United Nations S/PV.9662

Security Council

Seventy-ninth year

Provisional

9662nd meeting
Thursday, 20 June 2024, 10 a.m.
New York

President:	Mr. Cho Tae-yul/Mr. Hwang	(Republic of Korea)
Members:	Algeria	Mr. Bendjama
	China	Mr. Fu Cong
	Ecuador	Mr. De La Gasca
	France	Mr. De Rivière
	Guyana	Mr. Persaud
	Japan	Mr. Yamazaki
	Malta	Mrs. Frazier
	Mozambique	Mr. Afonso
	Russian Federation	Mr. Nebenzia
	Sierra Leone	Mr. Kanu
	Slovenia	Mr. Žbogar
	Switzerland	Mrs. Chanda
	United Kingdom of Great Britain and Northern Ireland	Dame Barbara Woodward
	United States of America	Mrs. Thomas-Greenfield

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 was called to order at 10 a.m.

Adoption of the agenda

The agenda was adopted.

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 President: I would like to warmly welcome the Secretary-General and the distinguished ministers and other high-level representatives present in the Chamber. Their presence today underscores the importance of the subject matter under discussion.

In accordance with rule 37 of the Council's provisional rules of procedure, I invite the representatives of Albania, Argentina, Australia, Austria, Bahrain, Bangladesh, Belgium, Brazil, Bulgaria, Cambodia, Chile, Costa Rica, Croatia, Cuba, Czechia, Egypt, El Salvador, Estonia, the Gambia, Georgia, Germany, Ghana, Greece, Guatemala, India, Indonesia, the Islamic Republic of Iran, Israel, Italy, Kazakhstan, Kiribati, Latvia, Liechtenstein, Morocco, Nepal, Norway, Pakistan, Panama, the Philippines, Poland, Portugal, Romania, Saudi Arabia, Singapore, Spain, Türkiye, Ukraine, the United Arab Emirates, Uruguay and Viet Nam to participate in this meeting.

In accordance with rule 39 of the Council's provisional rules of procedure, I invite the following briefers to participate in this meeting: Mr. Stéphane Duguin, Chief Executive Officer, CyberPeace Institute; and Ms. Nnenna Ifeanyi-Ajufo, Professor of Law and Technology, Leeds Beckett University.

In accordance with rule 39 of the Council's provisional rules of procedure, I also invite the following to participate in this meeting: Her Excellency Mrs. Hedda Samson, Chargee d'affaires a.i. of the Delegation of the European Union to the United Nations; Ms. Roraima Ana Andriani, Special Representative of INTERPOL to the United Nations; and Ms. Laetitia Courtois, Permanent Observer and Head of Delegation of the International Committee of the Red Cross to the United Nations.

The Security Council will now begin its consideration of the item on its agenda.

I wish to draw the attention of Council members to document S/2024/446, which contains the text of a 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, transmitting a concept paper on the item under consideration.

I now give the floor to the Secretary-General, His Excellency Mr. António Guterres.

The Secretary-General: I thank the Republic of Korea for convening this high-level debate on an issue that affects us all — peace and security in cyberspace.

Breakthroughs in digital technologies are happening at warp speed — from information and communication technologies and cloud computing, to blockchain, 5G networks, quantum technologies and more. Digital advances are revolutionizing economies and societies. They are bringing people together; delivering information, news, knowledge and education at the tap of a screen or click of a mouse; providing citizens with access to government services and institutions; and supercharging economies, trade and financial inclusion.

But the very quality of the seamless, instant connectivity that powers the enormous benefits of cyberspace can also leave people, institutions and entire countries deeply vulnerable. And the perils of weaponizing digital technologies are growing by the year. Cyberspace has kicked the doors wide open. Anyone can walk through, and many are. Malicious activity in cyberspace is on the rise by both State and non-State actors and by outright criminals.

Serious cybersecurity incidents are disturbingly common. From breaches of essential public services like health care, banking and telecommunications; to relentless illicit activity, including by criminal organizations and so-called cybermercenaries; to a legion of hate merchants littering the information superhighway with fear and division; to the increasing use of cyberspace as another weapon in ongoing armed conflicts — so-called civilian hacktivists are entering the fray and, in many cases, are blurring the line between combatants and civilians. And the growing integration of digital tools with weapon systems, including autonomous systems, presents new vulnerabilities.

At the same time, the misuse of digital technology is becoming more sophisticated and stealthy. Malware, wipers and trojans are proliferating. Cyberoperations enabled by artificial intelligence (AI) are multiplying the threat, and quantum computing could break down entire systems with its ability to breach encryption. Software vulnerabilities are being exploited, and cyberintrusion capabilities are even sold over the Internet. And companies' supply chains are being actively targeted by hackers, with serious, disruptive and cascading effects. Ransomware is one grievous example — a huge threat to public and private institutions and the critical infrastructure people depend on. According to some estimates, ransomware payments reached a total of $1.1 billion in 2023.

But far beyond the financial costs are the costs to our common peace, security and stability — both within countries and among them. Malicious activity that undermines public institutions, electoral processes and online integrity erodes trust, fuels tensions and even sows the seeds of violence and conflict.

Digital technology offers an incredible opportunity to create a more just, equal, sustainable and peaceful future for all. But breakthroughs must be oriented towards the good. The New Agenda for Peace places prevention at the heart of all peace efforts. It calls for developing strong frameworks in line with international law, human rights and the Charter of the United Nations, and for focused efforts by all States to prevent the extension and escalation of conflicts within and through cyberspace. As reflected in the New Vision for the Rule of Law, the rule of law must exist in the digital sphere as it does in the physical world.

I also welcome the General Assembly's commitment to action in that area. That includes its dedicated Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. States are building on the universally endorsed normative framework for responsible State behaviour in cyberspace, and they are actively considering the applicability of international law to State activities in that domain. And under the auspices of the General Assembly, Member States are working to reach consensus on a new cybercrime treaty in the coming months, which should deepen cooperation while protecting human rights online. But given the clear and growing links between cyberspace and global peace and security, the Council can also play a key role by integrating cyber considerations into its existing workstreams and resolutions.

This is only the second time that the Security Council has held a formal meeting on this issue. But so many of the issues considered around this table are affected by and linked to cyberspace, including the protection of civilians in armed conflict, peace operations, counter-terrorism and humanitarian operations. Integrating this issue into Council deliberations would be a useful way to lay the groundwork for more effective responses to this important question.

(*spoke in French*)

To guarantee peace and security in the physical world, we need new approaches to peace and security in the digital world. September's Summit of the Future will be a vital opportunity to enhance cooperation on critical global challenges and reinvigorate the multilateral system. The Pact that will emerge from the Summit represents a unique chance to support the maintenance of international peace and security in cyberspace. Among other priorities, chapter 2 of the Pact aims to reaffirm global consensus on safeguarding critical infrastructure against harmful digital practices and creating enhanced accountability for data-driven technology, including artificial intelligence. Meanwhile, my High-level Advisory Body on Artificial Intelligence is completing its final report on how we can govern AI for humankind, while addressing its risks and uncertainties. I look forward to working with the Council, the General Assembly and all Member States to ensure that technology is used appropriately: to work towards the progress and security of all people and the planet that we share.

The President: I thank the Secretary-General for his briefing.

I now give the floor to Mr. Duguin.

Mr. Duguin: It is an honour to address the Security Council today on a matter of critical importance: how to address the evolving threats in cyberspace. As the Chief Executive Officer of the CyberPeace Institute, an independent and neutral non-governmental organization based in Switzerland, I speak from experience, as the Institute offers free cybersecurity to the most vulnerable, namely, non-profit organizations, monitors threat actors, provides threat detection and analysis and advocates for respect for laws and norms in cyberspace.

As we analyse the evolution of the threat, I would like to address the cumulative effect of serious disruptions to the threat landscape, which together have a direct impact on the maintenance of international peace and security. I will touch on various topics: the proliferation of threat actors and how it increases the targeting of critical infrastructure; the mutation of the threat today, notably with the convergence of cyberattacks and disinformation and the usage of cyberattacks to circumvent international sanctions; and the evolution of the threat tomorrow, with the unique risk that artificial intelligence (AI) poses to cybersecurity. Those evolutions create unique challenges for international peace and security, notably by hampering attribution, meaning the process of identifying the perpetrator or source of a cyberattack or operation.

I will start with the proliferation of threat actors. Since the 2022 invasion of Ukraine by the Russian Federation, the CyberPeace Institute has been documenting a proliferation of threat actors siding with both belligerents. Warfare is no longer the sole preserve of States. A range of non-State actors — criminal groups, hacktivist collectives with geopolitical motives and other civilians — are taking part in cyberattacks and operations in the context of armed conflicts. They pursue four objectives: destroying infrastructure, disrupting the normal functioning of essential services, synchronizing disinformation and cyberattacks and stealing and weaponizing data through infiltration and espionage. In that context, we, the CyberPeace Institute, have traced more than 3,000 cyberattack campaigns by 127 threat actors, affecting 56 countries and targeting 24 critical infrastructure sectors. The harm caused by those cyberattacks has been felt far beyond the borders of the belligerent countries, with close to 70 per cent of all cyberattacks affecting organizations in non-belligerent countries. Those metrics are freely available on our Cyberattacks in Time of Conflicts Platform. Such a proliferation of attacks poses the question of de-escalation in the context of a potential cessation of hostilities. How can those 127 threat actors be made to stop their malicious activities or be brought under control in such circumstances?

That proliferation has a direct impact on the security of critical infrastructure. I would like to give two examples. In February 2022, a cyberattack using a wiper malware called AcidRain targeted Ukraine's broadband satellite Internet access. The impact was felt beyond the borders of Ukraine. It affected the functioning of wind turbines across Europe, with a major German energy company losing its remote monitoring access to more than 5,800 of those turbines, and thousands of subscribers to satellite Internet services in Germany, France, Hungary, Greece, Italy and Poland were affected. Such impacts are not solely being felt in times of armed conflict. During the coronavirus disease (COVID-19) pandemic, the CyberPeace Institute monitored 500 cyberattacks against health-care facilities over two years of the COVID-19 pandemic. Five hundred cyberattacks are not even the tip of the iceberg — they represent the ice cube on the tip of the iceberg. Those 500 attacks alone disrupted health care in 43 countries, led to the theft of 20 million patients' data and accounted for a cumulative disruption to access to health care of five years. That means a five-year accumulation of redirected ambulances, cancelled appointments and patients with reduced access to health care.

But another aspect of the evolving threat is the use of cyberattacks to evade international sanctions and to finance illegal activities. As an example, several civil society actors, cybersecurity organizations and States have analysed the activities of two alleged criminal groups, Kimsuky and the Lazarus Group, the tactics, tools, processes and intent of which have been attributed to the Democratic People's Republic of Korea. Those criminal groups coordinate global cyberattacks of all types: on the supply chain, ransomware, on cryptocurrency exchange and financial institutions. Beyond the important direct or primary harm of those attacks, they are a vector for circumventing international sanctions. According to recent estimates, Lazarus Group and Kimsuky have gained more than $3 billion from such attacks. That escalation creates massive harm. The WannaCry attack in May 2017, which affected more than a quarter of a million computers in less than 24 hours in more than 150 countries, caused significant disruption and had a widespread impact across the health-care, financial and transportation sectors.

To conclude on the evolution of threats, it is important to foresee new risks, such as the threat of quantum computing to cryptography, as mentioned previously, and that of generative AI to criminal models. Since the advent of generative AI and large language models, AI has been used by malicious actors merely to augment their capability. Today AI is used to scale up existing processes in what is called the

Cyber Kill Chain, which is the standard process that any attacker must go through in order to conduct a cyberattack. Using AI saves time in target recognition, automating vulnerability searches, increasing the production capacity of phishing, for example. That is only the first step, as groups are already experimenting with using generative AI to automate different parts of a cyberattack. That poses an unacceptable risk. Successful tests carry the risk of reaching such a high level of automation across the Cyber Kill Chain that a malicious actor could willingly or accidentally trigger an autonomous cyberattack.

Given the convergence of several cumulative disruptions — threat proliferation, the new specific modus operandi to attack critical infrastructure or circumvent sanctions and what is going to happen because of new AI technology, it is difficult to respond with a coherent strategy. Still, several steps can be taken, and I will conclude with this.

We can operationalize laws, norms and sanctions, notably through the transparent documentation of violations and a future-looking approach to prevent the malicious use of cyberspace, including the misuse of AI or quantum computing.

It is important to call out perpetrators, to enforce sanctions and to take appropriate and adequate measures. There cannot be de-escalation without attribution, as it is critical to inform decision-making about the measures to be taken and the defences to adopt. Attribution can have a deterrence effect, as holding perpetrators accountable can enable legal and diplomatic responses and strengthen policy development.

Finally, it is essential to be able to comprehensively and quantifiably measure harm from cyberattacks. The CyberPeace Institute is developing such a methodology to measure the harm from cyberattacks because, thus far, they have too often been described in terms of loss of money or capacity, whereas the harm to human populations and social constructs is also important.

Those aspects are critical to maintaining international peace and security.

The President: I thank Mr. Duguin for his briefing.

I now give the floor to Ms. Ifeanyi-Ajufo.

Ms. Ifeanyi-Ajufo: I feel privileged to have been asked to address this forum on maintaining international peace and security and addressing evolving threats in cyberspace, particularly by providing a regional perspective and looking at the situation in Africa.

In any discussion on peace and security in cyberspace, there is a need to measure the security of cyberspace through existing regional realities and perspectives. We must acknowledge that the effective realization of cybersecurity often collides with the realities of developing States, especially those in the African region that remain at the end of the digital divide and lack adequate capacity, skills and infrastructure to effectively ensure peace and security at anticipated standards. Therefore, as we acknowledge our cybersecurity commonalities, we must also acknowledge the differences and challenges among regions and consider cyberthreats in the context of country- and region-specific realities.

The peace and security dimensions of the cyberdomain have become a fundamental agenda for many regions. For example, November 2022 was the first time that the African Union Peace and Security Council approached the issue of peace and security in cyberspace from the perspective of regulating it within the rules of international law. Thereafter, the African Union has adopted cybersecurity as a flagship programme of the African Union Agenda 2063 and as a cross-cutting theme of the African Union's Digital Transformation Strategy for Africa (2020-2030). Importantly, the African Union Convention on Cyber Security and Personal Data Protection, which provides a unified regulatory framework for mitigating cyberthreats and protecting information and communications technology (ICT) infrastructure, entered into force in June 2023. In January of this year, the African Union also adopted a common African position on the application of international law to the use of ICTs in cyberspace. I must add that the African position is the first position document on the application of international law in cyberspace that includes a section on capacity-building. Africa is also the first region to develop a regional common position.

We must also acknowledge that there are various challenges to how regions can maintain peace, security and stability in cyberspace. Since last year, for example, we have seen cyberattacks on the African Union Commission headquarters that compromised the functioning of email systems. The Communications Authority of Kenya announced that, in 2023 alone, Kenya recorded 860 million cyberattacks, with sophisticated attacks targeted at the country's critical

information infrastructure. In July 2023 alone, Kenya suffered a high-profile cyberattack on the very important eCitizen platform, which incapacitated access to over 5,000 government services from ministries, county governments and agencies. A group that calls itself Anonymous Sudan declared responsibility for those cyberattacks in Kenya and other parts of Africa. A few months ago, organized cyberattacks forced the Government of Malawi to suspend the issuing of passports, following a cyberattack on the Immigration Service's computer network, which was deemed a serious national security breach.

This raises significant issues, including the blurry lines of the responsibility of State actors and non-State actors and the dynamics of how those emergent cyberthreats add cleavages to already existing conflicts. We see how the activities of organized terrorist and extremist groups are further enabled by conflicts in regions like Africa. We see how criminal activities in cyberspace are not only exacerbating existing threats and challenges to international peace and security in the region, but also how States breach international human rights under the pretext of cybersecurity through shutting down Internet access, especially during armed conflicts. Those actions not only infringe on the rights to communication and freedom of information of citizens, but have also prevented effective humanitarian action during conflicts in places like Africa and, of course, elsewhere. We also see how cyberenabled disinformation and misinformation are increasingly used as tools to scuttle peace and security in parts of the region. That is further being aggravated by the deployment of artificial intelligence in such circumstances.

However, we believe that the Security Council can make an immense difference to enhance peace and security in cyberspace, particularly from a regional perspective. Indeed, existing sources of inequalities require complex interactions in order to define a mandate on peace and security in cyberspace for the Security Council. These disparities in cybersecurity infrastructure and digital capacities are a key challenge, coupled with persistent political conflicts in regions like Africa. There is also a seeming lack of awareness of the obligations related to non-intervention, due diligence and peaceful settlement of disputes in the context of cyberspace.

As the Security Council determines its mandate for maintaining peace and security in cyberspace, it is therefore important to consider collaborative measures that can effectively be leveraged to counter existing threats and build capacity. It is necessary to establish and enhance capacity at regional levels. However, we must note that this is not only a matter of legal, technical and operational capacity, but also a matter of social, economic and political realities. Given the varied cybersecurity maturity levels and local contexts, strategic regional capacity-building is required. The specific realities of diverse regions must be considered because capacity gaps may not necessarily be the same across regions. Attempts to develop and transfer cybercapacity across regions must be approached purposefully, but also must be strategized based on defined accountability mechanisms.

In regions like Africa, priority areas where capacity-building is needed to address cyber-related threats include governance, policymaking, technical tools and infrastructure, as well as research. Capacity development for the protection of critical infrastructure is needed. It is important to ensure that cybersecurity incident response teams are established at regional levels where they are not yet in place, and to mandate the establishment of regional 24/7 points of contact. It is also important to develop and implement mechanisms for regional and international collaboration among those teams.

To promote trust and security in the cyberdomain, there is a need to focus on implementing the United Nations norms of responsible State behaviour in cyberspace across all regions. Many questions have been asked about the voluntary nature of the norms and the need to have more accountable approaches to maintaining peace and security in cyberspace, for example, having clear defined guidelines on the use of force, armed attacks and self-defence in cyberspace. Again, creating and supporting forums for developing confidence-building measures will decrease mistrust among Member States and contribute to the peaceful settlement of disputes in the cyberdomain.

It is also important for the Security Council to develop mechanisms to understand the cyberthreat landscape across regions. That will allow for making informed decisions on regulating security and stability. That may also imply setting up a working group on peace and security in cyberspace — in the first instance, to consider recommendations on conflicts and the promotion of peace and stability in cyberspace. Developing functional regional cybersecurity centres to enhance

cross-border cooperation and information-sharing will also aid in achieving those objectives. Capacity support for developing and implementing comprehensive regional and national cybersecurity strategies should also be given attention, as should advancing a culture of cybersecurity leadership.

Regional organizations have a key role to play in formulating policies and working with States in their region to deliver outcomes for peace and security. Therefore, existing cooperation between the United Nations and regional and subregional organizations in maintaining international peace and security should now include an agenda on cybersecurity. Finally, the Security Council should promote a platform that will allow effective dialogue aimed at encouraging each region to develop a framework for peace and security in cyberspace.

I will conclude by adding that it will be important for the Security Council to pursue a multilateral agenda that decisively affirms the peace and security dimensions of the rule of law in cyberspace. That also necessitates the establishment of defined cybergovernance principles and standards that will hold all regions and Governments accountable for peace and stability. As we are becoming more interconnected and even more affected by disruptive technologies, such as artificial intelligence, we are also becoming more vulnerable. Therefore, it is crucial to reinforce our human and institutional capacity to secure cyberspace by building trust and confidence in the use of cybertechnologies.

The President: I shall now make a statement in my capacity as the Minister for Foreign Affairs of the Republic of Korea.

I would like to begin by thanking once again Secretary-General Guterres for his presence and briefing today. Let me also thank Mr. Stéphane Duguin of the CyberPeace Institute and Professor Nnenna Ifeanyi-Ajufo of Leeds Beckett University for sharing their insights and expertise. My deep appreciation also goes out to all the representatives of Member States for participating in this high-level open debate.

Today's meeting marks only the second time in United Nations history that the Security Council is formally meeting to discuss threats to international peace and security from cyberspace. The Council convened its first-ever open debate on this topic three years ago in June 2021 (see S/2021/621). To be sure, significant milestones have been achieved outside the Security Council. Entities established by the General Assembly have advanced norms on responsible State behaviour in cyberspace. A number of Arria Formula meetings have also been held on cybersecurity, the most recent being the April meeting that the Republic of Korea co-hosted with the United States and Japan.

The Secretary-General has also demonstrated strong leadership, calling for measures to de-escalate cyber-related risks and establishing the High-level Advisory Body on Artificial Intelligence, of which Korea is a part. But developments since the first Security Council meeting three years ago sharply underscore why the Council, now more than ever, must proactively step up its engagement on threats emanating from cyberspace. The world has seen — in addition to myriad cross-border cyberattacks — the outbreak of major armed conflicts in which attacks were carried out not just on the traditional battlefield, but also in cyberspace.

The world has also seen how explosive advancements in artificial intelligence are dramatically empowering nefarious actors in their ability to cause further chaos and disruptions in cyberspace. The world has seen how malicious cyberactivities can have real-world impacts by undermining confidence in the integrity of political elections, the security of critical infrastructure and the fabric of peace and security. As a matter of fact, a Member State even had to declare a state of emergency after being subjected to ransomware attacks originating from another country.

Cybermeans are fundamentally dual use in nature: anyone with malicious intent can introduce new threats or trigger, amplify or accelerate existing threats. As Alvin Toffler, a famous futurist, once noted: "Our technological powers increase, but the side effects and potential hazards also escalate."

The Republic of Korea is no stranger to the threats posed by malicious cyberactivities and their impact on security, given that the development of the weapons of mass destruction that imperil Korea are largely funded through such activities. The most recent report of the Panel of Experts of the Committee established pursuant to resolution 1718 (2006) (S/2024/215) cites how 40 per cent of the weapons of mass destruction programmes of the Democratic People's Republic of Korea are funded by illicit cybermeans. The Panel was investigating some 60 suspected cyberattacks by the Democratic People's Republic of Korea on cryptocurrency companies

between 2017 and 2023. Sadly, the Panel is now defunct, for reasons we all know.

Through digital means, the Democratic People's Republic of Korea systematically evades the very sanctions adopted by the Council and challenges the international non-proliferation regime that is integral to the Council's work. At a time when peace and security in the physical world and in the cyberworld are increasingly intertwined, the Security Council must not bury its head in the sand. At the very least, it must keep pace with trends outside the Council and strengthen its engagement in response to the real and present threats from cyberspace. Just as the Security Council and the General Assembly work in synergy when it comes to discussions on small arms, terrorism and non-proliferation, the Security Council and the General Assembly can likewise carve out complementary roles on cybersecurity.

While there is as yet no authoritative approach to the path forward, the Republic of Korea would like to make the following three suggestions for the Security Council's consideration.

First, the Council needs to have a clear diagnosis of the present situation. To that end, the Security Council can request a report on a regular basis to consider how cyberthreats intersect with the Council's mandate and how evolving cyberthreats impact international peace and security.

Secondly, the prescription that follows must encompass the whole range of the Council's files. Cybersecurity could be mainstreamed into the Council's agenda in a manner similar to other cross-cutting issues, such as women and peace and security, as well as youth and climate change. As many Member States pointed out at the Arria Formula meeting in April, there is a direct linkage between the malicious use of information and communications technology and the various issues under the Security Council's remit, including sanctions, non-proliferation and terrorism. In that vein, the Council can consider cybersecurity a major component that cuts across its regional and thematic files or issues.

Thirdly, and in the medium to long term, the Security Council should be able to come up with an appropriate treatment for the challenge. The Council can convene meetings on malicious cyberactivities that breach international law and harm peace and security. Furthermore, it could urge all relevant actors to use cybertechnology in a responsible manner and to pursue accountability through the tools at the Council's disposal. It goes without saying that the Security Council should develop a programme of work on cybersecurity in a way that complements the ongoing discussions in the General Assembly.

The Security Council has a history of charting its own agenda, in line with the emergence of new security challenges. Little did the architects of the Charter of the United Nations imagine that climate change, human rights abuses and the pandemic would become the province of the Security Council. The Security Council must confront cybersecurity head on if it is to remain relevant and agile in addressing one of the most pressing security challenges of our time. I sincerely hope that today's open debate will generate momentum to make that happen.

Before I conclude, let me just add one final point. The borderless nature of cyberspace exposes all nations — whether digitally advanced or vulnerable — to the harms of malicious cyberactivities. International security in cyberspace is only as strong as its weakest link. The humanitarian-development-peace nexus is therefore no less real in the cyberworld. A cyberspace free from malicious cyberactivities will facilitate digital development and unleash digital opportunities that ultimately contribute to the attainment of the Sustainable Development Goals. An open, secure, accessible and peaceful cyberspace in which cyberthreats can be effectively deterred will also protect freedom and human rights online.

I resume my functions as President of the Council.

I now call on Her Excellency Mrs. Linda Thomas-Greenfield, Permanent Representative of the United States and member of President Biden's Cabinet.

Mrs. Thomas-Greenfield (United States of America): I want to start by thanking the Republic of Korea for bringing us together again to discuss this critical issue and matter of peace and security. I want to welcome you here to the Security Council, Mr. President, and to express my strong appreciation. I had the honour of meeting you in Seoul during my visit some months ago, and it is wonderful to have you here. I thank the Secretary-General and the briefers for their briefings and welcome the other Ministers, who have honoured us with their presence today.

Since our previous gathering in April, we have continued to see the imperative of robust cyberspace security and, therefore, the need to discuss it in the Council. Cybersecurity enables our most basic systems to function — our economies and democratic institutions and, yes, even the United Nations itself. The United States is committed to working with all responsible actors to safeguard the benefits of cyberspace, build digital solidarity and leverage technology to meet the Sustainable Development Goals. And yet, far too many State and non-State actors have taken the opposite tack. Across the world, they have exploited digital connectivity to extort victims for profit, steal money and ideas from Governments and private entities, target journalists and human rights defenders, pre-position for future conflict and threaten our critical infrastructure, including here at the United Nations.

As a Council, we must work together to address the cyberthreats posed by non-State and State actors and strengthen the norms of responsible State behaviour, hold countries accountable for irresponsible behaviour in cyberspace and support victims affected by that behaviour and disrupt the networks of criminals behind dangerous cyberattacks around the globe. Already, there exists a framework for doing so. The framework for responsible State behaviour in cyberspace, adopted repeatedly and by consensus, makes clear that international law applies to cyberspace and that States are expected to uphold voluntary norms of State behaviour during peacetime. Among those norms is the expectation that States investigate and mitigate malicious cyberactivity emanating from their territory aimed at the critical infrastructure of another. And yet, some of those who have endorsed that framework nevertheless choose to ignore — or worse, empower — bad actors.

That is highlighted in April's Arria Formula meeting on cybersecurity, which includes malicious cyberoperations carried out by the Democratic People's Republic of Korea that are used to fund its weapons of mass destruction and ballistic missile programmes. And it includes Russia's cyberactivity in Ukraine, Germany, Czechia, Lithuania, Poland, Slovakia and Sweden, where, among other activities, Russia's General Staff Main Intelligence Directorate has targeted political parties and democratic institutions. Not only that, but the Russian Government has also served as a safe haven for ransomware actors, who, in recent years, have caused billions of dollars of losses and significant damages to hospitals and other critical infrastructure.

For our part, in February, the United States and the United Kingdom announced operations to disrupt the LockBit ransomware group, which has targeted 2,000 victims and has made ransom demands totalling hundreds of millions of dollars, more than $120 million of which were paid out. In recent months, we unsealed an indictment charging Russian nationals Artur Sungatov and Ivan Kondratyev, also known as Bassterlord, with deploying LockBit against numerous victims across the United States and internationally. That comes in addition to efforts through the International Counter Ransomware Initiative that we set up in 2021, which is now the largest cyberpartnership in the world. As individual States, through that partnership and in multilateral forums, including the United Nations, we call on all States to do their part to implement the framework and to promote peace and stability in cyberspace. And we call on the Council to ensure that cybersecurity is a cross-cutting priority that is considered in every aspect of our mandate. Whether it is considering how peacekeeping operations can promote good cyberhygiene to limit risks or better understanding how cybersecurity could enhance non-proliferation efforts, the Council must continue to view challenges through the lens of cybersecurity.

We have the ability to protect our most critical infrastructure and all those who count on it. And we have the potential to safeguard the benefits of cyberspace for all. And so, with the framework for responsible State behaviour in cyberspace as a guide, let us reaffirm the applicability of international law to State-on-State behaviour. Let us promote adherence to voluntary norms of responsible State behaviour in peacetime and help to reduce the risk of conflict arising from cyberincidents. And let us uphold the rules-based international order and ensure that the digital world influences the physical world for the better.

I thank you again, Mr. President, for bringing us together to discuss this important issue.

Mr. Persaud (Guyana): I thank His Excellency Mr. Cho Tae-yul, Minister for Foreign Affairs, and the presidency of the Republic of Korea for organizing today's open debate on addressing evolving threats in cyberspace. I also thank the Secretary-General and the briefers for their insightful contributions to the discussion.

Rapid technological advancements have created a world of limitless possibilities, with enormous economic, social and geopolitical benefits. However, as digital technologies become more sophisticated and are deployed by malicious actors, they pose unprecedented risks to both human and national security. The malicious use of digital technologies has also demonstrated the potential to disrupt institutions and to pose regulatory and policy challenges related to governance. Moreover, the transnational nature of cyberthreats has rendered traditional notions of national security and defence obsolete.

The cybersecurity threats to which we are now exposed can have a crippling impact on the health, safety and security of our citizens and the functioning of essential services. As the contemporary threats to cybersecurity become more sophisticated and multifaceted, ranging from State-sponsored cyberespionage, interference in democratic processes, human rights violations, attacks on critical infrastructure and the spreading of misinformation, disinformation and hate speech, so too must our response.

In that regard, I suggest three areas for consideration.

First, there must be accountability and oversight mechanisms to guard against cyberattacks. In that regard, we note recent discussions on whether cyberattacks targeting critical infrastructure, such as medical facilities or power plants, with grave consequences for life, can amount to war crimes, crimes against humanity, genocide and/or the crime of aggression. That must be thoroughly examined and included in a global legal framework that must also ensure that digital tools and technologies are developed and used with due regard for ethical considerations and respect for human rights. In that regard, Guyana recognizes the importance of concluding the work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes and the need for a widely ratified convention.

Secondly, we must prioritize cooperation, collaboration and partnerships to build cybersecurity capacity and resilience and to investigate and prosecute cybercrimes across countries and regions. In terms of partnerships, we must invest in building trust and enhancing regional and international collaboration to foster knowledge-sharing, information exchange and technology transfer. We must also seek to develop interoperability among our national, regional and international systems that deal with the tracking and monitoring of cybersecurity threats. To be effective, a global framework must be developed which caters for intelligence-sharing among States and relevant stakeholders on the emerging threats to cybersecurity. While ongoing discussions within the United Nations and regional mechanisms have contributed positively to that endeavour, including within the framework of the Secretary-General's Road Map for Digital Cooperation and the Sustainable Development Goal Digital Acceleration Agenda, there remains a lot of work to be done. We must also capitalize on the opportunities provided in the cyberdomain to adopt a whole-of-society approach to counter cyberthreats and bolster cybersecurity.

New technologies such as artificial intelligence systems can help to identify and mitigate such threats. In that regard, as Governments we must redouble their efforts to collaborate with technology companies and the private sector to develop stronger security tools and policies and to enhance information-sharing in the analysis of threat intelligence. Furthermore, many developing countries such as Guyana lack the necessary resources and expertise to combat cyberthreats and build resilience. Building technical capacity in such countries must be viewed as an investment in our collective security that would serve to remove existing inequalities and imbalances in cybersecurity capabilities. Considering that, as a global community we can explore the possibility of setting up a global fund that caters for training and capacity-building, as well as software and hardware development. Furthermore, Guyana calls on developed countries with advanced technological capabilities to provide technical assistance and funding to enhance cybersecurity infrastructure and response capabilities in developing countries. No effort should be spared in ensuring that no single country or entity monopolizes the technological tools and capacities which could further exacerbate the vulnerabilities of developing countries, for instance through the imposition of laws and regulations with an extraterritorial impact.

Thirdly, notwithstanding the ongoing processes within other United Nations forums, the Security Council must be a part of the cybersecurity dialogue, given the threat posed by malicious cyberactivity in the international maintenance of peace and security. The Council must therefore intensify its discussion of

that issue by building on the Arria Formula meetings and open debates, including the current debate, to raise awareness of emerging threats posed by new technologies and explore collectively effective measures that can be deployed against the malicious use of such technologies.

In closing, the challenges posed by cybersecurity threats are daunting but not insurmountable. Through our collective effort and will and concerted action, we can build a resilient and secure digital world that fosters trust, innovation and prosperity for all. Let us seize the moment, not merely to respond to the threats before us, but to proactively shape a future to ensure that no one is left behind. Guyana stands ready to work with all Member States towards that endeavour.

Mr. Nebenzia (Russian Federation) (*spoke in Russian*): We are glad to see you, Mr. President, presiding over the Security Council. We thank the Secretary-General for his briefing. We also listened carefully to the briefers.

Russia was present at the start of discussions of issues of international information security at the United Nations. In 1998, 26 years ago, we raised the topic for the first time in the General Assembly, through the introduction of the first resolution (General Assembly resolution 53/70) on that specific topic. The adoption of resolutions on that topic has since become an annual event supported by the overwhelming majority of Member States.

On our initiative, the relevant United Nations Group of Governmental Experts was established to discuss security issues in the use of information and communication technologies (ICTs). Later, it evolved into an inclusive format — the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies — which is a unique and unified negotiation platform under United Nations auspices for discussing all issues of international information security.

Over the course of its activities, the Open-ended Working Group has proven effective and relevant. Its practical results include the launch in May — at Russia's initiative — of a directory of points of contact for exchanging information on computer attacks or incidents. A detailed review of existing and potential threats in the area of international information security is under way. Concrete steps are being taken to build the digital capacity of States. Last year, universal principles for assistance in that area were agreed upon.

We believe that the efforts of the international community should be focused on continuing to strengthen cooperation among States within the framework of the Open-ended Working Group in order to achieve concrete, practical results to ensure international information security. We believe it is crucially important to consolidate and build upon the results achieved by the Open-ended Working Group, both within the framework of its current mandate and a future negotiating format. Russia has already presented its vision for a permanent inclusive mechanism in that area. We believe it would be wise to preserve our common gains by establishing a permanent open-ended working group with a decision-making function after 2025.

The above facts clearly demonstrate that the United Nations has a long record of consistent, incremental work on international information security. Therefore, the need to involve the Security Council raises serious questions. The topic has its own specificities and should be discussed in specialized forums where there is the relevant expertise. It is crucial to keep discussions professional and constructive and avoid politicization. Duplicating the efforts of the international community and spreading the topic across various United Nations forums is counterproductive and could reverse all the results achieved over decades under the auspices of the General Assembly.

Equally important is the fact that the Open-ended Working Group's discussions are inclusive. All United Nations Members can participate without exception and on an equal footing, as decisions are made by consensus. Transferring the subject to the Security Council would automatically exclude from decision-making all States that are not members of the Council. Those who today supported the presidency's call to make international information security part of the Security Council agenda should obviously bear that in mind.

Finally, any discussion of potential risks must take into account the technological peculiarities of cyberspace. Unlike in the physical world, threats in cyberspace are extremely difficult to identify, and identification of the source of an attack — so-called attribution — is even more difficult. It often takes a long time to become aware, through circumstantial evidence, of the fact that an attack has taken place. Therefore, we do not yet have even a basic understanding of which cases

of malicious use of ICTs can be confidently considered direct threats to international peace and security. Until the problem of attribution is resolved, and a unified approach is developed to other complex aspects of that multifaceted and specific problem, including legal ones, any discussion in the Security Council could turn into another exchange of unsubstantiated allegations and deepen the divide in the international community. That would undermine the authority of the Council and would in no way help to develop constructive solutions.

All States that have spoken or that will speak today are participants in the Open-ended Working Group, and the issues proposed for discussion are similar to those discussed by the Group. In May, a ministerial-level round table on capacity-building in the area of international information security was held, and the eighth session of the Open-ended Working Group will take place in July. In fact, discussion of the topic is already under way, and its progress and results are available to all.

Therefore, we do not support the call to raise the awareness of the international community of the issues of international information security through the convening of regular meetings of the Security Council. The mandate of the Security Council envisages a prompt response to real threats to international peace and security, rather than a philosophical exchange of views on common topics in the public domain. There are other forums and formats for that.

The attempts by Western colleagues to make allegations about malicious activities using ICTs and then use them as leverage against "undesirable" States are also extremely concerning. What is more, they never offer any convincing evidence to back up those words.

The Panel of Experts on the Democratic People's Republic of Korea of the Security Council Committee established pursuant to resolution 1718 (2006) has repeatedly served as a tool in that unscrupulous game. Based on a tip from one specific Member State, the Panel approached the Russian side regarding computer attacks attributed to Pyongyang. When we asked for the precise data necessary to investigate the alleged incidents, the experts replied that they had not received any additional information from their "sources". However, the lack of any details does not prevent our Western colleagues from baselessly accusing countries that disagree with their actions of all "cybersins". Usually, such accusations are characterized as "highly likely", which is the favourite expression of Western countries. Such unsubstantiated insinuations are unacceptable. Attribution of responsibility requires a professional approach and comprehensive technical evidence.

We categorically reject any speculation that Russia allegedly encourages malicious acts online. For a quarter of a century, we have been advocating the prevention of the militarization of the online space, and we started to propose concrete steps in that area long before Western countries even recognized that such a risk existed.

Our country's priority is the establishment of universal legally binding instruments on cybersecurity, which will contribute to preventing of inter-State conflicts in that area. To that end, in 2023 Russia submitted to the General Assembly a prototype of a specialized international treaty. It was a concept for a United Nations convention on ensuring international information security. Not only would the adoption of such a universal agreement make it possible to legally set out the rights and obligations of countries related to their activities in the ICT sphere, but it would also regulate the question of political attribution of computer attacks in international relations. It would also help to ensure full compliance online with the principle of the sovereign equality of States, which, at present, is being openly ignored by many technologically advanced countries. We invite all Member States to engage in a substantive discussion on the basis of our proposal at the General Assembly.

Unfortunately, Western countries, primarily the United States, reject that idea, trying to preserve as much free rein for themselves as possible. That becomes especially evident in view of the fact that high-ranking United States officials recognize that offensive attacks were carried out against Russia using ICTs. It is also reflected in the fact that the doctrines of Washington and NATO stipulate "offensive" — in fact, aggressive — approaches.

Our briefers today and the delegations that took the floor earlier spoke about cyberattacks. However, they forgot to mention that an unprecedented disinformation war is being waged against Russia. All that malicious activity is coordinated from Great Britain by organizations based in London, namely, the "Public Relations and Communications Association" and "PR Network", as well as "IT Army of Ukraine", the last of which is working tirelessly on the disinformation field. Through the efforts of those IT resources, tons

of disinformation and lies about Russia and the Russian special military operation are being disseminated.

We are also worried about the attempts to water down global discussion on countering the use of ICTs for criminal purposes. A clear example of that is the "Counter Ransomware Initiative". Such "exclusive clubs", which do not particularly hide their politicized aims, undermine the efforts of Member States to develop universal mechanisms to fight the use of ICTs for criminal purposes, in particular, through the specialized United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

For more than 26 years now, the Russian Federation has been promoting a constructive agenda in the area of international information security, making its own contribution to maintaining peace and stability, both in the real world and online. We will continue to advocate for the creation of a peaceful and secure ICT environment on a global scale.

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.

Mr. Afonso (Mozambique): Mozambique wishes to convey its gratitude to you, Mr. President, and to the Republic of Korea, for the pertinent choice of this important theme as the signature event of its presidency of the Security Council for the month of June. We are deeply grateful to the Secretary-General for his extremely insightful approach to the topic, an approach that is so well and aptly aligned with the Charter of the United Nations. We have followed with great attention the important perspectives provided by Mr. Stéphane Duguin, President of the CyberPeace Institute, and Professor Nnenna Ifeanyi-Ajufo, Professor of Law and Technology.

We extend our greetings to the Ministers and high-level dignitaries present in the Chamber today.

All the statements made thus far bear testimony to the fact that the boundaries between cyberspace and the physical world continue to blur rapidly. As a consequence, virtually all aspects of our modern life have migrated to, and are relying on, digital technology. The imperative of the Council's involvement is therefore supported by the fact that many countries, big and small, seriously consider cyberspace — which has no borders — to be a domain of possible conflict, alongside the land, sea, air and space dimensions.

As a matter of fact, we may consider that a starting point was established in 2013, when the General Assembly agreed that international law, including the United Nations Charter, does apply to cyberspace. Nonetheless, the global diplomatic conversation about the rules of engagement in cyberspace has, thus far, made slower progress. In that connection, discussions under the auspices of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies have yet to yield results.

The landscape and scope of cyberthreats are rapidly evolving, with the speedy progress of artificial intelligence and with significant threats posing new challenges to national and international peace, security and stability. With cyberthreats on the rise, hardly a day goes by without a report of a ransomware attack against public or private entities, the proliferation of artificial intelligence-generated deepfakes that look very real or a denial-of-service attempt against parts of a country or its essential services, such as finance, health care, electricity grids, e-Government and other critical infrastructure. As the tools developed to make modern life possible are misused and weaponized, cybercrime has emerged as one of the most significant threat multipliers, undermining public trust in institutions and amplifying political and social tensions.

To compound those challenges, intensifying geopolitical competition has become a driving force in cybersecurity. Adversaries are striving to acquire military and intelligence cybercapabilities, triggering a cyberarms race amid increasing accusations, attributions, retaliation and escalation. As cybersecurity becomes more entangled with geopolitics, the prospects for progress towards an international agreement on better cybersecurity norms continue to stall or even recede. Such immobility or lack of progress on a matter that is so important to humankind risks undermining our collective security.

Given the fast-evolving threat landscape and the absence of agreed rules of engagement, the Security Council should agree to undertake, as a matter of urgency, several specific roles and actions that include the following.

First, it should set international norms and frameworks for the responsible behaviour of States and private entities in cyberspace, based on global cooperation.

Secondly, in the spirit of fostering our collective security, the Council could support capacity-building initiatives to enhance the cyberdefence capabilities of Member States, particularly those with limited resources.

Thirdly, the Council could promote situational awareness briefings and facilitate the sharing of threat intelligence and best practices among nations to improve our common cybersecurity resilience.

Fourthly, cyberthreats should be intrinsically linked to other Security Council agenda items, such as counter-terrorism, election interference, the protection of critical infrastructure and the safeguarding of peace operations and humanitarian action.

We believe that it is crucial to update and broaden the debate on cybersecurity. Issues related to the theft of ideas, data, intellectual property, human rights and privacy, as well as design parameters for critical consumer products and public utilities, deserve equal attention. For countries such as Mozambique, it is essential that the voices and perspectives of the global South be heard in the global discussion on cybersecurity. Having a diversity of perspectives at the table and avoiding one-size-fits-all approaches are crucial for making global progress towards a fairer and more resilient governance framework. By encouraging discussions such as the one we are having under the presidency of the Republic of Korea, the Council can play a pivotal role in safeguarding international peace and security in the digital age. Mozambique pledges to remain engaged.

Mr. Kanu (Sierra Leone): I thank you, Mr. President, for convening this important open debate. I also thank His Excellency Mr. António Guterres, Secretary-General, for his insightful brief. We also thank Mr. Stéphane Duguin and Ms. Nnenna Ifeanyi-Ajufo for their insights. We welcome the participation of the high-level Ministers in this meeting.

Sierra Leone appreciates the opportunity to speak on the critical issue of addressing evolving threats in cyberspace, while recognizing the immense benefits and interconnected challenges that information and communications technologies (ICTs) present to international peace and security. We also recognize the fundamental development challenge of addressing the global digital divide and the risk of the deepening of the divide with the proliferation of artificial intelligence (AI), particularly generative AI.

In this statement, Sierra Leone will speak specifically to the guiding questions. The key emerging and evolving trends of malicious activities in cyberspace that pose challenges to international peace and security include the proliferation of malware, decoy ransomware, ransomware-as-a-service models and cryptocurrency heists. Those activities pose a significant risk to civilian populations and have devastating effects on national security and the overall stability of our countries, posing significant risks to international peace.

We are deeply concerned about the evolving tactics being employed in cyberspace, which not only fuel terrorist activities but also jeopardize the integrity of financial systems and critical services. We stress that the increasing use of ransomware-as-a-service models and cryptocurrency thefts to support nefarious activities highlights the pressing need for enhanced cooperation and capacity-building to combat those threats effectively. The recent escalation in the frequency and scope of ransomware attacks, targeting critical infrastructure and essential public services, demonstrates the severe impact of cyberthreats on public safety and political stability and requires continued vigilance. Sierra Leone is deeply concerned about the implications of cyberthreats, including the use of cybercrimes to fund illicit activities and evade international sanctions. They all underscore the urgent need for enhanced international cooperation and capacity-building efforts to combat those threats effectively. We call for increased collaboration among Member States to bolster the Security Council's capacity to respond effectively to malicious activities in cyberspace, particularly those threatening critical infrastructure, humanitarian operations and the protection of civilians. A holistic approach is essential in maintaining peace and security in the digital era.

It is our considered view that the malicious use of ICTs acts as a threat multiplier when they exacerbate existing conflicts and challenges. The increasing prevalence of malicious cyberactivities targeting critical infrastructure, including hospitals and other health-care systems, financial services, the energy sector, satellites, transportation and other emergency

systems, underscores the urgent need for concerted global action to safeguard our digital networks and systems and the importance of the Security Council's engagement in addressing those issues and managing and resolving conflicts that involve cyberelements.

As we have heard already, despite its huge benefits, AI can be weaponized to enhance the scale, speed and sophistication of cyberattacks. Autonomous systems can conduct continuous and adaptive attacks, learning from their environment to exploit vulnerabilities more effectively. Such AI-driven attacks can target critical infrastructure, financial systems and even individual privacy, resulting in widespread disruption and damage. However, we also recognize that leveraging AI for cyberdefence can help us to stay ahead of emerging threats. AI can enhance threat detection, response times and incident management. By investing in AI-driven defensive technologies, we can build more resilient cyberinfrastructure. By investing in capacity-building and technology transfer, we can level up the capabilities of developing States Sierra Leone is of the view that the Security Council can play a pivotal role in addressing the evolving nature of cyberthreats and promoting international peace and security through comprehensive engagement with the relevant General Assembly committees and specialized agencies and bodies.

Over the past decade, the Security Council has become increasingly seized of the international peace and security implications of cyberspace. Since 2016, the Council members have convened several Arria Formula meetings, during which States addressed cybersecurity, with various linkages to topics such as the protection of critical infrastructure, the protection of civilians and disinformation and hate speech in cyberspace.

Sierra Leone therefore commends Estonia for convening the first high-level open debate on the topic during its presidency in June 2021. In the light of the Security Council's growing focus on cybersecurity, we support the proposal to convene regular briefings to assess the evolving cyberthreat landscape, incorporating insights from diverse stakeholders in order to ensure a comprehensive understanding of emerging challenges and to stay ahead of them. We emphasize the need for effective Council coordination, cooperation and engagement if we are to combat cyberthreats comprehensively.

We underscore that the engagement of the Security Council can take place in a manner that is complementary to other ongoing United Nations processes on ICTs, including relevant discussions on norms of responsible State behaviour in the use of ICTs and the United Nations framework for responsible State behaviour in cyberspace, which was adopted by consensus, under the auspices of the General Assembly.

Developing assessment and strategies on the evolving cyberthreat landscape by incorporating comprehensive insights from the United Nations system, private sector, civil society and academia would ensure that the Security Council remains abreast of new developments and their implications for international peace and security.

Recognizing the linkages between cyberthreats and other agenda items of the Security Council, Member States should explore ways to effectively mainstream cyber and ICT-related concerns into the Council's existing body of work. Sierra Leone suggests mainstreaming cyber-related concerns into the Council's discussions on various thematic files, including peacekeeping missions, Council-mandated sanctions and non-proliferation and counter-terrorism efforts.

Strengthening national cybersecurity capabilities and promoting international cooperation are vital components of that approach and could also be integrated into each of those lines of effort. By integrating considerations of cyber-related themes into its work, the Council can better address the complex challenges posed by cyberthreats in a comprehensive and holistic manner.

For our part, the creation of the National Computer Security Incidence Response Coordination Centre in Sierra Leone has led to the centralization of the mandate to address all cybersecurity issues, including responding to cybersecurity incidents in Sierra Leone.

Since its establishment, the Centre has achieved significant milestones in bolstering the nation's cybersecurity resilience through a multifaceted approach to capacity-building and collaboration. Significant activities include capacity-building initiatives focused on cybersecurity and crime. The Centre has played a pivotal role in raising awareness and providing training programmes for various stakeholders, collaborating with regional and development partners to conduct specialized trainings for the judiciary and law enforcement agencies on cybercrime and electronic evidence, knowledge transfer and the sharing of best practices in cybersecurity

and cybercrime investigations. Such collaborations enhance the collective capability to effectively combat global cyberthreats through the strengthening of national capacities.

Firstly — and regrettably — let me conclude by noting the increasingly brazen cyberthreats directed at our multilateral, international and judicial institutions. In that regard, Sierra Leone unequivocally condemns attacks directed against the International Criminal Court. One such attack was described by the Court as a "targeted and sophisticated attack with the objective of espionage and can therefore be interpreted as a serious attempt to undermine the Court's mandate". As a State party, Sierra Leone reiterates its commitment to uphold and defend the principles and values enshrined in the Rome Statute and to preserve its integrity from any interference and pressure against the Court, its officials and those cooperating with it.

Secondly, let me reaffirm Sierra Leone's commitment to promoting cybersecurity as a fundamental aspect of international peace and security and working collaboratively within the Security Council and the broader international community to address the complex and evolving threats in cyberspace posed by malicious activities.

Mr. Bendjama (Algeria): I thank you, Mr. President, for organizing this important open debate on the growing risks of cyberthreats to global security. I also thank the Secretary-General and the briefers for their presentations on the worrying increase in harmful cyberactivities.

Ransomware attacks on critical infrastructure and the theft of digital assets and data put public safety and political stability at risk. The involvement of both governmental and non-governmental actors makes the situation even more complex and dangerous. The spread of disinformation on online platforms fuels division, hatred, intolerance and, ultimately, terrorism, with false information interfering in State affairs hampering cooperation and, ultimately, threatening peace and security in the world.

New technologies, including artificial intelligence, are making cyberthreats even worse and harder to deal with. We therefore need to address those challenges, globally and urgently. Considering those realities, I want to emphasize several key points.

First, the principles of the Charter of the United Nations should apply equally to cyberspace. Information and communications technologies must be used in accordance with those principles.

Secondly, we are striving to ensure an open and secure cyberspace, which is essential for achieving the global development goals of the 2030 Agenda for Sustainable Development. For that reason, we need a legally binding framework created within the United Nations.

Thirdly, we must help developing countries to build protection against cyberthreats and close the digital gap. Building their abilities is essential for securing cyberspace for all nations and should be a top priority.

Fourthly, the international community must work together to fight the spread of false information online. Governments are involved parties, and involved parties must cooperate following international law. International cooperation is key in our endeavour to effectively fight ever-changing cyberthreats.

Fifthly, we need to strengthen the legal framework to prevent and punish cybercrime. In that regard, I would like to highlight that my country plays an active role in international efforts to fight the harmful use of technology for criminal activities. That is especially clear in Algeria's leadership of the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. We hope that that Committee will achieve successful outcomes at its next session this summer.

In conclusion, Algeria strongly supports the role of the United Nations in dealing with issues related to the use of information and communications technologies that affect international peace and security. The Open-ended Working Group on Security of and in the Use of Information and Communications Technologies and the General Assembly are essential platforms for inclusive discussion of cyberthreats. They ensure that all Members can participate in shaping the global response to cybersecurity challenges, and we reiterate our commitment to supporting their valuable work.

Mr. Žbogar (Slovenia): I extend my thanks to the Republic of Korea for organizing today's debate. I would also like to thank the Secretary-General for his briefing, and I would like to thank our briefers today for their insights and recommendations.

Allow me to address two points that are pertinent to the topic of today's debate.

First, on evolving threats in cyberspace, it is our view that having an accurate understanding of the ever-evolving cyberthreat landscape, particularly in the context of the rapid growth of emerging technologies, such as artificial intelligence, is paramount for discussing the cooperative measures that the international community can take in response to malicious cyberactivities. In that regard, we commend the ongoing work of the dedicated Open-ended Working Group on Security of and in the Use of Information and Communications Technologies established by the General Assembly, but we also recognize the complementary potential for enhanced consideration by the Council, for instance, by addressing the findings of the Secretary-General's report on cyberthreats (A/77/92). Malicious cyberactivities, such as ransomware attacks and attacks targeting critical civilian infrastructure, particularly when transboundary in nature, can pose new challenges and exacerbate existing threats to international peace and security.

That brings me to my second point, namely, addressing the evolving threats in cyberspace. The Council bears the primary responsibility for the maintenance of international peace and security. In order to fulfil its responsibility in accordance with its mandate, the Council should play a decisive role in de-escalating tensions and promoting accountability when malicious cyberactivities threaten international peace and security. In our view, activities that support terrorism or the proliferation of weapons of mass destruction or that exacerbate existing conflicts or target critical civilian infrastructure, pose such a threat and thereby warrant the Council's response. In the same vein, the Council should address malicious cyberactivities, such as disinformation campaigns, that incite violence against civilian populations, cause humanitarian suffering or disrupt the work of humanitarian organizations, peacekeeping and peacebuilding operations.

In an era marked by the growing digitalization of conflicts, it is crucial to emphasize the applicability of international law, including international humanitarian law and international human rights law, which must be respected.

Allow me to conclude by assuring the Council of our commitment to collaborate with Council members and the broader United Nations membership in continuing discussions on cyberthreats to international peace and security. We also remain steadfast in our commitment to implement measures aimed at mitigating those risks, including by implementing the existing norms of responsible State behaviour in cyberspace.

Mrs. Frazier (Malta): I begin by thanking the Republic of Korea for organizing this open debate on this highly topical and important issue. I also thank the Secretary-General and the briefers for their insightful briefings.

Malicious cyberactivities present multifaceted challenges that can have serious impacts on the maintenance of international peace and security. Those range from ransomware attacks on government institutions, critical infrastructure and essential public services to the unauthorized access and use of electronically stored data.

We are alarmed by the malicious cyberactivities targeting government institutions and democratic processes, often with the direct intent to undermine stability and security and to erode trust in the outcome of democratic elections. The growing reliance on digital technologies by women human rights defenders and other activists increases their risk of exposure to online harassment and attacks. Furthermore, human rights and fundamental freedoms, including freedom of expression and assembly, are being increasingly restricted by strict surveillance, Internet shutdowns and bandwidth throttling. At the same time, digital platforms are often exploited to spread disinformation, misinformation and hate speech, including misogynistic, homophobic and radicalizing content.

Our collective efforts to promote stability in this domain must be rooted in human rights, both online and offline. Cyberpolicies must be conflict-sensitive, age-sensitive and gender-responsive in order to detect and prevent the harmful impacts of digital security threats, such as gender-based violence that is facilitated by technology. Women's full, equal, safe and meaningful leadership and participation in cyberdecision-making is crucial, especially in conflict and post-conflict contexts.

We reaffirm that international law, in particular the Charter of the United Nations, is applicable to activities in cyberspace, as recognized by the General Assembly. In the same vein, the framework of responsible State behaviour in cyberspace provides agreed guidelines for Member States. The framework should be upheld by

all Member States, and we support the establishment of a programme of action to ensure continued and institutionalized dialogue. In addition, we call upon all States to exercise diligence, take appropriate measures in line with the norms of the framework for responsible State behaviour in cyberspace, and refrain from participating in or aiding malicious cyberactivities originating from their territories.

State-sponsored malicious cyberactors exploit ransomware and digital thefts to generate illicit revenues. Those include attacks against critical infrastructure, financial institutions and cryptocurrency firms. Cyberattacks and crimes know no borders, and no country is immune to them. Reports estimate that, in 2023 alone, malicious cyberactivities perpetrated by hackers sponsored by the Democratic People's Republic of Korea have generated the equivalent of $1 billion. The regime utilizes those revenues to fund its illegal weapons of mass destruction programme, which threatens peace and security in the peninsula and beyond. Those activities have been well documented in the reports of the Panel of Experts of the Committee established pursuant to resolution 1718 (2006), which played an invaluable role in investigating those crimes.

To conclude, the Security Council can play an important role in addressing the issue of cybersecurity. Its efforts can and must be complementary to other cybersecurity forums based in the General Assembly, including its Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. The Council can serve as a powerful platform to reinforce agreed principles and enhance further discussions. It should promote an open, secure, accessible and peaceful cyberspace. We will continue to support its renewed engagement on that topic.

Mr. Yamazaki (Japan): I extend my sincere gratitude to you, Mr. President, for your leadership in convening this significant and timely open debate and to the Secretary-General and the briefers for their invaluable insights.

At the outset, Japan would like to express its commitment to promoting a free, fair and secure cyberspace. In recent years, we have witnessed a concerning trend of a qualitative and quantitative increase in cyberoperations used for malicious purposes, including ransomware attacks, damage to critical infrastructure, interference with democratic elections and the theft of sensitive data. The alarming rise in cryptocurrency theft also poses a clear and present threat to international peace and security, potentially financing illicit weapons programmes. In particular, it is well known that North Korea is financing its weapons of mass destruction and ballistic missile programmes through malicious cyberoperations, and the international community must urgently tackle such threats, as reported by the Panel of Experts of the Committee established pursuant to resolution 1718 (2006). Furthermore, the proliferation of commercial cyberintrusion tools, such as spyware, raises profound concerns about their impact on national security, human rights and international peace and security. The stakes have never been higher.

To address those alarming challenges and ensure a free, fair and secure cyberspace, we should uphold the rule of law in cyberspace by advancing concrete discussions on applying existing international law and implementing the agreed norms, rules and principles of responsible State behaviour. We should also place great importance on sharing information on existing potential threats, sharing best practices and promoting capacity-building efforts. Through dialogues at all levels, we should aim to foster trust, reduce threats and, most importantly, reduce miscalculations. Under the United Nations framework, Japan will continue its constructive engagement in the current Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. Japan also believes that, as an action-oriented framework, the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security should serve as a future permanent platform to support the implementation of the agreed norms, rules and principles for responsible State behaviour.

At the same time, Japan fully agrees that the Security Council, which bears primary responsibility for the maintenance of peace and security, needs to have a greater and complementary role in the field of cybersecurity. The Council must closely monitor serious cyberincidents with grave consequences for international peace and security, including those targeting critical infrastructure. Regular Council briefings would be very useful to keep track of the evolving threat landscape in information and communications technology (ICT) security. In addition, the Council needs to address growing cyberthreats to the global arms control and non-proliferation regime,

including proliferation risks potentially posed by non-State actors.

In conclusion, Japan reaffirms its unwavering commitment to safeguarding a free, fair and secure cyberspace. The Security Council must remain on high alert regarding emerging security risks associated with ICTs. We look forward to further discussions on the Council's next steps to effectively address this important topic based on today's debate, which has been held on your initiative, Mr. President.

Dame Barbara Woodward (United Kingdom): I thank Mr. Cho Tae-yul, Minister for Foreign Affairs of the Republic of Korea, for convening this debate and for bringing to the Security Council some clear ideas on how we can move our work forward in this area. I also thank the Secretary-General and our briefers today for setting out how cyberthreats can have an impact on international peace and security.

I will touch on three trends of importance to the United Kingdom.

First, as we heard, ransomware can disrupt government functions and the provision of vital public services. That creates conditions for instability when it occurs at scale or for sustained periods, which, as the Council knows, can have an impact on peace and security. Any State can be a victim of ransomware. That is why an international response is needed to constrict the ecosystem that facilitates it and to enable all States to increase their resilience and response capability. The United Kingdom is playing a leading role alongside Singapore as co-Chairs of the policy pillar of the Counter Ransomware Initiative. We urge others to join the initiative.

Secondly, as the use of artificial intelligence (AI) systems in our societies grows, we need to understand how cyberthreats will change, while identifying opportunities for AI to support our cybersecurity goals. Malicious and irresponsible actors can exploit vulnerabilities in AI systems to induce specific behaviour or manipulate its decision-making. To maintain international peace, AI systems will have to be secure by design. That is why the United Kingdom held the first ever Council debate on AI last year during our presidency (see S/PV.9381), and it is why we published guidelines for secure AI system development alongside the United States and a cross-regional group of 18 States.

Thirdly, malicious and irresponsible actors are also able to take advantage of the growing market in advanced cyberintrusion capabilities, leading to a more unpredictable threat landscape for us all. The United Kingdom and France invite international partners to join us in the multi-stakeholder Pall Mall Process as we consider approaches towards that shared concern.

In that context, we must continue to raise awareness of cyberthreats. For example, we are very concerned about the Democratic People's Republic of Korea's use of malicious cyberactivities to obtain cryptocurrencies to fund their illegal weapons programme. That is why we must redouble our efforts to ensure the effective implementation of the Democratic People's Republic of Korea's sanctions regime.

Finally, cyberthreats also increase disinformation risks. That is clearly a major challenge to our work. For Russia to accuse the United Kingdom of running a disinformation war is astonishing when its own disinformation machine has been so obviously and clearly exposed, including here at the United Nations. We were not the delegation that brought to the Chamber and to the Internet the conspiracy of weaponized bats and ducks.

Cyberthreats will present an ever-greater number of risks to international peace and security, and governments need to evolve in order to address them effectively. As part of that, the United Kingdom remains committed to upholding the United Nations framework for responsible State behaviour in cyberspace and to working with others through capacity-building and by enabling public-private partnerships.

Mrs. Chanda (Switzerland) (*spoke in French*): I thank the Republic of Korea for organizing this important debate on threats to cybersecurity. I also thank the Secretary-General, Professor Nnenna Ifeanyi-Ajufo and Mr. Stéphane Duguin, Chief Executive Officer of the CyberPeace Institute in Geneva, for their briefings.

Switzerland is witnessing two decisive developments in cyberspace that are of concern to us. On the one hand, the increasing digitization of conflicts and the use of cyberoperations in armed conflicts are transforming the nature of those conflicts. On the other, the growing intensity of attacks by ransomware and State-sponsored cyberattacks against critical infrastructure is a major concern for Switzerland. The use of ransomware to extort currency and cryptocurrencies or the targeting of critical infrastructure threatens to paralyse key structures in our societies. These activities also affect

the international community's ability to achieve the Sustainable Development Goals, owing to the heightened vulnerability of developing countries. They can pose a threat to international peace and security, and therefore fall within the mandate of the Council.

The concept note proposed by the Republic of Korea (S/2024/446, annex) asks what role the Council can play in addressing threats arising from malicious activities in cyberspace. Allow me to outline some options in this regard.

First, the Council should regularly take note of current cybersecurity developments and threats. Given the multidimensional implications and geographical scope of the issue, it would be appropriate for the Council to hold a regular briefing. The briefing could include presentations by representatives of United Nations entities, the private sector, civil society and academia, as well as other relevant entities. This awareness-raising would enable the Council to make fully informed decisions, in particular on specific geographical issues and in the context of peacekeeping operations.

Secondly, the Council should reaffirm certain established principles. We attach particular importance to the applicability of international law to cyberspace, and especially international humanitarian law to activities in cyberspace in the context of armed conflict. The Council should also emphasize the importance of State responsibility and due diligence and recognize the 11 norms of responsible State behaviour in cyberspace. These elements, complemented by confidence-building and capacity-building measures, constitute the framework for responsible State behaviour in cyberspace, a framework that has been adopted by consensus by all Member States. We would support a Council product that affirms this framework and thus contributes to rebuilding trust.

Finally, the Council's activities must be complementary to those of other bodies. It is not for the Council to develop rules of behaviour or agreements. That is the prerogative of the General Assembly and the expert processes it has mandated. The Council should focus its attention on developing its understanding of risks and their mitigation, including in specific cases.

The responsible use of cyberspace offers enormous opportunities to meet tomorrow's challenges, despite the recognized risks. In his New Agenda for Peace, the Secretary-General encourages us to find new ways to protect ourselves from these new threats. While the negotiations on the Pact for the Future provide us with an opportunity to develop a common understanding in this regard, the Council also has a key role to play. Today's debate confirms this.

Mr. Fu Cong (China) (*spoke in Chinese*): I thank you, Mr. President, for presiding over today's meeting. I thank Secretary-General Guterres for the briefing and the two experts for the presentations.

At present, we find ourselves in an unprecedented digital age, where the revolution of information technology is making rapid progress, digital economies and cybereconomies are flourishing, and the international community is seeing accelerated integration into a community with a shared future featuring intertwined interests and shared weal and woe. At the same time, risks and challenges in cyberspace are ever more serious. Cyberattacks, cyberespionage, cybercrimes and disinformation continue unabated. Cyberterrorism has become a global public menace. Cyberspace is increasingly militarized, camp-based and ideology-driven, and the digital divide among countries and regions continues to widen.

In cyberspace, while all countries enjoy common opportunities and have common interests, they also face common challenges and bear common responsibilities. The international community should deepen exchanges, enhance mutual trust, work together and jointly promote the governance of and international rule-making on cyberspace. China wishes to propose the following.

First, we need to build a more peaceful and secure cyberspace. Cyberspace is deeply integrated with the physical world and is an important anchor for the development of human society. It must never become a new battlefield. A certain country designates cyberspace as a domain of military operations, develops offensive military cybercapabilities, builds military cyberalliances, and pushes for the definition of rules of engagement in cyberspace. This will only undermine the mutual trust among countries, escalate risks of friction and conflict in cyberspace and threaten international peace and security. All parties should abandon the zero-sum game and cold war mentality, foster a vision of common, comprehensive, cooperative and sustainable security, firmly uphold the peaceful nature of cyberspace, effectively prevent the militarization of and and an arms race in cyberspace, address threats to cybersecurity through dialogue and

cooperation, and remain committed to realizing one's own security through common security.

Secondly, we need to build a more universally beneficial and prosperous cyberspace. Digital economies and cybereconomies have already become major engines for global economic growth. All countries should adopt more active, open, coordinated and inclusive policies, promote the application and popularization of information and communications technologies (ICTs) and ensure the openness, stability and security of the ICT industrial chain so that more countries and people can enjoy the dividends of the Internet. Developed countries should help developing countries enhance digital, Internet-driven and smart development, enhance the latter's capacity for risk prevention and emergency response, and ensure equitable access to key resources such as cyberinfrastructure technologies and computing power to minimize the digital divide and implement the Sustainable Development Goals of the 2030 Agenda for Sustainable Development. The practice of forming cliques along ideological lines, overstretching the concept of national security, erecting a digital iron curtain, seeking technological dominance and advantages, and even blatantly interfering with and suppressing the economic and technological development of other countries will only hinder the international community's efforts to promote the governance of cyberspace.

Thirdly, we need to build a more equitable and orderly cyberspace. Developing international rules on cyberspace acceptable to all is key to upholding lasting peace and stability in cyberspace. All parties should earnestly abide by the purposes and principles of the Charter of the United Nations, in particular principles such as sovereign equality, non-interference in internal affairs, non-use or threat of force and the peaceful settlement of disputes, and comply with and implement the United Nations framework for responsible State behaviour in cyberspace. At the same time, all parties should always uphold the role of the United Nations as the main channel and, on the basis of equal and extensive participation, translate long-standing international consensus into legally binding norms of behaviour in cyberspace. The constructive solutions proposed by China, such as the Global Artificial Intelligence Governance Initiative and the Global Initiative on Data Security can serve as blueprints for future rule-making on cyberspace.

Fourthly, we need to build a more equal and inclusive cyberspace. Diversity is the fundamental feature of the world and a driver of human progress. The Internet connects all countries, peoples and civilizations in ways never seen before and, naturally, should become an important platform for all of humankind to showcase diverse cultures and promote the development and inheritance of civilizations. We need to fully leverage ICTs, step up online exchanges in dialogue, encourage mutual understanding and amity among the people of all countries, promote tolerance and coexistence among different civilizations and better promote the shared values of humankind. We must be vigilant against the practice of a small number of countries of imposing their own values as universal values and even interfering in the internal affairs of other countries and disrupting their development and stability. We must resolutely oppose the use of cyberspace for spreading extremism, terrorism, disinformation and hate speech.

China is a witness to and a beneficiary of the development of the Internet. Today, it is home to nearly 1.1 billion Internet users. We have built the world's largest and most technologically advanced cyberinfrastructure and have put in place a sound system of policies for cyberspace governance. In recent years, China has been actively increasing its policy-related communication and experience-sharing with the global South; promoting practical cooperation in capacity-building in such areas as infrastructure, technology, law enforcement and emergency response; engaging actively on cybersecurity processes under frameworks including the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies; the Group of 20; the Asia-Pacific Economic Cooperation forum; the Brazil, Russia, India, China and South Africa group; the Shanghai Cooperation Organization and the Regional Forum of the Association of Southeast Asian Nations, among others; and making important contributions to promoting global cyberspace governance.

The information revolution as a trend of the times is surging forward. Cyberspace evokes the infinite hope of humankind for a bright future. China stands ready to work with the international community to build a more peaceful, secure, open, cooperative and orderly cyberspace and to join hands to build a community with a shared future in cyberspace.

Mr. De La Gasca (Ecuador) (*spoke in Spanish*): I would like to welcome the presence of Mr. Cho

Tae-yul, Minister for Foreign Affairs of the Republic of Korea. I also thank Secretary-General António Guterres for the information provided and the briefers, Mr. Stéphane Duguin and Ms. Nnenna Ifeanyi-Ajufo, for their briefings.

In an increasingly interconnected and interdependent world, cybersecurity is a global challenge that requires a coordinated and cooperative response from the entire international community.

The malicious use of information and communication technologies (ICTs) acts as a multiplier of threats to peace and security, including in the following areas.

First, it can affect critical infrastructure, such as health systems, financial services and energy grids, which are essential to the functioning of societies.

Secondly, it can spread disinformation and hate speech, further polarizing societies and fuelling conflict.

Thirdly, it can support terrorist activities and finance the illicit activities of State and non-State actors.

In view of those challenges, the Security Council must not lag behind with regard to the evolving cyberthreats, as such threats are interconnected with several of the items on the Council's agenda, including non-proliferation and counter-terrorism. In that regard, the Security Council should consider the possibility of incorporating cybersecurity-related elements in its products, according to the needs of each dossier. One example is the strengthening of strategic communications in peace operations and special political missions.

The promotion of a safe, open and peaceful cyberspace requires standards of responsible behaviour in the use of ICTs. In addition, the development of international law in that area must be accompanied by capacity-building, particularly in countries in conflict situations, as they are most vulnerable to the misuse of ICTs. The Open-ended Working Group on Security of and in the Use of Information and Communications Technologies is making progress in that area. The product of its work could serve as a guide for the Council's work.

I conclude by recalling the need to preserve and promote responsible use of cyberspace in order to guarantee its stability and security and thereby to reduce the substantial risk that it poses to nations.

Mr. De Rivière (France) (*spoke in French*): I thank the Secretary-General, Mr. Duguin and Ms. Ifeanyi-Ajufo for their briefings, and I thank you, Mr. President, for convening this debate.

The expansion of information and communication technologies is contributing to progress and to the achievement of the Sustainable Development Goals. Nevertheless, it also poses major challenges to our collective security. In societies that rely heavily on those technologies, malicious cyberactivities have continued to grow in frequency, gravity and sophistication. They are able to exploit numerous vulnerabilities and use increasingly diverse vectors, which are now accessible to multiple actors. Intrusion tools and services are spreading uncontrollably across markets, and their irresponsible use is contributing to the increase in cyberthreats.

Cyberattacks can, in and of themselves, constitute threats to international peace and security through their impact on critical infrastructure and the risks of escalation that they entail. Ransomware attacks, which, according to the French authorities, increased by 30 per cent in 2023, can thus affect such essential sectors as the energy sector, destabilize economies and even disrupt the functioning of government institutions. Cyberattacks are now being carried out in the context of armed conflict, as we saw in the attacks carried out by Russia against the Viasat satellite network in the early hours of its illegal invasion of Ukraine.

Malicious cyberactivities can also fuel other threats to international peace and security, including proliferation. The most recent report of the Panel of Experts of the Committee established pursuant to resolution 1718 (2006) (S/2024/215) indicates that the North Korean regime's illegal weapons of mass destruction programmes were financed up to 40 per cent by illicit cybermeans, such as ransomware or cryptocurrency thefts.

The United Nations and the Security Council, in fulfilment of its mandate, do nevertheless have the means to implement a coordinated response to those threats. First of all, let us recall that cyberspace is neither the Wild West nor a normative void. International law, including the Charter of the United Nations, international humanitarian law and international human rights law, is fully applicable. Norms for responsible State behaviour were defined by consensus in order to promote cooperation, foster conflict prevention and enhance stability in cyberspace.

France supports the work of the First Committee of the General Assembly to further develop that normative framework. In order to support its implementation, France has proposed a structure for an ambitious future programme of action mechanism for cyberspace. The Security Council must place respect for the normative framework for responsible State behaviour in cyberspace at the heart of its work on cyberthreats and encourage States to uphold their commitments to contribute to the security and stability of cyberspace.

Beyond that, the Security Council must continue its efforts to incorporate cyberissues into the different dimensions of its mandate. It is essential that the Council receive regular briefings by experts on the evolution of cyberthreats and their implications for international peace and security. Today's debate is a valuable example of that.

The Council must also continue to pay attention to the use of cybermeans to circumvent sanctions regimes. The malicious cyberactivities undertaken by the North Korean regime to finance its weapons of mass destruction programmes deserve continued attention in that regard. France will remain actively engaged to ensure that the Council, despite the failure to extend the mandate of the Panel of Experts of the 1718 Committee, continues to vigilantly monitor violations of its resolutions in that area.

The President: I now give the floor to His Excellency Mr. Mamadou Tangara, Minister for Foreign Affairs, International Cooperation and Gambians Abroad of the Republic of The Gambia.

Mr. Tangara (Gambia): First and foremost, I would like to thank the briefers for their enlightening remarks and to congratulate the Republic of Korea for organizing this debate.

We stand today at a crossroads. The digital age has woven a web of connection, opportunity and progress. Yet, within that very fabric lurks a growing darkness that threatens international peace and security. The ever-evolving threat of cybercrime is not merely a matter of financial gain or stolen data. The new wave of cyberthreats directly challenges international peace and security, demanding our urgent attention. In that connection, we thank the Republic of Korea for drawing our attention to another innovative engagement of the Security Council with a view to exchanging substantive insights on the agenda item "Maintenance of international peace and security: Addressing evolving threats in cyberspace". As the body entrusted with maintaining international peace and security, the Security Council cannot afford to remain silent, and we commend it for its continued efforts to sound the alarm on this important and shared issue. We need a comprehensive approach that addresses this evolving threat.

In that regard, I wish to suggest the following three points to support our joint efforts in curbing cyber-related international peace and security threats.

First, the Security Council must become a champion of exemplary norms of responsible State behaviour in cyberspace, and we can achieve that by raising awareness regularly to foster related cybersecurity discussions with a view to amplifying the work of General Assembly cyberforums and by working with Member States to translate those norms into action, promoting capacity-building and information-sharing to deter malicious activity.

Secondly, the Security Council can strengthen accountability for cyber-related security threats by advocating improved cybercapabilities of Member States to identify malign actors and build a unified front against impunity.

Thirdly, the Security Council can leverage the expertise of United Nations entities, such as the Office for Disarmament Affairs and the Office of Counter-Terrorism, to adequately address the threat of undermining sustainable international peace, security and democracy. Collaborating with those entities can also lead to coordination to avoid duplication and ensure a holistic approach that is fit for purpose.

Those actions, undertaken within the Council's mandate, will not only promote international peace and security but also strengthen existing efforts by advancing awareness, promoting accountability and fostering effective collaboration among States and related international institutions. The Security Council is therefore well situated to become a leader in building a more secure and stable cyberspace for all.

We must elevate the discussion and regularly integrate cyberthreats into our deliberations concerning regional conflicts and thematic issues. That amplifies the work of General Assembly forums dedicated to cybernorms. We must also encourage Member States to translate those norms into concrete action. That

includes building capacity for cyberdefence, promoting information-sharing and deterring malicious activity.

In conclusion, I must once again commend the Republic of Korea for this laudable initiative, which gives Member States the opportunity to participate in this very important and topical debate on an issue of common concern. The Security Council is central to the much-needed critical support required to mitigate and end cyber-related international peace and security threats.

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

Mr. Lindner (Germany): Germany thanks the Republic of Korea for its leadership role in bringing cybersecurity issues to the attention of the Security Council. I would also like to thank the Secretary-General and the briefers for their enlightening contributions.

The international community is exposed to a growing number of both State-sponsored and private malicious cyberactivity incidents. Those incidents have a serious impact on the maintenance of international peace and security. Severe attacks by cybercriminals, including ransomware attacks, have shown that such attacks have the potential to threaten the stability of State institutions. They have affected entire societies.

A recent trend is the emergence of hacktivist groups in the theatre of international conflicts that attack key critical infrastructure targets. That has eroded trust in the delivery of public services and has spread fear among civilians. The increasing cooperation of a number of State actors with private information technology companies, hacktivist groups and cybercriminals has further exacerbated existing risks. Those trends all serve as threat multipliers, given that the cyberdomain extends conventional battlefields far into the civilian domain.

In the light of that dramatically evolving threat landscape, Germany proposes the following four areas in which the Security Council should become active.

First, we see an important role for the Security Council in assessing the threat, both following Article 34 of the Charter of the United Nations, which gives the Security Council the authority to investigate any situation that might lead to international friction or give rise to a dispute, and more generally in the sense that the Council should consider and analyse more deeply the risks emanating from cyberattacks for international peace and security.

Secondly, the Security Council has an important dispute resolution role, based on the full applicability of the Charter of the United Nations to cyberspace.

Thirdly, we see potential for the Security Council to have a strong trust- and norm-building role. By putting international cyberconflicts on its agenda, investigating situations of cyberconflict or facilitating the peaceful settlement of such situations, the Council will help to build the evolving framework of responsible State behaviour in cyberspace. That must be based on international law and complemented by voluntary United Nations norms and confidence-building measures.

Finally, Germany would welcome efforts by the Security Council to mainstream cybersecurity threats into its agenda. That should encompass protecting the United Nations from being the target of malicious cyberattacks, in particular its presence in the field, such as peacekeeping operations.

In conclusion, I would like to stress that Germany will continue to contribute to the international discussion on this important issue. To highlight just one example, last year, we launched a global dialogue format on Cyber in Conflict. It seeks specifically to address the increased risks to civilians posed by the use of cybertools in international conflict, raise awareness and formulate mitigation options. The next event in that series will be held here in New York at the German House on 8 July in cooperation with Japan, Senegal and the International Committee of the Red Cross.

The President: I now give the floor to the representative of the United Arab Emirates.

Mr. Sharaf (United Arab Emirates): I thank His Excellency Mr. Cho Tae-yul, Minister for Foreign Affairs, for presiding over this open debate and commend the Republic of Korea for its stewardship of the Security Council this month. I also thank the Secretary-General and the other briefers for their insightful contributions.

As we heard today, threats to cyberspace are evolving rapidly. Malicious cybertools and techniques, such as ransomware, phishing and denial of service attacks, are being used to target government and private sector networks, threatening critical infrastructure and public safety. That is especially concerning as our nations, including the United Arab Emirates, are

undergoing digital transformations, which makes us more reliant on secure online systems. Educational institutions are also at risk, with educational digital infrastructure and valuable information assets being targeted by malicious actors. Furthermore, the malicious use of information and communication technology, including but not limited to emerging artificial intelligence (AI) technologies, acts as a threat multiplier in existing conflicts.

As a global hub for technology and innovation, the United Arab Emirates established the Cybersecurity Council in 2020. The Council is aimed at achieving a safer digital transformation and improving cybersecurity in the country for all targeted sectors. We are committed to capacity-building and information-sharing with our partners, as well as to promoting the responsible design of technology and using AI for good to combat the spread and amplification of hate speech, misinformation and disinformation. In line with that commitment, together with Albania, we hosted an Arria Formula meeting in December 2023 to address those challenges.

With that in mind, I would like to offer four points for consideration.

First, international law must guide the use of cybertechnologies. The Charter of the United Nations, sovereignty, non-interference in the internal affairs of States, State responsibility and the laws of armed conflict must be respected, including the United Nations norms of responsible State behaviour in cyberspace. Addressing normative gaps requires continued convergence on how to uphold and maintain international law in the cyberdomain.

Secondly, the United Arab Emirates supports mainstreaming cyberconcerns within the Council's work on international peace and security. That could include referencing cyber-related concerns, trends and developments in briefings, statements and priority issues more regularly, as well as in relation to country-specific and other thematic files. For instance, resolution 2341 (2017) recognizes the necessity of protecting critical infrastructure against terrorist attacks, including cybersecurity, underscoring the need to better address the broad spectrum of cyberthreats that come with digitization and cyberspace.

Thirdly, the Council should consider convening an annual briefing on emerging technological threats and their implications for international peace and security. Furthermore, the publication of an annual cybersecurity report by the Secretary-General would provide a comprehensive assessment of the global cyberthreat landscape and recommendations for enhancing international cooperation. The report should also include gender analysis to better respond to threats in cyberspace that target women and girls.

Fourthly, fostering strong public-private partnerships is crucial for leveraging expertise and resources to counter cyberthreats effectively. The United Arab Emirates is committed to collaborating with the private sector to develop robust cybersecurity tools and build national and international capabilities, along with supporting the private sector in ensuring the secure and responsible design of their solutions.

Harnessing cybertechnologies is crucial for our future, but vigilance against their risks is essential. International cooperation and capacity-building are vital for global security resilience. The United Arab Emirates will continue to advance responsible behaviour in cyberspace and ensure that it reflects our collective aspirations for peace and security.

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

Ms. Melbārde (Latvia): Latvia would like to express its gratitude to the Republic of Korea for organizing this high-level open debate of the Security Council. We would also like to thank the Secretary-General and the briefers from CyberPeace Institute and Leeds Beckett University for their insightful presentations.

The use of and reliance on digital technology has grown significantly since cybersecurity-related matters were first added to the United Nations agenda more than 20 years ago. Today the cyberdomain has become the connective tissue of global economic and social development. While providing vast opportunities for progress, the expansion of cyberspace has also been linked to rising risks and challenges. In recent years, we have encountered several negative trends regarding international peace and security. There is a growing number of cases in which critical infrastructure, including critical information infrastructure, has been targeted in cyberattacks with the threat of catastrophic real-world consequences. Furthermore, we have seen cyberattacks become an integral part of Russia's full-scale aggression against Ukraine.

Cyberthreats often intersect with other hostile acts, such as the spread of disinformation and misinformation

and the malicious use of artificial intelligence and other emerging technologies. Cybercrime is also rampant, with ransomware payments hitting a record high in 2023. Those developments affect global peace and security. The global community must coordinate its response, and the Security Council has a role to play in line with its mandate.

Latvia therefore believes that cyberspace threats and challenges merit regular discussion in the Council. Such discussions could be informed by a periodic report by the Secretary-General. Increasing the Council's attention to cybersecurity could also facilitate the integration of cyber-related aspects into other thematic mandates, such as peacekeeping and women and peace and security. The Council should also look into strengthening its ability to respond to large-scale cyberattacks with potential international security implications.

It is evident that developing a more robust role for the Council in addressing cybersecurity matters cannot be accomplished overnight. It is a step-by-step endeavour, and meetings such as today's play a critical role in facilitating that process. It is also clear that the Council should not replace the work that is already done in other United Nations formats under the General Assembly. Quite the opposite, the Council should reinforce the understandings reached in those formats, particularly the applicability of international law in its entirety to cyberspace. There is also more work to be done collectively on implementing the framework of responsible State behaviour in cyberspace. Anticipating the establishment of a permanent United Nations mechanism to address cybersecurity, known as the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, we see potential for new synergies between the Council and the General Assembly in this field.

In conclusion, I would like to underline Latvia's commitment to continuing to support efforts within the United Nations to address growing cybersecurity threats and challenges. We have been actively engaged in discussions on this topic in the General Assembly Committees, and we will also continue to advocate for a larger role for the Council.

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

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

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

Furthermore, the relevant technologies developed by States are being transferred, copied and reproduced by terrorists and criminals. The malicious use of ICT by terrorist and criminal organizations is a serious threat to international peace and security, particularly in the light of the attribution-related challenges. Under international law and the Charter of the United Nations, all Member States should refrain from any act that knowingly or intentionally damages or otherwise impairs the use and operation of the critical infrastructure of other States or interferes in their internal affairs. There is no doubt that the international security aspects of ICT have become too important and strategic to be left without clear binding rules at the international level. An inclusive process within the United Nations system is the best and most efficient way to establish arrangements that are equitable, comprehensive and effective in that domain.

The United Nations has already taken some steps towards establishing a normative framework that complements the principles of international law. With the adoption by consensus of two annual progress reports of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, established pursuant to General Assembly resolution 75/240, and of other consensual reports of United Nations-related processes, the United Nations has already established the initial elements of a framework for conflict prevention and stability in cyberspace.

The General Assembly called on Member States to be guided in their use of ICT by the cumulative and evolving framework for responsible State behaviour

in cyberspace contained in the consecutive reports of the Groups of Governmental Experts under the First Committee. However, the implementation of those norms remains quite minimal at best, owing to their voluntary nature and the lack of any follow-up mechanism.

While acknowledging the progress made in the Open-ended Working Group established pursuant to General Assembly resolution 75/240 on different aspects of its mandate, it is important that the Group lay the groundwork for a future mechanism, under United Nations auspices, that is action-oriented, single-track, consensus-based and inclusive. It should build upon the agreed outcomes of United Nations-related processes and focus on implementing the agreed outcomes, including the framework for responsible State behaviour in cyberspace, further developing that framework and promoting international cooperation with and assistance to developing countries.

Inclusive processes within the United Nations, primarily under the auspices of the General Assembly, are the most efficient way to establish equitable, comprehensive and effective arrangements in that domain. For its part, the Security Council is encouraged to take into account the opportunities offered by emerging technologies when considering such topics as peacekeeping and counter-terrorism. Nevertheless, the Council should not be utilized as a legislative body that attempts to set norms and rules on behalf of the States Members of the United Nations on matters that necessarily require inclusive and transparent processes.

The recommendations that have been endorsed by the General Assembly by consensus can form the basis for politically or legally binding rules, especially given that they are derived from the principles of international law and the Charter of the United Nations. While we believe that international law and the principles of the Charter of the United Nations do apply to all domains, including cyberspace, we also believe that there is a pressing need to identify specific obligations that make State behaviour in cyberspace consistent with international law and the objectives and principles of the Charter of the United Nations.

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

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

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 Ukraine.

Ms. Hayovyshyn (Ukraine): We thank the Security Council presidency of the Republic of Korea for convening this high-level open debate. We also extend our appreciation to the Secretary-General and other briefers for their remarks.

Ukraine aligns itself with the statement to be delivered on behalf of the European Union (EU) and would like to make some remarks in its national capacity.

We strongly believe that the Security Council plays an important role in addressing threats to international peace and security, including in cyberspace. The cyberthreat landscape continues to evolve and has become more challenging than ever before. Ransomware has posed an increasingly common and significant risk to governments, businesses and individuals. In addition, we are witnessing an increased number of malicious cyberoperations targeting critical infrastructure and critical information infrastructure, including the energy sector, public services and electoral processes. Some State actors continue to undermine the international rules-based order and the framework of responsible State behaviour in cyberspace by conducting malicious cyberactivities.

In that regard, the Democratic People's Republic of Korea has been engaged in cyberespionage and cryptocurrency theft, with the aim of further developing its nuclear and weapons of mass destruction programmes, in violation of the relevant Security Council resolutions. Recently, Russia's cyberespionage

group, APT28, conducted cyberattacks against a number of EU member States.

Ukraine has been facing Russia's aggression, including in cyberspace. Since the beginning of the war, Russia's cyberattacks have been growing more sophisticated and targeting government and security agencies, businesses and financial institutions. Moscow's cybercriminals have been conducting phishing attacks, cyberespionage and attacks against critical infrastructure, in addition to spreading disinformation and propaganda.

In order to effectively prevent, combat and mitigate cyberthreats, Ukraine actively cooperates with international partners to develop effective cybercapacity-building, which is fundamental for the exercise of the right to self-defence in cyberspace. In addition, Ukraine has also started to investigate and prosecute cyberattacks as war crimes.

States must abide by their international commitments and obligations, including in the context of the security of the use of ICTs. As we reaffirmed here at the United Nations, international law, including the Charter of the United Nations, is applicable in the cyberdomain. Therefore, all State actors that behave in a manner contrary to the agreed framework should be held to account.

To conclude, we encourage the States Members of the United Nations to continue working together on strengthening and implementing the normative framework of responsible State behaviour in cyberspace, raising awareness and exchanging best practices in response to existing and emerging threats in the cyberdomain.

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

Mr. Tammsaar (Estonia): We welcome today's exchange of views and thank the briefers, the Secretary-General in particular, for their most valuable insights.

Estonia aligns itself with the statement to be delivered by the representative of the European Union. Allow me to make a few observations in my national capacity.

We cannot ignore the increasing sophistication and damage caused by malicious cyberincidents carried out by both State and non-State actors. With high-profile targets, such as critical infrastructure, financial institutions and democratic processes; the cross-border nature of the incidents and increasing capacities, cyberattacks are able to cause greater and greater damage. Therefore, cybersecurity is clearly part of both national and international security challenges, and preventing and mitigating such threats are our common priority.

Russia's aggression against Ukraine has highlighted how cyberoperations are intertwined with acts of kinetic warfare. We have witnessed how Ukrainian critical infrastructure is targeted by Russia, in violation of international humanitarian law. Russia's actions have underscored the need to focus on a comprehensive approach to national defence and internal security. In order to strengthen Ukraine's readiness for and resistance to cyberattacks, Estonia has actively supported Ukraine in the cyberdomain bilaterally, as well as through the Tallinn Mechanism and the IT Coalition.

We are also deeply concerned by the most recent news coming from Pyongyang suggesting that the military cooperation of the Democratic People's Republic of Korea with Russia has been further enhanced, in gross violation of the corresponding Security Council resolutions. Estonia strongly condemns the ongoing malicious cyberactivities perpetrated by the Democratic People's Republic of Korea, which aim to fuel the weapons programme of the Democratic People's Republic of Korea, destabilize regional security and threaten global peace.

The United Nations framework of responsible State behaviour in cyberspace builds upon existing international law. International law — in particular the Charter of the United Nations, the law of State responsibility, international human rights law and international humanitarian law — applies fully to cyberoperations. We need to work together to uphold international law and ensure that it is also adhered to in cyberspace. In order to support the implementation of the framework of responsible State behaviour in cyberspace, Estonia advocates the establishment of an inclusive and action-oriented programme of action as a single permanent structure following the conclusion of the current Open-ended Working Group on Security of and in the Use of Information and Communications Technologies in 2025.

An open, secure, stable, accessible and peaceful information and communications technology

environment cannot be taken for granted and is not separate from the physical world. While Russia's aggression against Ukraine has showcased the integrated nature of cyberattacks and kinetic warfare, we believe that that is a pattern that will also be used in future conflicts. The Security Council therefore has a substantial role to play in serving as a forum for sharing information on existing and future cyberthreats, as well as raising awareness on the strategic implications of cybersecurity, which Estonia already underlined during its Security Council tenure.

In conclusion, that is why Estonia commends the Republic of Korea for holding the current discussion in the Chamber, where it belongs. Open discussions on cybersecurity such as this one will be essential for supporting the enhancement of domestic, regional and global cyberresilience by contributing to the prevention and mitigation of cyberconflicts.

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

Mr. Kulhánek (Czechia): I would first like to thank the Republic of Korea for organizing this highly relevant open debate. We welcome today's discussion on the Security Council's role in the field of cybersecurity, particularly regarding the implementation of the agreed framework for responsible State behaviour in cyberspace.

Needless to say, we share many of the concerns and warnings expressed here today. We are particularly concerned about attacks on critical infrastructure, cyberespionage, ransomware attacks against both public and private institutions, including the health-care sector, cryptocurrency thefts and efforts to gain ongoing access to critical industrial systems, not only for espionage and intellectual property thefts, but also with the aim of being able to control them in an openly hostile manner. The increasing use of information and communications technologies (ICTs) in armed conflicts and their harmful effects on civilians are alarming. Those irresponsible acts endanger international peace and security, for which the Security Council bears responsibility. Similarly, cyberspace is being used more and more to spread disinformation, exacerbate existing social conflicts and even incite terrorist acts. The Council, along with the relevant United Nations forums and other international organizations addressing the cyberagenda, should intensify its efforts to find effective ways to address those less obvious malicious activities in cyberspace. It should also work to raise awareness about the true scale of those threats and facilitate activities that promote greater resilience.

In May, Czechia, in coordination with Germany and other States, publicly condemned the activities of the Russian State-controlled actor APT28, which had been conducting a long-term cyberespionage campaign in European countries and targeting Czech government institutions. Such activities are in violation of United Nations norms of responsible State behaviour in cyberspace. We will continue to address them robustly, together with our partners and in accordance with our international obligations.

Czechia fully endorses an international order based on international law that promotes an open, secure, stable, accessible and peaceful ICT environment. We reiterate our support for the establishment of a permanent, single-track, inclusive and action-oriented mechanism under the auspices of the United Nations and on the conclusion of the current Open-ended Working Group on Security of and in the Use of Information and Communications Technologies in 2025. We believe that the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security could serve as such a mechanism.

Finally, I would like to reiterate that my country remains committed to being an active participant in what must be a truly global partnership to tackle the cybersecurity threats of today and tomorrow. It will indeed require an all-hands-on-deck approach. We are already engaged in detailed discussions with a number of countries in Africa, the Indo-Pacific and Latin America to map out the evolving threat landscape and strengthen our joint response. For instance, at the end of April, Czechia organized a seminar in Bogotá on the current challenges in the field of criminal activities in cyberspace. We were grateful that experts from Colombia, Costa Rica, the Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras and Panama attended the event and shared their valuable insights with us.

I thank you again, Mr. President, for the opportunity to share my country's views on this important subject.

The President: I now give the floor to Mrs. Samson.

Mrs. Samson: I have the honour to speak on behalf of the European Union (EU) and its member States. The candidate countries North Macedonia, Montenegro, Albania, Ukraine, the Republic of Moldova, Bosnia and

Herzegovina and Georgia, as well as Andorra, align themselves with this statement.

I thank you, Mr. President, for organizing this high-level open debate. The EU welcomes the discussion today to exchange views on the evolving cyberthreat landscape and its implications for the maintenance of international peace and security.

The statements delivered just now captured a wide range of emerging and evolving threats, from low-impact denial of service attacks to large-scale cyberoperations and attacks on critical infrastructure. We add to those concerns the potential cross-border impact that could arise from malicious cyberactivity. We also note the blurred lines between criminal activities and State-sponsored attacks using cybercriminals for hire, making the already difficult task of attribution all the more challenging. It must be our joint commitment to strengthen our toolkit for collective resilience, and we welcome other delegations sharing their insights and their experiences.

The EU and its member States are alarmed by the number, sophistication and scale of malicious cyberactivities targeting government institutions and democratic processes. Last month, Germany shared its assessment that the Russia-linked cyberespionage group APT28 compromised email accounts of the German Social Democratic Party. State institutions, agencies and entities in EU member States, including in Czechia, Poland, Lithuania, Slovakia and Sweden, have been targeted by the same threat actor before. Those malign activities must stop.

The United Nations norms of responsible State behaviour in cyberspace provide guidance in that regard. The main commitments are straightforward: international law applies in cyberspace; States are expected to uphold voluntary norms of State behaviour; States must prevent the misuse of cyber in their territory; practical confidence-building measures are needed to help to reduce the risk of escalation and conflict stemming from cyberincidents. For the EU, focusing on the development and implementation of the agreed framework for responsible State behaviour in cyberspace is crucial if we are to fulfil our shared responsibility in line with our common interest and protect all States from the risks of malicious cyberactivity. States can make meaningful progress by clarifying the application of existing international law and discussing the implementation of and adherence to existing norms of responsible behaviour. For the agreed framework for responsible State behaviour to be effective, we must uphold it together. That reinforces the importance of establishing a permanent, inclusive and action-oriented mechanism under the auspices of the United Nations. We therefore support the creation of a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security and hope to agree on modalities this summer.

We look forward to further advancing discussions on this important topic, and we welcome efforts such as this one, aimed at highlighting the important role of the Security Council in fulfilling its mandate as set out by the Charter of the United Nations to address threats to international peace and security by highlighting the unique and specific international threats emerging in the cyberdomain. We also wish to continue exploring how the Council's future work can effectively complement other relevant United Nations processes in that regard.

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

Mr. Lagdameo (Philippines): The Philippines takes this opportunity to re-emphasize the critical importance of addressing information and communications technology (ICT) threats to international security. The rapid advancement of digital technologies poses new challenges that require immediate and concerted action. In that regard, we wish to highlight three key points: trends in ICT threats, the impact of cyberthreats on international peace and security and cyberattacks as a threat multiplier.

First, regarding trends in ICT threats, the rise of robocalls powered by artificial intelligence (AI) being used for fraud, the proliferation of deep fakes and misinformation, and ransomware attacks present significant risks and complex challenges. Comprehensive strategies are essential to counteract those sophisticated threats. The malicious use of AI in cyberspace poses profound risks. We must prioritize assessing those threats to develop robust cybersecurity policies and ensure the safe deployment of AI technologies.

Secondly, regarding the impact of cyberthreats on national peace and security, the Philippines has experienced first-hand the devastating impact of cyberattacks on national security and public trust. Recent incidents, such as the defacement of government

websites, data breaches targeting critical institutions and the large-scale theft of personal information, highlight the urgent need for enhanced cybersecurity measures. Cyberattacks can disrupt essential services, undermine trust in institutions and have far-reaching socioeconomic consequences. We are also particularly concerned about malicious ICT activities that are aimed at interfering in the internal affairs of States. We are seeing a reported increase in States' malicious use of covert information campaigns enabled by ICT to influence the processes, systems and overall stability of other States. Such uses undermine trust, are potentially escalatory and can threaten international peace and security. Another alarming consideration is the availability of those sophisticated ICT capabilities to non-State actors and their ability to use those technologies maliciously for commercial gain and to evade responsibility.

Thirdly, regarding the threat-multiplier effect of cyberattacks, criminal activities in cyberspace exacerbate existing challenges to international peace and security. The Philippines has witnessed how cyberattacks can serve as significant threat multipliers, complicating efforts to maintain peace and stability. The transnational nature of cyberspace means that no State is immune, and our collective security is only as strong as its weakest link. Given the serious risk posed by cyberthreats, the Philippines underscores the Security Council's pivotal role in addressing those threats. While the ongoing discussions of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies are of value, it is also imperative for the Security Council to remain engaged in shaping the global cybersecurity agenda.

In that regard, the Philippines supports the Council taking the following collective measures to counter cyberthreats, as raised during the Arria Formula meeting on cybersecurity held in April: first, reinforcing the agreed normative framework for responsible State behaviour in cyberspace; secondly, convening annually to discuss and review the ICT threat landscape and, in that regard, requesting that the Secretary-General prepare an annual report on trends to inform the discussions of Member States; and thirdly, leading on information-gathering or studying specific threats or incidents for the guidance and reference of Members States.

The Philippines reaffirms its commitment to enhancing cyberresilience and promoting responsible behaviour in cyberspace. We call for continued cooperation, capacity-building efforts and support mechanisms, including a regular trust fund to assist developing countries in addressing cyberthreats. We count on partnerships and technology transfers to help us to narrow the digital divide and bolster our cyberdefences.

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

Mr. Nasir (Indonesia): Indonesia thanks the Republic of Korea for convening this important meeting. We also thank the Secretary-General and the briefers for their presentations.

Threats in cyberspace have become a real and present danger to national and international peace and security. We are increasingly exposed to new threats from new and rapidly developing technologies. Only through a coordinated response and robust legal frameworks can the international community enhance cyberresilience and mitigate those risks effectively.

In that context, allow me to highlight the following points.

First, we must prioritize mitigating the human cost of cyberattacks that target critical infrastructure. We must ensure that cyberspace is safeguarded as a domain that is free from conflict and not an arena of conflict. While advancements in artificial intelligence (AI), including generative AI and machine learning, can benefit the human race, they can also be destructive and facilitate cyberattacks, with a considerable negative impact on the global population. It is therefore essential to safeguard critical infrastructure in our efforts to prevent significant harm being caused by malicious cyberactors and irresponsible States.

Secondly, synergy and coherence within the United Nations system in the areas of cybersecurity, information and communications technology (ICT) and international peace and security are essential. While the Security Council has the important mandate to maintain international peace and security, other United Nations organs have equally important mandates to work on the issues of digital and ICT security and cybersecurity. It is important for the Security Council to establish parameters and mechanisms that can help it to foster collaboration and synergy, providing a better understanding of the risks that cyberthreats pose to international peace and security. Indonesia thus reaffirms its commitment to the work of the Open-

Ended Working Group on Security of and in the Use of Information and Communications Technologies and other processes being undertaken in the field, including in the Summit of the Future process.

Thirdly, we must enhance global cybersecurity by strengthening regional cooperation. Cooperation with regional organizations is necessary, as they play an important role in contributing to a robust and comprehensive approach to cybersecurity. In our region, the Association of Southeast Asian Nations (ASEAN) has played an instrumental role in creating frameworks and initiatives, including through the ASEAN Regional Forum, to enhance regional resilience to cyberthreats. Leveraging such expertise from regional organizations can indeed provide valuable insights and advance a more holistic international effort.

Finally, we must bridge the technology gap to improve cyberresilience. The cybersecurity capacity gap is a critical challenge for developing countries, leaving them vulnerable to escalating threats and undermining their stability. Cooperative measures at all levels, including with relevant private sector stakeholders, are crucial to bolstering stability in cyberspace, particularly through capacity-building, technical assistance and the transfer of technology. Only through united efforts can we create a secure cyberspace that fosters global peace and stability.

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

Mr. Seah (Singapore): We thank the Republic of Korea for convening today's meeting on this important issue.

Since the Security Council's first open debate on cybersecurity, which took place in June 2021 (see S/2021/621), the cyberthreat landscape has continued to evolve at a worrisome pace. Against that backdrop, international cooperation at the United Nations is vital and indispensable to combat the global and transboundary nature of the cyberthreat landscape. In that regard, it is necessary for the General Assembly and the Security Council work together to strengthen adherence to the normative framework for responsible State behaviour in cyberspace, based on the application of international law and respect for the principles of the Charter of the United Nations. As a small State, Singapore has always supported a multilateral system based on the rule of law. Our approach is no different when it comes to cybersecurity, which is of vital importance for many small and developing States. Singapore firmly believes in the importance of the United Nations as a key platform for discussing the development and implementation of the rules, norms and principles of responsible State behaviour that govern cyberspace.

Singapore is honoured to have served since 2021 as Chair of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. The Open-ended Working Group builds on more than two decades of work at the United Nations, which have resulted in a cumulative and evolving framework for responsible State behaviour in cyberspace that has been endorsed by all Member States. It is encouraging to note that the Open-ended Working Group has made good progress over the past three years in further strengthening the normative framework for responsible State behaviour in cyberspace.

The Open-ended Working Group has also served as a valuable confidence-building measure in and of itself. In addition to the common understandings reached in the Open-ended Working Group's two annual progress reports agreed by consensus in July 2022 (see A/77/275) and July 2023 (see A/78/265) respectively, the Open-ended Working Group has spearheaded the development and operationalization of concrete action-oriented initiatives that have an important role to play in enhancing international peace and security in cyberspace, most notably in the form of the global points-of-contact directory, which was officially launched on 9 May. Also in May, the Open-ended Working Group convened a successful and substantive ministerial-level meeting on information and communications technology (ICT) security capacity-building. The key message from that meeting was that capacity-building is urgently needed to help many small and developing countries to attain cyberresilience. Equally important, there was widespread recognition that capacity-building can be an important means of building confidence and trust between States.

In your guiding questions, Mr. President, you asked how cyberthreats are interlinked with other Security Council agenda items and what specific role the Security Council can play in addressing international peace and security challenges emanating from cyberspace. Given the ongoing work being undertaken in the General Assembly, it is important for the Security Council to avoid duplicating the work already being

done in other processes. At the same time, however, we must recognize that the Security Council has a clear mandate to discuss matters relating to the maintenance of international peace and security. We cannot rule out the possibility that a cyberincident could create misunderstanding between States and lead to an escalation and potentially conflict, thereby creating an international peace and security incident. We therefore cannot rule out a role for the Security Council as part of its Charter-given responsibility for the maintenance of international peace and security.

The Council should therefore take an inclusive view of what constitutes threats to international peace and security and operate with the awareness that cyberthreats can have physical and real-world consequences. In that regard, we are open to the idea of the Security Council continuing to convene open debates such as today's as a means of exchanging information and enhancing understanding between Member States. The discussions in the Council can help to inform the General Assembly's work, including in areas of capacity- and confidence-building, and further help to strengthen the framework for responsible State behaviour in cyberspace, including in considering how best to apply rules, norms and principles to existing and potential cyberthreats.

Let me conclude by underlining the need for greater international cooperation in order to strengthen our collective resilience in cyberspace. Promoting greater cooperation between the Security Council and the General Assembly on international peace and security issues and working together in a sustained, holistic and synergistic manner will enable the international community to better preserve international peace and security in the domain of cyberspace. Singapore stands ready to work with all Member States towards that goal.

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

Ms. Chan Valverde (Costa Rica) (*spoke in Spanish*): I thank the Republic of Korea for convening this open debate.

Two years ago, Costa Rica fell victim to large-scale ransomware attacks. We are still feeling the impact caused by the disruptions to our health-care system, social security, finance and other critical sectors.

In that regard, Costa Rica would like to make three points today.

First, Costa Rica strongly believes that the protection of civilians agenda should be extended to encompass cyberactivities that affect the civilian population during armed conflicts. States must join the growing consensus that civilian data enjoys the same protection under international humanitarian law as all other civilian objects and that cyberoperations that disable or impede the functionality of civilian systems are prohibited under international humanitarian law. States must also refrain from involving civilians in military cyberactivities, as doing so may put them in danger.

Secondly, Costa Rica believes that it is time to update the women and peace and security agenda to address women's digital safety. Costa Rica calls on the members of the Security Council to consider adopting a new draft resolution that would provide for measures for protecting women and girls from online violence, abuse and exploitation, particularly in conflict and post-conflict settings. Digital safety considerations must also be integrated systematically into all new mandates, objectives and initiatives pertaining to that agenda.

Thirdly, all States, whether they are members of the Council or not, are responsible for strengthening the international rule of law in cyberspace. Costa Rica is a proud member of a growing group of States that have issued national positions on the application of international law in cyberspace. Those position papers build on the global consensus that international law, including international humanitarian law and international human rights law, applies to States' use of information and communications technologies and is essential to maintaining peace and stability. We encourage other States to develop such position papers, and we commend the existing legal capacity-building resources, such as the Cyber Law Toolkit, which can guide efforts in that area.

As our societies grow increasingly vulnerable to cyber and digital threats, Costa Rica urges the Council to include those concerns in its work and to do so in a way that enhances the respect for international law in times of both peace and armed conflict.

The President: There are still a number of speakers remaining on my list for this meeting. I intend, with the concurrence of members of the Council, to suspend the meeting until 3 p.m. this afternoon.

The meeting was suspended at 1.10 p.m.