-General, Mr. António Guterres, and of the briefers, whom I would like to thank for their comprehensive briefings.

Morocco is proud to have co-sponsored, alongside 62 other countries, the joint statement on the use of information and communications technologies (ICTs) in the context of international peace and security.

Morocco has continuously advocated greater cooperation among Member States in the field of cyberspace and affirms its support for initiatives undertaken under the aegis of the United Nations and aimed at establishing a safe, secure and resilient cyberspace, as a shared domain that should always preserve its peaceful and prosperous nature and take full advantage of the opportunities presented by the responsible use of ICTs.

Faced with such a complex and unpredictable geopolitical context, the international community is called on to lay the foundations for a global, sustainable and peaceful digital transition, which will be determined by our collective efforts to promote mutual trust, transparency, the exchange of best practices, capacity-building and technical assistance — at the request of States parties and according to their needs, a reduction of the widening gap between developed and developing countries in the field of ICTs and more particularly respect for the national sovereignty and territorial integrity of Member States.

The Kingdom of Morocco, under the leadership of His Majesty King Mohammed VI, has always been a fervent advocate of the responsible use of ICTs, digital trust and digitalization, thanks to its new national cybersecurity strategy 2030, which is aimed at consolidating and building on the achievements made since 2012, when the national cybersecurity

strategy was adopted, with a view to better supporting a digital transformation, as a crucial lever for socioeconomic development.

The Moroccan approach to cybersecurity is also based on international cooperation, including with brotherly and friendly Arab and African countries, with a view to benefiting optimally from the advantages and opportunities represented by that vital field, within the framework of South-South and tripartite cooperation.

The United Nations is establishing multiple mechanisms and platforms dedicated to the review of cyber and digital threats. Morocco believes that the Security Council should engage more dynamically and actively in that sensitive area, in order to fulfil its mandate, notably in the maintenance of international peace and security in the cyberdomain, given the nature of cyberthreats which know no borders.

We believe that the Security Council should consider having more in-depth discussions on the definition and prioritization of cyberthreats posing a direct and ongoing risk to international peace and security, including by focusing on the following. First, the Council should focus on key parameters that determine whether the threat is of a sufficient level of alert to be considered by the Security Council. Secondly, it should address the measures to be taken to prevent the escalation of cyberthreats. Thirdly, it should hold an annual debate of the Security Council outlining emerging threats in cyberspace. And fourthly, it should focus on increasing the participation of women, young people, the private sector, civil society and academics to enable the Security Council to keep abreast of emerging threats in the field of ICTs and their impact on international peace and security.

Morocco stresses that further discussions within the Security Council on cyberthreats would provide the Council with an opportunity to play its leading role in developing action-oriented responses and mitigating the collective cyberthreats that Member States are facing on a daily basis.

In conclusion, we believe it is time to maintain the momentum generated over the past decade within the United Nations, in order to preserve our collective and constructive commitment to a secure, safe and resilient cyberspace. Cybersecurity and cybercrime do not exist in isolation but have widespread consequences that disproportionately affect the entire international community.

The President: I now give the floor to the representative of Liechtenstein.

Mr. Wenaweser (Liechtenstein): We thank the Republic of Korea for continuing the process initiated by Estonia of engaging the Security Council on cybersecurity (see S/2021/621). Security Council engagement with this topic helps ensure that the rule of law effectively addresses modern technological challenges, including the evolving threats in cyberspace, which is central to the Council's mandate.

The advent of new cybertechnologies in today's interconnected world not only offers unprecedented opportunities for international cooperation, but also presents the risk of malicious cyberoperations with potentially disastrous effects. The escalating sophistication and frequency of cyberattacks, including in Russia's aggression against Ukraine, requires us to be clear on how international law applies to cyberspace.

First and foremost, we recall the broad consensus that international law applies to cyberspace, including international humanitarian law, international human rights law, international criminal law and, of course, the Charter of the United Nations. The International Committee of the Red Cross has affirmed that international humanitarian law extends to cyberoperations during armed conflicts, emphasizing the need for adherence to legal standards also in the digital realm. Moreover, as many cyberoperations are increasingly deployed to enable international crimes, including war crimes and crimes against humanity, there is a critical need to understand their implications under the Rome Statute system of the International Criminal Court (ICC). Relevant assessments have affirmed that the Court can already investigate and prosecute relevant cyberattacks. That is only logical: international humanitarian law applies to cyberoperations, therefore violations of international humanitarian law that meet the ICC's gravity threshold are prosecutable. A council of advisers, convened by Liechtenstein in 2020 and 2021, produced a report clarifying how each of the Rome Statute's four core crimes — the crime of aggression, war crimes, crimes against humanity and genocide — apply in the context of cyberoperations.

Prosecuting cyber-enabled crimes at the ICC is instrumental to effectively address the evolving cyberthreat landscape. Building on the council of advisers' report, the International Criminal Court's Prosecutor has recently launched a multi-stakeholder

consultation process together with Microsoft to develop an ICC policy to address cyber-enabled crimes. That will help international law practitioners gain a deeper understanding of the complexities associated with prosecuting cyber-enabled crimes. Moreover, enhancing dialogue among the Court, the United Nations, governments, the private sector and civil society will foster important policy development in the cybercontext and ultimately support the Court's role as a key component of the international peace and security architecture.

Finally, the Security Council has a crucial role to play in ensuring accountability for cyberattacks by way of its power to make referrals to the ICC and to send relevant situations to the Court for investigation. The relationship between the Court and the Security Council is imperative to ensuring that justice is not outpaced by the shifting nature and developments of the tools of war.

The President: I now give the floor to the representative of Türkiye.

Mr. Çetin (Türkiye): We thank you, Mr. President, for organizing this open debate on evolving threats in cyberspace.

Information and communication technologies (ICTs) have become an indispensable part of society and the economy, affecting every aspect of life.

Today, States' capabilities in developing and using technology play an important role in their development and growth. While developments in technology provide us with many opportunities, cyberthreats are evolving and becoming even more complex. Security vulnerabilities in ICT systems often threaten the economy, public order and national security. Terrorism, digital espionage, fraud, online child abuse and the exploitation and misuse of personal of data undertaken via ICTs, are among the threats that also pose a risk to international peace and security.

We are particularly alarmed by the growing number of cyberattacks. Studies show that in 2023 there were more than 317 million ransomware and more than 6 billion malware attempts worldwide. Owing to technological developments, cyberattacks have become easier to carry out, while the adverse effects and burden on the victims are rapidly increasing. Combating those attacks and addressing threats require up-to-date methods and instruments, both in practice and in law.

Given the transborder nature of cyberthreats, increasing international cooperation and capacity-building in that area are crucial. With that understanding, Türkiye engages in cyberthreat intelligence-sharing and contributes to policies and cooperation strategies within regional and international organizations.

Within the international law context, Türkiye is a party to Convention on Cybercrime of the Council of Europe. We are also actively engaged with efforts carried out within the United Nations, in particular through the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. We are of the view that terrorism-related offences, when committed through ICTs, should also be regulated in a future convention.

There is also the question of the applicability of international law in cyberspace. Türkiye is one of the co-sponsoring States for the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security and strongly supports General Assembly resolutions 77/37 and 78/16.

As cyberspace is a borderless field and cybersecurity is a multi-stakeholder issue, international cooperation is of paramount importance. Service providers and security companies should cooperate more effectively with governments and international organizations in order to contribute to global cybersecurity. We welcome that the Security Council focuses on utilizing cyberspace to address growing threats, and we are committed to continuing our engagement and dialogue in that regard.

The President: I now give the floor to the representative of Saudi Arabia.

Mr. Alwasil (Saudi Arabia) (*spoke in Arabic*): At the outset, I would like to congratulate His Excellency Ambassador Joonkook Hwang, Permanent Representative of the Republic of Korea, on his presidency of the Security Council. I wish the delegation of the Republic of Korea every success during its tenure as President. I would also like to thank His Excellency Secretary General António Guterres, Mr. Stéphane Duguin, Chief Executive Officer of the CyberPeace Institute and Ms. Nnenna Ifeanyi-Ajufo, Professor of Law and Technology, for their briefings. They have made tireless, extraordinary and significant

efforts to confront the dangers facing cybersecurity and increasing cyberthreats.

The need for a safe and secure cyberspace that enables growth and prosperity is more urgent than ever. That underlines the importance of enhancing cybersecurity as a State priority in order to protect the vital interests of States and their national security. The Kingdom of Saudi Arabia believes that strengthening international cooperation in that regard and consolidating international efforts to reduce cyberthreats are vital and necessary. The time has come for the international community to take a serious and practical approach that unites international efforts to confront cyberthreats through the relevant United Nations commissions and specialized bodies.

The field of cybersecurity in the Kingdom of Saudi Arabia has witnessed vigorous and accelerating advances, and the groundwork for that was built upon the Saudi Vision 2030, its enablers and targets. The Kingdom of Saudi Arabia started its path of transformation by developing a Saudi model for cybersecurity based on centralized governance and decentralized operability that relies on the responsibilities of national bodies.

In that regard, we established the National Cybersecurity Authority in 2017 as the Kingdom's responsible body for cybersecurity and its national point of reference. The Kingdom's adopted model is a comprehensive one that deals with all aspects of cybersecurity, whether legislative, security, economic or developmental. The Kingdom's cybersecurity efforts have been recognized internationally, most notably through the International Telecommunication Union's Global Cybersecurity Index, which ranked us second globally and first within the Arab world, the Middle East and Asia. Moreover, the International Institute for Management Development's World Competitiveness Ranking placed the Kingdom of Saudi Arabia second globally in cybersecurity for two years in a row — 2022 and 2023. In 2024, the Kingdom's role as a global cybersecurity pioneer was confirmed through its first-place ranking in the World Competitiveness Yearbook.

The Kingdom of Saudi Arabia believes in strengthening international cooperation in cybersecurity. As such, the Kingdom established the Global Cybersecurity Forum, a global platform that brings together decision makers from around the world to discuss strategic issues pertaining to cybersecurity. During its session last year, the Forum witnessed the participation of over 120 States. Moreover, the Kingdom established the International Forum for Cybersecurity, an organization based in Riyadh, with a view to bolstering cybersecurity globally, promoting international cooperation and socioeconomic development in that regard and further consolidating international efforts in the field of cybersecurity in order to support human prosperity worldwide.

The Kingdom of Saudi Arabia participates in capacity-building for a number of States and international organizations. Over 40 States and organizations took part in the cyberexercises conducted by the Kingdom. Moreover, we have sought to pool regional efforts to enhance regional cybersecurity. Those efforts have led to the establishment of a ministerial committee specialized in cybersecurity, under the auspices of the Cooperation Council for the Arab States of the Gulf, based on a recommendation by the Kingdom. Moreover, upon a proposal submitted by the Kingdom of Saudi Arabia, the Arab Cybersecurity Ministerial Council was formed under the auspices of the League of Arab States. At its most recent summit, Arab leaders decided that the Ministerial Council, its Secretariat and executive office will be based in the city of Riyadh.

In conclusion, enhancing cybersecurity is the responsibility of all, and it requires all of us to cooperate and work in partnership in order to create a safe and secure cyberspace that will enable the growth and prosperity of all peoples worldwide.

The President: I now give the floor to the representative of Argentina.

Mr. Mainero (Argentina) (*spoke in Spanish*): We would like to thank the Republic of Korea for completing this high-level open debate on cybersecurity, an issue of great importance for Argentina.

Argentina is of the view that the main threats we must counter are not unrelated to geopolitical developments worldwide. That is particularly true given the global nature of cyberspace and the transnational nature of cyberevents. In that regard, we would like to highlight, that identifying potential or existing threats and the measures that States must take in order to prevent and mitigate them, in addition to cooperation and capacity-building efforts, must not violate international law, including international human rights law and international humanitarian law. Nor should they undermine the principles enshrined in the Charter

of the United Nations, such as the territorial integrity and sovereignty of States, non-interference in their internal affairs and the peaceful settlement of disputes.

We believe that the role of the Security Council and its efforts in the area of cybersecurity must not duplicate other work, but should instead complement and draw from the long-standing efforts of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, created in 2004, and the current efforts of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, which, in July, will be considering the draft of the third annual progress report, with a view to its adoption.

With regard to the proposal of convening a regular briefing to evaluate the evolving cyberthreat landscape as it relates to the current mandate and agenda of the Council, we think it is fundamental to contemplate the possibility of inviting to said briefings representatives of the Office for Disarmament Affairs, in their capacity as the secretariat of the Open-ended Working Group, as well as the Chair of the Working Group and representatives of the academic sector, civil society, and the private sector.

In particular, regarding new threats in cyberspace, we believe that the Security Council would benefit from receiving reports or presentations by private sector representatives, given that they are, in most cases, the owners and operators of critical infrastructure. They also have greater capabilities and resources to explore the operation of malicious software, which allows them to update their threat lists consistently over time.

We also welcome the fact that in the concept note (S/2024/446, annex), the presidency recognizes that capacity-building is an indispensable element. We believe that capacity-building is critical to bridging the cybersecurity gap — a gap that does not discriminate and affects all States equally, regardless of their level of development. Those States with less cybersecurity capacity often have vulnerabilities that can be exploited by malicious actors. Owing to the inherently interoperable nature of cyberspace, vulnerabilities anywhere in global cyberspace can have significant and wide-ranging repercussions. Cooperation in capacity-building is therefore imperative. Only through robust and sustained international cooperation in capacity-building will we be able to ensure a truly resilient, open, secure, stable, accessible, peaceful, free and interoperable cyberspace for all.

In that regard, we argue that capacity-building is inherently linked to the implementation of the framework for responsible State behaviour in cyberspace. The implementation of the norms, rules and principles of responsible behaviour in cyberspace must be complemented by the promotion of innovation, technical assistance for capacity-building and technology transfer for cyberresilience, in accordance with existing international law and taking into account the needs of developing countries. That will contribute not only to the well-being and economic development of our countries but also to the implementation and adoption, on equal terms, of the cumulative and evolving framework of responsible behaviour in the use of information and communications technologies (ICTs) and therefore to international peace and security.

Argentina is particularly concerned about the increasingly frequent operations using malware, ransomware and phishing and their effects on critical infrastructure. The ecosystem of vulnerabilities in that critical infrastructure has grown considerably, which represents a shared concern for States, the private sector and civil society. In that regard, we highlight the importance of multi-stakeholder cooperation to continue to analyse existing and potential threats to cyberspace and promote actions at the global level, such as the exchange of experiences. At the same time, we note with great interest the opportunities offered by ICTs and other emerging technologies for the development of our societies. We understand that emerging technologies are neutral and that the problem lies in our control and our use of them. In that regard, we recognize the need to find a fair balance between the regulatory frameworks that are being established on the transfer of ICTs and the right of all States to access emerging technologies for their well-being and socioeconomic growth, as well as to contribute to the resilience of cyberspace for the benefit of all.

In conclusion, the Security Council can play a crucial role in the field of cybersecurity by building on the work carried out by the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies and other relevant forums. It is essential to ensure that the actions of the Council are aligned with the already established regulations and recommendations. Multilateral coordination will facilitate cooperation among States

and international organizations, promoting a unified approach to cybersecurity.

The President: I now give the floor to the representative of Georgia.

Mr. Inashvili (Georgia): Georgia aligns itself with the statement made on behalf of the European Union and would like to add some remarks in its national capacity.

First of all, we thank the presidency of the Republic of Korea for convening today's open debate. We would also like to express our appreciation to the briefers for their insightful presentations earlier today.

Recent developments in cyberspace provide significant opportunities for innovation, economic progress and development. It carries the potential to enhance Member States' ability to better protect open and peaceful societies. However, it may also pose potential threats if misused. Cybersecurity threats are constantly evolving as technology advances, including malware, phishing, data breaches and so on. In the face of globally interlinked crises, the Security Council's role remains crucial in addressing and minimizing threats to international peace and security, including those coming from cyberspace.

In recent years, the international community has witnessed how certain State and non-State actors can threaten the rules-based international order by combining conventional methods of warfare with newly developed unconventional means. Some have used cybertactics to gain strategic advantages, such as disabling communication networks, targeting critical infrastructure and compromising military systems.

Against that background, Georgia remains committed to promoting responsible State behaviour in cyberspace. Our cybersecurity posture is in line with the normative framework developed by the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and by the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies.

Over the past few years, we have seen greater contributions to peace and security thanks to women's engagement. Women's increased participation in the cybersecurity field has paved the way for more inclusive and diverse perspectives. However, despite the Georgian Government's efforts to ensure responsible behaviour in cyberspace, we are witnessing Russia's aggressive use of a hybrid toolkit against Georgia's sovereignty. Georgia was the first case in which, along with conventional military engagement, a country became the target of numerous attacks in cyberspace over the course of Russia's full-scale military aggression in 2008.

We therefore consider capacity-building to be an indispensable element of multilateral cooperation. Along with strengthening national cybersecurity capabilities, it will promote more efficient international cooperation for addressing complex cyberthreats, which often transcend national borders and require a coordinated response. Given the uneven distribution of information and communications technology capabilities, we believe that the United Nations can better support national efforts for establishing a normative framework and assist Member States in capacity-building to reduce the existing divide.

In conclusion, we reaffirm our commitment to strengthening cybersecurity at both the national and international levels, while emphasizing the cross-cutting nature of cyberthreats and the necessity to effectively address them through collective action.

The President: I now give the floor to the representative of Australia.

Mr. Larsen (Australia): I thank the Republic of Korea for bringing us together to discuss this important topic.

I am glad to speak on behalf of Canada, New Zealand and Australia.

Cyberthreats undermine the transformative opportunities of digital technologies. They are increasing in scale and sophistication and pose particular challenges when employed in connection with armed conflicts. We all rely on such services every day as citizens and consumers, which means that cyberincidents involving critical infrastructure can have devastating and cascading impacts across society. They serve as a threat multiplier to existing risks and can threaten, at the most basic and fundamental levels, the effective functioning of, and public trust in, government.

Around the world, we have seen significant cyberincidents take down critical infrastructure and disrupt essential services and government operations. In our own countries, we have experienced that very directly. In Australia, a ransomware incident involving

the health-care sector exposed the personal information of millions of individuals. In Canada, a ransomware incident paralysed the systems of provincial health-care providers, which caused serious delays and imperilled sensitive information pertaining to thousands of staff and patients. In New Zealand, the proportion of financially motivated cyberactivity has exceeded State-sponsored activity for the first time.

In ongoing situations of armed conflict, we have seen military cyberoperators deploying destructive malware against government and private sector networks and compromising civilian critical infrastructure and entities involved in crisis response, including emergency services and energy, transport and communications networks. We also see a clear link between the use of ransomware tools to perpetrate financial crime, including cryptocurrency theft, to directly fund nuclear and weapons of mass destruction programmes and the undermining of our efforts towards global stability and disarmament. The Security Council has a crucial role to play in preventing that. We welcome opportunities such as this to discuss cyberthreats, which help mainstream those issues within Security Council discussions, raise their profile and bring in the expertise of the multi-stakeholder community, including civil society organizations.

Collectively, we have sent an unambiguous message that all States' activities in cyberspace have limitations and are subject to obligations, just as they are in the physical domain. 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 — applies in cyberspace. States must be unequivocal in their commitment to act in accordance with international law and with the expectations set out by the agreed non-binding norms.

In conclusion, we have two key requests.

First, we ask the Security Council to affirm the agreed framework of responsible State behaviour in cyberspace which underpins peace and stability and promotes an open, secure, stable, accessible and peaceful cyberspace. Achieving those key objectives requires the implementation of and adherence to related commitments, supported by coordinated capacity-building to support all States in increasing their ability to respond to the challenges posed.

Secondly, we call on the Security Council to affirm that international humanitarian law applies to cyberspace in situations of armed conflict. Such affirmations reinforce our collective commitments to protect critical infrastructure and to bolster international law, in particular the Charter of the United Nations.

The President: I now give the floor to Ms. Courtois.

Ms. Courtois: The International Committee of the Red Cross (ICRC) shares the Republic of Korea's concern about the potential human cost of cyberoperations during armed conflict.

The ICRC works to protect and assist people affected by over 120 armed conflicts worldwide. In a growing number of those conflicts, cyberoperations are creating additional risks for people's security and well-being. Three trends are of particular concern.

First, cyberoperations have disrupted the provision of essential services for civilian populations — such as electricity, water and medical care. Such cyberoperations endanger people already suffering from the devastation and insecurity caused by armed conflict and are often conducted in disregard of international humanitarian law.

Secondly, we are deeply concerned about the growing involvement of civilian actors — individuals, hacker groups, and tech companies — in cyberoperations related to armed conflicts. The closer civilians and civilian objects are drawn to hostilities, the greater the risk that they will be harmed.

Thirdly, the ICRC and the broader International Red Cross and Red Crescent Movement — as humanitarian organizations — also face a growing threat of cyberoperations, including data breaches and harmful information operations. If our relief operations are disrupted or trust in our operations and work is undermined, our ability to assist and protect people is weakened.

In the Security Council, members have the primary responsibility for the maintenance of international peace and security and a key role in the protection of civilian populations during armed conflict. The Security Council has always been clear: wars have limits. The Council has left no doubt that belligerents must not target civilians or civilian objects and that medical facilities, as well as humanitarian relief operations and personnel, must be respected and protected. Thus, the ICRC encourages the Security Council to mainstream the potential human cost of cyberoperations in its work and to systematically uphold the long-standing limits

that international humanitarian law imposes on all means and methods of warfare — old and new, cyber and kinetic.

The recently adopted resolution 2730 (2024), which explicitly expresses concern about malicious information and communication technologies (ICTs) activities that target humanitarian organizations and condemns disinformation and the incitement of violence against humanitarian personnel, has been an important first step in that direction. In today's digitalized world, the Security Council should not ignore the threats that ICT activities pose to civilian populations during armed conflict.

The President: I now give the floor to the representative of Kiribati.

Mr. Tito (Kiribati): Kiribati appreciates the opportunity to share its thoughts on the use of information and communications technology (ICT) in the context of international peace and security. We would like to thank the Secretary-General and the briefers from non-governmental organizations and academia for sharing their perspectives.

Earlier this week, Kiribati endorsed the joint statement issued by the Republic of Korea on this subject. We would like to commend the Republic of Korea for its leadership on this matter and would like to acknowledge the presence of the Republic of Korea's Minister for Foreign Affairs, Mr. Cho Tae-yul, who is presiding over this meeting. I thank you, Mr. President, for highlighting the role of the Security Council in ensuring that information and communications technology are responsibly used for advancing world peace and security and not for purposes that jeopardize international peace and security, especially at this time when regional wars and violent conflicts are on the rise.

We share similar concerns about the use of malicious cyberactivities against civilian infrastructure and the impact that they may have on human lives and well-being, particularly with regard to the most marginalized and vulnerable members of our societies. We would like to express our deep concerns about cyberoperations targeting critical civilian infrastructure, such as water and electricity. Those objects are protected under international humanitarian law. In addition, under international humanitarian law, medical facilities must be respected and protected. In times of armed conflict, humanitarian relief operations must also be respected and protected.

When stakeholders voice their views about harmful cyberoperations in situations of armed conflict and call for the application of and discussions about international humanitarian law, they do so out of an honest concern for the safety of their populations. Let us imagine a world in which those protections did not apply to cyberoperations and ask ourselves whether such a world is the kind that we would want to live in and call home. For us, the answer is no, especially in the Pacific where we enjoy a lot of peace and harmony with nature and with ourselves.

We must uphold the application of international humanitarian law to the cyberdomain. As a result, we firmly believe the international community, especially the Security Council, should listen to the stakeholders and actors from non-governmental organizations and academia who voice concerns about the malicious activities of cybercriminals. We must be ready to uphold and apply the principles of international humanitarian law. Therefore, we strongly encourage the Security Council to mainstream the humanitarian concerns of cyberoperations and uphold the limits placed on all means of warfare, including cyberoperations under international humanitarian law. We cannot risk the erosion of international humanitarian law in the emerging cyberdomain of ICTs.

I wish to conclude by recalling the statement that former United States President Harry Truman delivered 79 years ago to welcome the newly launched Charter of the United Nations.

> "Only if we understand what the Charter is and what it can mean to the peace of the world, will the document become a living human reality."

Let us all respect the Charter of the United Nations in its entirety and call on all global tech companies, most of which are outside government control, in control of all information and communication technologies to ensure that such technologies are responsibly used for promoting full respect for the Charter and for advancing the Charter's noble goal to build a more peaceful, prosperous, human and loving world for all.

The President: The representative of the Islamic Republic of Iran has asked for the floor to make a further statement.

Mr. Ahmadi (Islamic Republic of Iran): I understand that today's meeting has been lengthy, and I do not intend to take up much of the Council members'

time. However, I requested the floor to make a further statement because the representatives of Albania and the Israeli regime have misused the Chamber to level unsubstantiated claims against Iran, falsely accusing my country of supporting cyberattacks.

We categorically reject and denounce those baseless claims. Concerning an unwarranted reference made to Iran in the statement of the representative of Albania, we responded to and rejected that false assertion in our letter to the Security Council dated 10 September 2022 (S/2022/685). We believe that the Government of Albania was misled by misinformation from the terrorist organization, namely the Mojahedin-e Khalq Organization, and falsely attributed the cyberattack to Iran.

The Mojahedin-e Khalq Organization, which is currently located in Albania, has already carried out several cyberterrorist attacks against Iran's critical infrastructure, with the assistance and support of certain States, including the Israeli regime. This terrorist organization has martyred numerous Iranian officials and civilians through terrorist bombings and assassinations and, since 1981, has claimed the lives of almost 17,000 Iranian citizens.

Despite that fact, the Government of the Islamic Republic of Iran, in good faith, extended an offer to the Government of Albania to cooperate and engage constructively in order to clarify the unfounded accusation levelled against Iran. Unfortunately, our request went unanswered.

Regarding the unfounded allegations made by the Israeli regime, we categorically reject them. Ironically, a representative of a regime notorious for its malicious, criminal and terrorist activities in both cyberspace and real space is accusing others of the very actions that the Israeli regime has repeatedly committed.

For over nine months, Israel, the occupying regime, has waged a genocidal war and military aggression against defenceless Palestinian people and is involved in vicious and terrorist acts in the region, in flagrant violation of all international legal rules, principles and norms, including international humanitarian law and international human rights law. The regime shamelessly employs every possible means to decimate the vulnerable population, including the use of starvation as a method of warfare, the indiscriminate targeting of civilians, including women and children, the deliberate assault on vital civilian infrastructure and the obstruction of essential humanitarian aid and services to civilians, in direct violation of the relevant Security Council resolutions.

In addition, this terrorist regime has a long and dark history of cyberattacks against the critical infrastructure of sovereign States. As mentioned in Iran's statement, delivered earlier in the Chamber, the Stuxnet and Duqu attacks on Iran's peaceful nuclear facilities are clear examples of Israel's criminal activities and cyberattacks against critical infrastructure. Those criminal actions were openly admitted by the regime and demonstrate its involvement in malicious cyberoperations.

With its history of egregious violations of basic principles of international law, the Israeli regime is in no position to accuse or lecture others on the observance of those principles. The regime should not go unpunished, and the Security Council must hold it accountable for all the international crimes it has committed and continues to commit.

The meeting rose at 5.55 p.m.