United Nations S/PV.9039

Security Council

Seventy-seventh year

Provisional

9039th meeting
Monday, 23 May 2022, 10 a.m.
New York

President:	Mrs. Thomas-Greenfield	(United States of America)
Members:	Albania	Mr. Hoxha
	Brazil	Mr. De Oliveira Marques
	China	Mr. Zhang Jun
	France	Mr. De Rivière
	Gabon	Mr. Biang
	Ghana	Mr. Agyeman
	India	Mr. Tirumurti
	Ireland	Mr. Flynn
	Kenya	Mr. Kiboino
	Mexico	Mr. Gómez Robledo Verduzco
	Norway	Ms. Juul
	Russian Federation	Mr. Nebenzia
	United Arab Emirates	Mrs. Nusseibeh
	United Kingdom of Great Britain and Northern Ireland	Mr. Roscoe

Agenda

Maintenance of international peace and security

Technology and security

This record contains the text of speeches delivered in English and of the translation of speeches delivered in other languages. The final text will be printed in the *Official Records of the Security Council*. Corrections should be submitted to the original languages only. They should be incorporated in a copy of the record and sent under the signature of a member of the delegation concerned to the Chief of the Verbatim Reporting Service, room U-0506 (verbatimrecords@un.org). Corrected records will be reissued electronically on the Official Document System of the United Nations (http://documents.un.org).

22-35745 (E)

Accessible document Please recycle

The meeting was called to order at 10.05 a.m.

Adoption of the agenda

The agenda was adopted.

Maintenance of international peace and security

Technology and security

The President: In accordance with rule 39 of the Council's provisional rules of procedure, I invite the following briefers to participate in this meeting: Ms. Rosemary DiCarlo, Under-Secretary-General for Political and Peacebuilding Affairs; Ms. Nanjala Nyabola, Director of Advox, the Digital Rights Project of Global Voices; and Mr. Dirk Druet, Adjunct Professor at the McGill University Center for International Peace and Security Studies and Non-resident Fellow at the International Peace Institute.

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

I give the floor to Ms. DiCarlo.

Ms. DiCarlo: Digital technologies have profoundly transformed every facet of our societies. They offer boundless opportunities for sustainable development, for education and for inclusion. Social media, for example, has transformed human rights and humanitarian advocacy, making it possible to mobilize people around the world quickly and efficiently around issues requiring urgent attention. They have also created fresh possibilities for our peace and security work. Technological developments have improved our ability to detect crises, to better preposition our humanitarian stocks and to design data-driven peacebuilding programming.

We are using digital technologies in our work in conflict prevention, peacemaking and peacebuilding. Allow me to share a few examples.

Digital tools strengthen our information-gathering and early-warning capacities. In Yemen, the United Nations Mission to Support the Hodeidah Agreement has used various mapping, geographic information system and satellite technology tools to enhance its monitoring of the ceasefire in the governorate. They have increased our preparedness to understand, analyse and respond to crises that may have a digital dimension and to address digital risks. We have, for example, worked with partners to build an e-learning platform on digital risk management.

New technologies can be beneficial in support of political processes, particularly to promote inclusion. In various peace negotiations, we have used artificial intelligence-assisted digital dialogues to reach out to thousands of interlocutors and to hear their views and priorities. That has been a particularly useful way to reach traditionally excluded groups, including women.

In Libya, the United Nations Mission held five digital dialogues, each with more than 1,000 participants. That effort increased the legitimacy of the process, as different communities saw that their voices could be heard. In Yemen, through digital consultations, the Special Envoy engaged hundreds of women from various governorates, which provided deeper insight into the gender dimensions of the war.

The use of digital technologies also can improve the safety and security of our peacekeepers and civilian staff on the ground. The launch of the Strategy for the Digital Transformation of United Nations Peacekeeping represents an essential step towards that goal, as well as towards more effective mandate implementation, thereby increasing early-warning capacities.

Finally, with those tools, we are able to visualize information and convey data-rich analysis to support the Security Council's decision-making. Our recent virtual-reality presentation to the Security Council on Colombia shows how we can bring our work on the ground to the attention of this body in new ways.

The benefits of digital technologies for the maintenance of international peace and security are manifold. However, advances in technology have also created significant new risks and can affect conflict dynamics for the worse. There are several areas of concern.

The number of State- and non-State-sponsored incidents of malicious use of digital technologies for political or military ends has nearly quadrupled since 2015, according to some estimates. Of specific concern is activity targeting the infrastructure that provides essential public services, such as health and humanitarian agencies. Meanwhile, lethal autonomous weapons raise questions regarding human accountability for the use of force.

As the Secretary-General has made clear, machines with the power and discretion to take lives without

human involvement are politically unacceptable, morally repugnant and should be prohibited by international law. In addition, non-State actors are becoming increasingly adept at using low-cost and widely available digital technologies to pursue their agendas. Groups such as the Islamic State in Iraq and the Levant and Al-Qaida remain active on social media, using platforms and messaging applications to share information and communicate with followers for the purposes of recruitment, planning and fundraising. The increasing availability of digital payment methods such as cryptocurrencies brings additional challenges.

Furthermore, digital technologies have raised major human rights concerns, from artificial intelligence systems that may be discriminatory to the widespread availability of surveillance technologies that can be deployed to target communities or individuals. We are also concerned about the increasing use of Internet shutdowns, including in situations of active conflict, which deprive communities of their means of communication, work and political participation.

In Myanmar, for example, Internet and mobile shutdowns have grown in number and duration since the military coup on 1 February 2021, particularly in areas of military operations. Social media can fuel polarization and, at times, violence. The misuse of social media and the sometimes limited or not fully adequate response of social-media companies are enabling the spread of disinformation, radicalization, racism and misogyny. That can heighten tensions and, in some cases, exacerbate conflict. In Ethiopia, as the fighting escalated, there was an alarming rise in social media posts spreading inflammatory rhetoric, with some going as far as inciting ethnic violence, as recognized by the Security Council in its press statement of 5 November 2021 (SC/14691).

We have seen how online disinformation and hate speech can result in offline harm, including violence. We know that disinformation can hinder the ability of our missions to implement their mandates by exacerbating falsehoods and fuelling polarization. We are undertaking a number of actions to mitigate those risks, driven by the United Nations Strategy and Plan of Action on Hate Speech, launched by the Secretary-General, and initiatives such as Verified. In Iraq, for example, after reports of increased online harassment of women candidates in last year's election, the United Nations Assistance Mission for Iraq partnered with civil-society organizations to monitor hate speech, issue public reports and strengthen voter education.

We must fully embrace the opportunities offered by digital technologies to advance peace, but in order to do that, we must also mitigate the risks that such technologies pose and promote their responsible use by all actors. Through the General Assembly, Member States have made important progress in establishing a normative framework to ensure responsible behaviour in cyberspace. Member States are also cooperating to develop and apply a range of confidence-building measures to prevent conflicts, avoid misperceptions and misunderstandings and reduce tensions.

However, more must be done to advance, elaborate and implement the emerging normative framework. In his report entitled *Our Common Agenda* (A/75/982), the Secretary-General called for a global digital compact that would outline shared principles for an open, free and secure digital future for all. Together with other aspects of *Our Common Agenda*, such as the new agenda for peace and the proposed code of conduct that promotes integrity in public information, we have a critical opportunity to build consensus on how digital technologies can be used for the good of people and the planet, while addressing their risks. But collective action by Member States remains essential towards achieving that goal.

The President: I thank Ms. DiCarlo for her briefing.

I now give the floor to Ms. Nyabola.

Ms. Nyabola: It is an honour and a pleasure to address the Security Council today on the question of digital technology as it pertains to peace and security. As members heard in the introduction, I am a researcher whose work examines the intersection of technology, society and politics, with a specific interest in deepening our collective understanding of digital rights.

In the past two decades, we have witnessed a dramatic expansion of the use of digital technology at all levels of our social lives — at the individual, the collective, the national and the transnational levels. Unfortunately, that expansion has not been complemented by a similar investment in protecting ourselves from the harms that the expansion has created, nor by a commitment to understanding and defending the rights of the human within the system that we are building. Simply put, our appetite for digitalization is outpacing our awareness of its implications, and with the mounting evidence of the

harms that disordered approach makes possible, now is a crucial moment to take stock and decide if we need to change or reverse our course of action.

It would be foolish to attempt to summarize all the rights implications of the digital age in the time I have been given. Rather, in this briefing I will emphasize some big-picture challenges created by digitalization and three key principles that create opportunities for action to safeguard peace and security.

As a preface, I would like to qualify my remarks by saying that speaking about digital technology in relation to peace and security must not be interpreted as an invitation for the militarization and securitization of the Internet. After all, the mandate of the Council is the preservation of peace and security, and it is important to be guided by a spirit that is animated as much as, if not more, by a desire for positive peace as it is by an interest in security. The Internet has been a space for tremendous innovation, creativity and opportunity, and, in thinking about resolving the challenges that face the Internet today, I would like to urge the Council to commit to preserving the Internet as a global public good, much like we are led by a spirit of cooperation in thinking about spaces like Antarctica or outer space.

Nonetheless, after many years of unchecked tech-optimism, we are now in a moment of growing cynicism, as the threats that were ignored while we were trying to accelerate progress have started to materialize. In the research that I lead with Advox, we use a simple typology to help us make sense of such threats, separating the domains of digital technology into four categories: data, access, speech and information.

With regard to the subject of data-concerns practices that specifically target the data stack, such as surveillance or the growing use of biometrics, there has been an alarming rise of the global surveillance economy, including the widespread use of technologies such as Pegasus against political leaders, journalists and members of civil society. The technology that is developed to make those practices possible is developed in wealthy countries and then deployed or exported to poor countries, with no overarching consideration for the rights context, putting those who are at the forefront of advancing peace at grave risk.

As such, we join the Office of the United Nations High Commissioner for Human Rights in urging a global moratorium on the development and sale of surveillance technologies and invite the Security Council to join in putting pressure on private corporations to comply with such a moratorium. There is also growing use of mass data-harvesting technologies by both State and non-State entities, or the datafication of our lives, without a supporting drive to protect or even raise awareness on key rights such as data privacy or protection. In conflict zones, the datafication of refugee lives has increased dramatically, including an increase in the collection and storage of biometric data from asylum-seekers that is held under opaque conditions and sometimes used to deny refugees entitlements or restrict their freedoms.

The question of access looks at active and passive practices that restrict people's ability to get to the Internet, ranging from Internet and social-media shutdowns to gender disparities and the deliberate underinvestment in infrastructure, to the detriment of low-resourced communities. In 2021, the global digital rights organization Access Now documented 182 Internet shutdowns across 34 countries — an increase from the 159 shutdowns in 29 countries recorded in 2020. The longest Internet shutdown endured almost three years. The country with the most Internet shutdowns experienced 109 in a single year.

In addition to Internet shutdowns, there has also been an increase in related practices such as bandwidth throttling and social-media shutdowns, particularly around fraught election periods. These disruptions are designed to chill civic discourse and participation and are a direct assault on democracy and peace.

More broadly, there are several countries where women still face systematic obstacles to accessing the Internet — a fact that became particularly visible as schools around the world attempted virtual education in response to the coronavirus disease pandemic. In several countries where the transition did not happen properly, young girls bore the brunt of exclusion from accessing whatever technology was available because they were girls. Furthermore, in some countries, including some wealthy countries, while there has been an uptick in making digital technology mandatory for civic life, including registrations of births, deaths and more, there has been a strikingly low investment in making digital infrastructure accessible to people with disabilities or in indigenous and non-dominant languages.

The question of speech looks at restrictions to the freedoms of expression, information or opinion. In many countries, digital platforms work alongside

analogue platforms, such as the media and physical public squares, as a place where people can assemble, deliberate and share ideas about how to improve their societies. There has been a dramatic increase in the use of legislation to restrict the ability of people to participate in such discourse, including laws that unjustly expand the definition of criminal libel to make almost all criticism of State officials illegal. The Office of the United Nations High Commissioner for Human Rights noted that at least 40 social media laws were passed between 2020 and 2021, and 30 more were under consideration during the same time period.

Many of those laws contain such broad definitions of the underlying injuries that they supposedly address that they are routinely used first against journalists and critics of the State. The passage of those laws is generally followed by a spike in civil and criminal cases against journalists. It is worth emphasizing at this point that there is often a gender dimension to those practices, with female journalists such as Maria Ressa and Rana Ayyub, or members of civil society and even ordinary young women, specifically targeted for alleged breaches of public morality or for simply doing their jobs.

Finally, the domain of information concerns practices that manipulate information in the public sphere in order to distort people's perception of reality and therefore their ability to act appropriately in response to social or political issues. That includes practices such as misinformation, disinformation or malinformation, as well as the use of coordinated inauthentic behaviour or astroturfing to shift the public agenda on social media platforms. Those practices are made possible by an Internet on which advertising drives traffic and, therefore, in which the perception of popularity can be purchased.

In conflict zones, hostile Governments use coordinated inauthentic behaviour to silence critics by bombarding them with so many negative comments that their social media becomes unusable. Administrations in several countries have built Government departments specifically designed to shape online discourse, or news-like organizations to distort the perception of State behaviour or to pollute the lines of communication with so much noise that the signal cannot get through. Those practices together make it difficult to achieve peace because they make it difficult for people to agree on the causes of conflict and, therefore, what must be done to stop it.

Perhaps the biggest cause for alarm is that the rise of those practices is not necessarily restricted to certain types of Government or those that we would readily label authoritarian. Rather, our research found a growing tolerance for allowing concerns about national security to overtake concerns about human rights and democracy.

Significantly, I must raise the alarm on the practice of building and exporting technologies that enable digital authoritarianism from countries that are nominally democratic to countries that are explicitly authoritarian. That is all before we address the injustices embedded within the technologies themselves, including concerns about the injustices embedded within artificial intelligence, for example.

At the same time, looking at the challenges facing the Internet today as purely national challenges results in the fragmentation of the regulatory response, and that undermines the value of the Internet as a connector. Our research finds that the threats emerging from digitalization are multilateral — that is, rarely remaining contained within a single country; transnational, because they routinely involve the transfer of technology across national borders; and generational, because we are mortgaging the possibility of a free Internet for future generations on the perceived security of the present moment. Those realities require a commensurate response. It is not enough to just single out individual countries. What we need to do is to identify cultures of digital authoritarianism before they take root and travel around the world.

In conclusion, I would like to once again recall the mandate of the Security Council in the preservation of peace and security and urge a multilateral, transnational and generational approach to addressing the challenges of human rights in the digital age. To achieve such an approach, I would urge the Council to recall three principles.

First, digital rights are human rights, and any effort to address those challenges must first begin with the protection of the human from the excesses of the power of the State and private corporations.

Secondly, despite those and more challenges, the power of the Internet can and must still be harnessed for the greater good, and we must shape and protect it as a global public good, without allowing the interests of security or profit to drown out the interests of peace.

Finally, whatever actions the Council chooses to take must look beyond this moment to protecting the aspirations of future generations. What shared digital future do our actions make possible, and what futures do they circumscribe? Evidently, there are many tensions and contradictions embedded within these principles. Do we want more Government or less? What role should private corporations play? How do we balance our desire for technical progress with a desire for holistic, equitable use?

I believe that with those principles in mind, some actions that the United Nations can take to protect digital rights and ensure that digital technologies play a positive role in international peace and security become apparent. The United Nations must continue to use its unparalleled convening power to foster deliberation and rally support for the preservation of the Internet as a global public good. The United Nations must use its agenda-setting power to ensure that human rights are embedded retroactively and proactively in the digital technologies that we build and use. The United Nations must use its norm-setting power to foster agreement on the human rights standards that would make a free, safe and just digital future possible, not just for this generation but also for future generations.

Finally, the United Nations must rally support for those who have been at the forefront of this work all over the world, often at great personal risk, speaking out in defence of those, such as Alaa Abd El-Fattah, who have suffered grave injustices because of the way they have used the Internet to advance democratic ideals.

At this moment we are collectively on a trajectory towards an unjust digital future, but a different and more just path is possible, and the Council has an opportunity to move us closer towards that better future.

The President: I thank Ms. Nyabola for her briefing.

I now give the floor to Mr. Druet.

Mr. Druet: I am very grateful for this opportunity and for the honour of briefing the Council on how evolving digital technologies impact the nature of violent conflict and on the implications that has for the efforts of the United Nations to prevent violence, sustain peace and alleviate suffering and war.

As the Council President mentioned, I have participated in the development of the technological capabilities of the United Nations over several years, particularly from the perspective of situational awareness, analysis and peacekeeping intelligence. Today I conduct research on those issues at McGill University and provide advice to a variety of stakeholders on the intersections of technology, the nature of conflict and international peace and security interventions.

Today I would like to offer my perspective on three interlinked topics — first, how digital technologies are reshaping the conflicts on which the Security Council is engaged; secondly, how those technologies and their use by parties to conflict and the United Nations itself impact the Organization's efforts to prevent and resolve violence; and, thirdly, I would like to offer some suggestions to the Council on how the United Nations peace and security toolkit, especially its peace operations, can adapt to work more effectively and responsibly in those evolving contexts.

With regard to the first topic, on impact, the Council has heard on several previous occasions how digital technologies have served as accelerants of in- and out-group dynamics, platforms for the rapid spread of anti-information or misinformation and tools for the manipulation of populations, including by State, non-State and extremist actors. In Myanmar, for example, the unchecked incitement of violence on Facebook and algorithms that raised the profile of extreme ideas are well documented in contributing to the genocidal violence perpetrated against the Rohingya people. Since then, access to the Internet and communications has been used as a tool to control refugee populations in Cox's Bazar. More recently, the conflict in Ukraine has highlighted the centrality of public narrative to the strategies of most, if not all, parties to modern conflict.

In many of the conflicts and fragile settings in which the United Nations is engaged, it is important to note that populations are distinctly vulnerable to misinformation and disinformation. Some countries, such as the Central African Republic, lack a traditional journalistic professional culture and media infrastructure, leaving people almost exclusively dependent on social media for news. Moreover, while social media companies make much of their work to combat disinformation on their platforms, the disclosure of internal documents from Facebook in 2021 revealed that content moderation resources were heavily skewed towards the United States and the West, while some fragile and conflict-affected settings were virtually ignored. In that regard, the Security Council has an opportunity to demand of

social media companies that their responsibilities apply equally across their global reach.

In addition to their impact on conflict dynamics, digital technologies are increasingly an important arena for the protection or deprivation of human rights in conflict settings. In Afghanistan, civilians have spoken about the impact of the ever-present hum of unmanned aerial systems on their mental health, while in Myanmar the military junta has used its control over the Internet to target opponents of the 2021 coup d'état and limit their ability to communicate and organize. During the migrant crisis brought about by the conflict in Syria and more recently in the conflict in Ukraine, serious questions around informed consent for the collection and management of biometric data, including by humanitarian actors, have come to the fore.

Turning to the second topic, on the impact on peace operations, as the centrality of digital technologies and of the narrative to the logic of war grows, United Nations operations deployed in those conflicts have inevitably been drawn into strategies by conflict parties to influence the outcome in their favour. In the Central African Republic, the United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic has been the target of deliberate campaigns aimed at undermining the credibility of the Mission in the eyes of the population. The motivations for those activities seem to differ widely depending on the setting and the actors involved. In Mali, for example, disinformation targeting the United Nations Multidimensional Integrated Stabilization Mission in Mali from some local power brokers appears aimed at undermining Mission operations that would disrupt illegal economic networks. In other cases, disinformation actors seem to be motivated by ideological objectives, while in still other situations the United Nations seems to provide an effective foil for a host State or its partners seeking to deflect attention from its performance in delivering security and services to its population. Whatever the motivations, those attacks grievously reduce United Nations access to local populations in need, undermine its relationship with host Governments and parties to mediation and peace processes, and in some cases seriously threaten the safety and security of peacekeepers.

But it is equally important to acknowledge the role played by digital technologies in enabling the United Nations to effectively execute its mandates in modern conflict environments. United Nations peace operations in Somalia and Mali, for example, are making use of natural language processing technologies to rapidly gain a nuanced understanding of local perceptions and national political discourse. Monitoring and surveillance technologies such as unarmed unmanned aerial systems are being used with increasingly effective integration into mission-wide qualitative and quantitative data-gathering tools and analysis systems to generate higher-quality peacekeeping intelligence. That translates into better-informed detection of threats and more rapid action to protect civilians and, of course, to ensure the safety and security of United Nations personnel.

In that context, I would like to offer some thoughts for the Council's consideration on how the United Nations can adapt to the impacts of digital technologies on conflict, mitigate the negative impacts of those technologies on their own operations and use digital technologies more effectively and responsibly in those contexts. In that regard, I see four areas in particular.

First, the United Nations should take on a more explicit and deliberate role as an information actor in conflict environments. Access to accurate information can be increasingly considered as a human right in situations of information warfare, and the United Nations has a role in truth-telling and as a conduit for reliable information. I should point out that that is a role that United Nations missions have played for many years within the mechanisms of peace processes, for example, through ceasefire monitoring. So it bears considering how good practices developed through those mechanisms could be brought to bear to inform societies more broadly in conflict.

For the United Nations to play such a role, however, it will be critical that its operations gain and keep the trust of different facets of the population. That is no easy task when some United Nations activities such as the protection of civilians or support to host State authorities can leave missions open to criticisms — sometimes warranted, sometimes not — and even more so when those missions are the target of disinformation campaigns. That is why, as a second priority, United Nations peace operations need to significantly scale up their capacities to monitor and analyse the information space and to respond effectively in the face of malicious communications. To quote a recent report from the International Peace Institute, missions need to "anticipate crises and proactively reframe the narrative, to engage in two-way rather than

one-way communication” and “to tailor their messages to specific audiences”.

Thirdly, the United Nations itself will require new technologies and the capacities to use them effectively, both in the field of communications and in the areas of situational awareness and peacekeeping intelligence, data analytics for strategic planning and new technologies for dialogue and mediation, to name just a few. As the United Nations pushes forward with many exciting innovations in those areas, including those highlighted by Ms. DiCarlo, it is vital that we recognize that those tools bring with them important and complex ethical, legal and political questions that have a bearing on the rights of people already suffering under conflict. While it may be tempting to adopt the frames and doctrine of Member States for the use of those tools, I would submit to the Council that United Nations operations are distinct in their interests and responsibilities when using sensitive technologies in conflict settings.

Therefore, as a fourth recommendation, I would like to highlight the importance of the ways in which the United Nations acquires and uses new technologies to the credibility and political positioning of those missions in the field. Experience has shown that the procurement of, and partnerships for, sensitive new technologies are most effective when they reinforce the impartiality of the United Nations and provide credible public assurances of responsible use.

I therefore urge the Secretariat to develop its own organic tools, policies and procedures that take the distinct nature of the United Nations as a user of those technologies into account. There is already valuable work to that effect under way, including in the Department of Peace Operations, which is working to enrich its policies on monitoring and surveillance, and also in the United Nations-wide efforts led by United Nations Global Pulse to roll out a data privacy policy across the system. If done well, and in full transparency of Member States and the public, I believe that those efforts have an important normative effect in setting the standard for how sensitive technologies can be used responsibly in conflict situations with vulnerable populations.

Those efforts should include a frank reckoning on the limits of the ability of the United Nations to protect sensitive information, especially individual information, from intrusions by State and non-State actors and a subsequent review of practices around, for example, the gathering of biometric data during the course of humanitarian operations. That review should also include the development of further guidance on how the United Nations shares information with non-United Nations forces, including parallel military forces, host authorities and international rule-of-law actors, in line with the United Nations Due Diligence Policy on Human Rights.

In conclusion, today’s discussion engages two very distinct yet deeply interlinked sets of issues: first, how digital technologies are changing the nature of conflict in situations in which the United Nations is engaged; and, secondly, how the United Nations itself employs digital technologies in the service of its mandates. Both require nuanced consideration and debate as well as distinct policy and operational responses. It is vital to the success of our current and future operations that we get both sets of issues right. The Council has a critical role to play in that regard.

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

I would like to draw the attention of speakers to paragraph 22 of presidential note S/2017/507, which encourages all participants in Council meetings to deliver their statements in five minutes or less, in line with the Security Council’s commitment to making more effective use of open meetings.

I shall now make a statement in my capacity as the representative of the United States.

I thank Under-Secretary-General Di Carlo for her briefing. Her remarks made clear that new technologies are already playing a critical role in the United Nations peacekeeping efforts, and it is essential that they be used in a constructive manner. I thank Ms. Nyabola for her invaluable perspective on both the benefits and the challenges that human rights activists and civil society face from the potential use, as well as the misuse, of those technologies. I thank Mr. Druet for sharing the ways in which digital technology can be used to support the work of our peacekeepers, while its misuse can also undermine them. Let me be sure to maximize the former and minimize the latter. This briefing is about an enormous opportunity and a pressing challenge.

The opportunity is for the Security Council to harness the power of digital technology to advance peace and security in order to responsibly use those tools to do enormous good in the very conflicts and

contexts where they are doing harm. After all, such technologies have immense potential to support the good work of the United Nations system around the world. Social media tools and messaging applications can facilitate access to life-saving information prior to and during conflict. Data from satellites can identify risk from climate change, provide critical information to peacekeepers and improve emergency communications during conflict and natural disasters. We can identify and stop famines before they start. We can find homes, housing and jobs for refugees. We can better protect our peacekeepers and those whom they are mandated to serve.

But we also have to address a pressing challenge, which is the way in which digital technologies are being misused to restrict human rights and fuel conflict. In the hands of State actors and, in some cases, non-State actors, such technologies are being used to cut off access to information, suppress freedom of expression and spread disinformation, thereby escalating conflict, undermining the foundational values of the Charter of the United Nations that we are charged with upholding.

In the Central African Republic and Mali, disinformation targeting United Nations peacekeeping missions has threatened peacekeepers' safety and security and has undermined the ability of missions to protect civilians. In Ethiopia, the authorities have cut off Internet access in the Tigray region since November 2020 as conflict erupted between the Ethiopian National Defence Forces and regional forces in Tigray. Such actions hamper the ability of civilians to access health services, delay the documentation of atrocities and human rights abuses, disrupt financial services and restrict family members from connecting virtually to loved ones.

Countries sitting at this very table are also using technology to harass, arbitrarily surveil and censor and repress civil society and independent media as never before. Nowhere is that more evident than in Russia's war of choice against Ukraine. The Russian Government continues to shut down, restrict and degrade Internet connectivity, censor content, spread disinformation online and intimidate and arrest journalists for reporting the truth about its invasion. Those practices are as wrong as they are widespread. As the Council already heard from Ms. Nyabola, the non-governmental organization Access Now estimates that in 2021 there were 182 Internet shutdowns in 34 countries. Even more troubling, we often hear claims that such actions are taken in the name of protecting peace and security. Nothing could be further from the truth.

We also continue to see non-State actors, including terrorists and violent extremists, use online communications platforms to recruit, radicalize and mobilize to violence. All of us who are committed to addressing and preventing conflict worldwide must do our part to ensure that technologies serve as a force for positive change, and not as a tool misused to perpetrate human rights abuses, fuel hatred and exacerbate conflict.

That is why the United States is working with civil society, the private sector and other stakeholders to advance this global effort. For our part, we are calling out the use of partial and complete Internet shutdowns, censorship and other tactics to prevent the exercise of freedom of expression online. Following on from the Summit for Democracy, we are continuing to join forces with our partners in the Freedom Online Coalition to protect Internet freedom and ensure that entire digital ecosystems respect international human rights frameworks.

We know that surveillance tools and other dual-use technologies can be misused to threaten human rights defenders and others. That is why we are using export controls to hold accountable companies that develop, traffic or use spyware and other technologies that enable such malicious activity.

We are working through the United Nations and other forums to champion the framework of responsible State behaviour in cyberspace. which makes clear that international law applies to States' cyberactivities and lays out a set of voluntary norms to guide their behaviour in peacetime. We are also standing together with countries around the world to protect against, and respond to, malicious cyberactivities. Across the globe gendered forms of online harassment and abuse, including disinformation campaigns against women leaders, are disrupting women's equal participation in decision-making on matters of peace and security.

We have to work together to combat misinformation and disinformation globally. The United Nations is already playing a key role in producing transparent and easily accessible information and advocating on behalf of journalists on the front lines.

We also need to embrace the opportunities to unlock technologies' latent potential for advancing peace and

security. Last month, a group of 60 global partners therefore launched the Declaration for the Future of the Internet to revitalize a democratic vision for the global Internet. We invite all relevant authorities and States Members of the United Nations that are committed to upholding the Declaration's principle to join us.

To effectively maintain peace and security in the twenty-first century, we need to respond to twenty-first-century threats and deploy twenty-first-century tools. Now is the time for the United Nations to responsibly harness the power of digital technology to take on our most pressing challenges and advance peace and security around the world.

I now resume my functions as President of the Council.

Mr. Hoxha (Albania): We thank the United States for organizing this timely meeting to discuss this as complex as important topic. We also thank Under-Secretary-General DiCarlo for her always thoughtful insights.

We are pleased that civil society was given a prominent place at this meeting — and for a good reason, as we heard with the breadth that they offered and the recommendations that they made. I therefore thank Ms. Nyabola and Mr. Druet.

The rapid development of technology has changed how the world works, impacting every aspect of modern life. It has become so ingrained in our daily lives that it is hard to remember what the world was like before.

Modern technology undeniably brings a number of advantages across multiple sectors. Individuals, States, Governments, industry, health care, financial systems, regional and international organizations and peacekeeping missions all take advantage of the rapid growth of digital technologies. They help people become more productive, and they help companies and entities become more innovative, flexible and adaptive than ever before.

We have happily embraced the interconnectivity of devices and systems, which has visibly made our lives and work easier, but that inevitably comes with the cost of exposure to a wide range of threats by malicious forces. The nexus "new tech, new threats" needs no explanation.

As we heard today, there is a common understanding about the immense risks arising from malicious activities by both State and non-State actors. The misuse of information and communications technologies has a direct impact on international peace and security, as it undermines the integrity, security, economic growth and stability of the global community, leading to disputes and conflicts.

Given the mounting concerns about the dual-use nature of technology and its implications for the maintenance of international peace and security, it is very important that the Security Council take a leading role in assessing such risks and implications. I therefore very much welcome the holding of today's meeting.

Artificial intelligence is doing wonders in many sectors, including agriculture and medicine — saving lives, increasing food production, improving energy sources and managing production processes. But, if not properly used and, especially, if ethics are not respected, it can lead to serious breaches of human rights, such as undue surveillance targeting specific groups and communities. As technology usually develops faster than States can grasp its full impact, we must make sure that core principles and values— such as equity, equality, inclusivity, responsibility, transparency and accountability— are preserved from negative impact.

Unfortunately, the potential of technology to dramatically impact social cohesion and, of course, international peace and security through misuse by State or non-State actors is growing significantly. Some countries are continuously trying to deliberately provide misleading information, distort facts, interfere in the democratic processes of others, spread hatred, promote discrimination and incite violence or conflicts by misusing digital technologies. In the same vein, we see with concern Internet shutdowns and the restriction or denial of human rights and freedoms in using them. The briefers offered concrete examples. We should redouble efforts to mitigate the harm that they may cause, as outlined in the report of the Secretary-General on a road map for digital cooperation (A/74/821), and look carefully at his recommendations.

I want to highlight Albania's firm position for a global, open, free, stable and secure cyberspace where international law, including respect for human rights and fundamental freedoms, fully apply, in support of social, political and economic development.

We are very concerned about the increase of malicious cyber and digital activities in recent months. We know that Russia's actions caused communication

outages, including against critical infrastructure, not only in Ukraine but also in other parts of Europe, by deliberately attacking Viasat's satellite on 24 February 2022, just one hour before Russia's unprovoked and unjustified invasion of Ukraine.

Cyberattacks reportedly originating in Russia have also attempted to interfere in Ukrainian elections, targeting its power grid, defacing its Government websites and spreading malware in their systems, with destructive effect. The Western Balkans, where I am from, are being systematically targeted by campaigns of interference and information manipulation in order to intentionally trigger political instability and undermine their Euro-Atlantic aspirations. We will not allow it, and we will resist it.

Other notorious examples are the repeated malicious activities by the regime of the Democratic People's Republic of Korea, which is trying to collect intelligence, conduct cyberattacks and generate unlawful income, which, inter alia, serves to fund its militarization and proliferation, in violation of international law and Security Council resolutions. We add to that list the Internet shutdowns in Myanmar, which were also mentioned today. We call for a stop to such activities and for upholding existing norms and the rules-based international order in cyberspace. The Internet is not and should not become a weapon but remain a public good.

We welcome the reports of the Group of Governmental Experts and the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Through them, Member States have agreed on a substantial United Nations framework that includes existing international law, 11 voluntary non-binding norms, confidence-building measures, capacity-building and the expertise of the multi-stakeholder community.

Let me end with this — throughout history, new challenges have opened new opportunities for cooperation. Today is no different, even if the challenges at hand are highly complex, quickly evolving and come amid a rising sense of conflict and crisis. But there is no alternative to meaningful dialogue, cooperation through responsible behaviour, first, and then normative frameworks on how technological developments are affecting individuals, States and societies and the uses and applications of technology generating the most disruption, particularly those that pose a direct threat to peace and security. As for many other aspects, it is for us to decide whether to share the huge benefits or bear the enormous costs.

Mr. De Rivière (France) (*spoke in French*): I thank Ms. DiCarlo, Ms. Nyabola and Mr. Druet for their briefings.

I will focus on three points.

First and foremost, digital technologies are an opportunity for international peace and security. Peacekeeping operations have been at the forefront of those efforts. The presidential statement adopted in August (S/PRST/2021/17) at the initiative of India took stock of the situation. These technologies contribute to the safety of peacekeepers and the performance of operations, particularly with a view to improving the protection of civilians. They are revolutionizing strategic peacekeeping communications. France will therefore continue to support all those innovations.

Technology is also a lever for mobilizing and including civil society. In the Sudan, the United Nations Mission in the Sudan conducted an online consultation that allowed all of civil society to make their voices heard, including in the regions. By facilitating the flow of information, technologies also contribute to the fight against impunity, as illustrated by the media coverage and open-source intelligence in the context of the conflict in Ukraine.

However, the malicious uses of technologies are proliferating and can constitute a threat to international peace and security. That is my second point.

That is true for the development of cyberthreats, as illustrated once again by the conflict in Ukraine. France and the European Union, as well as several partners, have condemned the cyberattacks conducted by Russia against a network of satellites one hour before the invasion of Ukraine, with the aim of facilitating its aggression. International law applies in its entirety to cyberspace. We also condemn North Korea's malicious cyberactivities of stealing sensitive information and cryptocurrencies to aid their nuclear and ballistic programmes. We are also concerned about the increasing use of cryptocurrencies for terrorist financing. We condemn the increasing attacks on humanitarian actors and non-governmental organizations.

Digital technologies also facilitate information warfare. We condemn the massive disinformation

campaigns under way in the Central African Republic and Mali, as well as those supporting Russia's war against Ukraine. In Mali, France recently thwarted an attempt to manipulate information by the mercenaries of the Wagner Group. That example shows the threat posed by hybrid strategies that seek to blur the line between State and non-State actors.

Internet shutdowns violate human rights. We deplore the ongoing interruption of telecommunications in northern Ethiopia. It has made it difficult to gather evidence of human rights violations, which must not go unpunished. In the Middle East, Internet shutdowns are used to weaken protest movements, and some rights defenders are monitored and harassed on social networks.

In the face of those increasing threats, Governments must respond through cooperation and law. That is my third point.

The United Nations offers an irreplaceable framework for doing so. France will continue to contribute to it, including by ensuring that Security Council resolutions take those challenges into account. Along with a group of 60 countries, we are promoting the establishment within the United Nations of a programme of action to increase the capacity of States to implement agreed standards in cyberspace and to strengthen the resilience of networks.

Mr. Tirumurti (India): I welcome the initiative of the United States in organizing today's important briefing. I thank the Under-Secretary-General, Ms. Rosemary DiCarlo, and the other briefers, Ms. Nyabola and Mr. Druet, for their valuable insights.

The increasing use of digital technologies has accelerated economic development, improved service delivery to citizens, generated greater social awareness and placed information and knowledge directly in the hands of individuals. They have made governance more inclusive, citizen-centric and transparent. Most activities in this digital age — political, social, economic, humanitarian and developmental — are now invariably conducted in or connected to cyberspace. However, given their dual-use nature and susceptibility to harmful uses by both State and non-State actors, they can also have a negative impact on international peace and security.

The nature of conflict and its underlying tools have changed tremendously over the decades. While inter-State conflicts continue, we are witnessing growing threats from non-State actors, including terrorist groups. Similarly, the theatres of war and conflict have also expanded. In addition to territorial conflicts, the world is facing newer conflicts in seas and space — and by space, I refer to both outer space and cyberspace. Technology has become the common underlying denominator, as well as a game changer, in these conflicts. Our conventional approach to security nationally and internationally therefore needs a reset.

I would like to submit the following five issues for the Security Council's consideration. First, there is the need to address the abuse of digital technologies by terrorist groups to disseminate terrorist ideologies, radicalize, incite violence and recruit the next generation of terrorist actors taking advantage of the enhanced online presence of young people. Terrorist groups are taking advantage of online tools to build networks, recruit new members, procure weapons and secure logistical support. The digital communications methods used by these groups are organized and sophisticated. They have become adept at using gaming chat rooms, dark-web and other restricted-access sites and unregulated online space to spread propaganda and incite violence. There have been instances of terrorists live-streaming their attacks on major platforms to maximize publicity and impact. The wide outreach of online space has enabled the terrorist groups to take advantage of the openness of pluralistic democratic societies, like our own, by fuelling societal divisions and sectarian hatred and by supporting anti-democratic movements and radical ideologies aimed at destabilizing Governments and State institutions.

The ability of terrorist actors to connect, communicate and share information over digital platforms only underscores the growing need to regulate such inflammatory content online. Equally needed are efforts to address the legal challenges in bringing the perpetrators of these crimes to justice, particularly owing to the remote nature of their involvement in terrorist activities. While we are used to looking at terrorism as a direct physical attack by perpetrators, in the digital domain, perpetrators inciting terrorist acts through hateful content and radical ideologies may be far from the actors actually committing the act of terror. The instigators should be held equally responsible for such acts of terror. They cannot be less culpable than those who commit acts of terror. This is essential when we consider terrorism in the cyberdomain.

Emergence of new financial technologies such as new payment methods (NPMs), virtual currencies and online-fundraising methods, including direct donations, non-fungible tokens and crowd-funding platforms — and the ease of access, anonymity and intractability offered by them — have enabled terrorist entities to collect and transfer funds while evading monitoring and enforcement structures. Such NPMs as prepaid phone cards, online-payment services and virtual money have enabled terrorist groups to exchange them for gold, silver and other metals and, most recently, for mobile-phone payments, and fund terrorist activities. Prepaid cards are frequently used as an alternative to cash. The use of bitcoins for funding terror activities is also well established. In addition, terrorist misuse of artificial intelligence and 3D printing for various terrorist purposes, which have a global reach, also demands our immediate attention.

The need for Member States to comprehensively address and tackle the implications of terrorist exploitation of digital technologies more strategically has never been more dire. In this regard, I am happy to inform the Security Council that India has proposed holding a special meeting of the Council's Counter-Terrorism Committee in India soon, which will exclusively focus on this issue and attempt to provide the way forward.

Secondly, some States are leveraging their expertise in the digital domain to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism, attacks on critical national infrastructure, including health and energy facilities, and disrupt social harmony through promoting radicalization through the online space. Open societies have been particularly vulnerable to such threats and disinformation campaigns. Emerging digital technologies —for instance, the use of machine learning and big data — have the potential to enhance the lethality of such acts, thus posing a considerable threat to international peace and security. The international community cannot take a selective approach and needs to avoid double standards when it comes to addressing these threats.

Thirdly, the interconnected nature of the digital domain requires that solutions to the complex problems and threats emanating from this domain cannot be resolved in isolation. There is an underlying need to adopt a collaborative rules-based approach and work towards ensuring its openness, stability and security. Fostering equitable access to digital technologies and their benefits should also form an important component of this approach. The widening digital divide, digital gender divide and digital knowledge gaps create an unsustainable environment in the cyberdomain. Growing digital dependency in the post-coronavirus-disease era has exacerbated risks and exposed these fissures of digital inequalities. These must be bridged through capacity-building and technology transfers.

Fourthly, United Nations peacekeeping missions need to be equipped with the latest digital technologies to counter those employed by armed groups. Protecting the protectors should be as much our priority as protecting civilians. We have acted on this front by rolling out, in partnership with the United Nations, the Unite Aware platform during our presidency of the Council in August 2021. This technology programme provides real-time threat assessment to peacekeepers and needs to be scaled up across all United Nations peacekeeping missions. I thank the representative of France for referring to the presidential statement on technology and peacekeeping (S/PRST/2021/17) adopted under our presidency in 2021.

Fifthly, maintaining international peace and security in cyberspace also depends on exchange of information among countries on the misuse of digital technologies for committing crimes. This cooperation needs to be effective and in real time in order to deter, disrupt and mitigate such misuse. The establishment of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is therefore a step in the right direction.

In conclusion, let me reiterate that the global community needs to leverage digital technologies for the benefit of all of humankind and not just for a select few. Our overarching objective should be to harness such technologies for the development, prosperity and empowerment of all people and to promote international peace and security. India stands ready to offer its expertise and share its experience in this shared endeavour.

Mr. Zhang Jun (China) (*spoke in Chinese*): The rapid development of science and technology has brought us new opportunities and new challenges. In May 2021, China, Kenya, Mexico and the United Arab Emirates jointly convened an Arria Formula meeting to exchange views in an in-depth manner on the impact

of emerging technologies on international peace and security. China welcomes the opportunity to continue the discussion on technology and security in the Security Council. In order to better develop and utilize science and technology for the benefit of humankind. China would like to propose the following.

First, we must vigorously advocate scientific and technological innovation. Innovation is a primary driver behind development. Each and every scientific, technological and industrial revolution in human history has profoundly transformed our mode of production and lifestyle and tremendously promoted the progress and well-being of humankind.

The world today is facing unprecedented and complex challenges. Fast-changing digital technology, artificial intelligence and biotechnology, inter alia, have played an important role in the fields of pandemic prevention and control, climate change, food security, energy security and others. Be it as a new impetus for world economic growth or as a new way and means for solving major complex issues, innovation in science and technology is simply indispensable.

As the world's economy is highly interdependent and the global industrial and supply chains are deeply intertwined, all countries should view international exchanges and cooperation in science and technology with an open mind and promote them using the relevant measures in order to jointly create an open, fair, just and non-discriminatory environment in that regard while actively conducting joint research and development with a view to fostering progress through concerted efforts.

Secondly, achievements in science and technology must be used for the benefit of all. Technology knows no borders and is part of humankind's shared wealth. Such achievements should not become treasures hidden in caves. At present, the widening technology divide between developed and developing countries — in particular the digital divide — is exacerbating new forms of inequality.

It is necessary to allow multilateral platforms such as the United Nations to fully play their part in supporting the research and development capacities of developing countries; to speed up the transfer of technologies; accelerate the commercialization of scientific achievements; share the dividends of progress in science and technology with developing countries; leapfrog the development gap by narrowing the digital divide; and fast-track the implementation of the 2030 Agenda for Sustainable Development.

Developing countries must be supported in using the latest technology and big data to improve social governance and effectively prevent and combat crimes.

In peacekeeping and peacebuilding, the Council should also actively use new technologies to strengthen its capabilities in information collection, early warning, emergency response and rescue.

Thirdly, it is imperative to work together to manage and control the risks posed by technology. Technological developments can be a source of risk in relation to conflicting rules, societal risks and ethical challenges. The international community should uphold the concept of science and technology for the benefit of humankind; enable the United Nations to fulfil its role as a main channel for active dialogue, exchanges and cooperation; adhere to multilateral and multi-stakeholder participation; jointly manage the risks of technological development; and formulate and improve universally accepted rules and norms.

It is necessary to curb the abuse of information technologies, oppose cybersurveillance and attacks and oppose an arms race in cyberspace. It is crucial to prevent terrorists from using the Internet for recruitment, financing or organizing terrorist attacks, as well as preventing the Internet from becoming a hotbed of hate speech, racism, pornography and violence. Governments should strengthen supervision and control in accordance with the law, standardize the application of technology and better safeguard public interests. Technology platform providers and Internet service providers must standardize their practice and strengthen self-discipline in order to fulfil their social responsibilities.

Fourthly, we oppose the politicization of issues of a technological nature. The world of science is not a zero-sum battlefield. Technological innovation should not produce only one champion. However, it is worrisome that for some time now, certain Governments have politicized issues of a scientific and technological nature. They have generalized the concept of national security, abused State power and wantonly intensified their suppression of other countries' high-technology companies. In order to maintain their monopoly in science and technology, those Governments have established exclusive circles and clubs under so-called strategies or frameworks. They have imposed

technology blockades on other countries and engaged in bullying practices in the field of science and technology. They have interfered with and obstructed economic, trade, scientific and technological cooperation among other countries.

That approach, which carries an obsolete cold war mentality, runs counter to the spirit of international cooperation and the trends of our time. It harms the collective interests of all countries and is doomed to failure. We urge certain Governments to adopt a rational and open-minded approach; to view scientific and technological developments and international cooperation from the right perspective; and to stop groundless attacks and restrictions on high-technology companies of other countries.

In the face of global challenges, the right path is one of solidarity and cooperation. China calls on the countries concerned to stop creating divisions around the globe, including in the Asia-Pacific region; to cease geographical confrontation; to stop drawing lines on the basis of ideology and using coercive measures to force other countries to take sides; to refrain from decoupling the economy and science and technology; and to cease their destructive practices affecting the stability of global supply chains and economic recovery.

China attaches great importance to scientific and technological innovation and has been preventing technology risks in a responsible manner. We have worked actively to promote international consensus and cooperation. In 2020, China, launched a global data security initiative, calling for openness, security and stability in global supply chains while opposing the practice of using information technology to destroy critical infrastructure or conduct large-scale surveillance. It also advocates for respect for national sovereignty and jurisdiction and the right of States to manage their own data. The initiative provides a blueprint for international rules on digital security, which we hope will attract the participation of Governments, international organizations and multi-stakeholders.

Facing the tremendous changes brought about by artificial intelligence and on the basis of the results of years of discussion at the United Nations, at the end of last year China put forward a position paper on regulating the military application of artificial intelligence. It provides a viable framework for the international community to explore the impact of military applications of artificial intelligence on strategic security governance rules and ethics.

In July, scientists from more than 20 countries agreed on the Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists, advocating for responsible research and development in biotechnology, which is the common aspiration of the international scientific community. China welcomes the voluntary adoption and further promotion of the Tianjin Biosecurity Guidelines by all countries and relevant stakeholders so as to prevent the misuse or abuse of biotechnology, to lower the risks associated with biosecurity and to promote the use of biotechnology for the benefit of humankind.

Using science and technology for peaceful purposes and conducting international cooperation in that regard constitute an inalienable right of all States under international law. During its seventy-sixth session, the General Assembly adopted a resolution entitled "Promoting international cooperation on peaceful uses in the context of international security" (resolution 76/234). China and 26 other countries co-sponsored that resolution, urging all countries to lift unreasonable restrictions on the right of developing countries to peaceful uses of science and technology while fulfilling their international non-proliferation obligations.

China welcomes the continued inclusive dialogue within the framework of the General Assembly with a view to enhancing mutual trust, building consensus and ensuring that developing countries fully enjoy their right to the peaceful use of science and technology. That will help us better achieve the Sustainable Development Goals and maintain international peace and security.

Mr. Kiboino (Kenya): I thank Under-Secretary-General DiCarlo; my compatriot, Ms. Nyabola; and Mr. Druet for their insights and recommendations on the topic under consideration today.

When we reflect on the phenomenal role digital technology has played in just this decade and the unprecedented implications the digital revolution has on the peace and security of our time, — and given the pervasive, consequential and largely ungoverned character of digital technologies, — what becomes abundantly clear is the need to have a community of discussants and actors, including the Security Council, to explore the delicate balance between ensuring digital innovation, on the one hand, and addressing

its malicious use by both State and non-State actors in matters related to peace and security, on the other.

Kenya has made significant strides in ensuring Internet accessibility and that the country and its citizenry are protected as much as possible from disruptive and unexpected occurrences and threats in the digital sphere. But we recognize that cybersecurity is not and cannot be a single-country endeavour. Indeed, the conventional pursuance of international peace and security by the multilateral system must now also be undertaken in the cyberdomain.

In that regard, I will highlight five key points for consideration. The first point concerns the need to appreciate that the United Nations should support countries in dealing with the consequences of the digital revolution on their citizenry and national stability, including the misuse of artificial intelligence, big data, social media and other digital frontiers. The Security Council has the responsibility of ensuring that the United Nations has the capacity and expertise to play that role.

My second point involves the link between digital technologies and peace, especially in political transitions. Electoral processes are a democratic promise, but they often face increased security vulnerabilities on digital platforms, with implications for national civic cohesion and crisis management. On 28 October 2021, during our presidency of the Security Council, Kenya convened an Arria Formula meeting on addressing and countering hate speech and preventing incitement to discrimination, hostility and violence in social media. It was evident that policymakers often face a dilemma in striking the balance between freedom of speech and hate speech and between democratic accountability and safeguarding private and proprietary information. We advocate that more attention and investment be accorded to supporting national Governments in addressing the link between cybersecurity and countries electoral security, particularly in conflict situations.

Thirdly, with regard to the partnerships between private sector and policy regulators, the Arria Formula meeting I just mentioned brought together representatives from leading technology companies, including Facebook, Twitter, TikTok and Google and civil society, who demonstrated that it is possible to establish such partnerships. Enhanced partnerships among technological companies, policy regulators and the United Nations will make it possible to establish effective mechanisms and standards for ensuring responsible conduct in cyberspace, based on principles that speak to the public good in a manner that builds bridges of peace among diverse groups and across divisive topics.

The fourth concerns the link between digital technologies and terrorism. The ubiquitous, programmable and data-driven nature of emerging technologies — although beneficial — has opened a door for their misuse by armed groups and terrorists. They capitalize on simplified user-interface systems to recruit, radicalize, mobilize resources and plan and carry out terrorist acts. There is a need to ensure that States have the capacities to mitigate the online terrorist threat, augment investigative skills and collaborate in reducing the rate of online radicalization and illicit financial flows and identifying and removing online extremist content.

The fifth involves inclusion and the protection of participation. We believe that governmental responsibility for Internet accessibility also includes the protection of those accessing the digital platform, including social media. In particular, the safety of women participating in peace and security processes remains critical. States must therefore ramp up accountability for and the prosecution of perpetrators of online attacks, intimidation, the publication of private media and physical violence against women participating in the peace agenda. As part of safeguarding the protection and participation pillars of the women and peace and security agenda, the Security Council should also take specific steps, particularly to increase the costs of all forms of online intimidation against women who have briefed the Council.

Mr. Gómez Robledo Verduzco (Mexico) (*spoke in Spanish*): At the outset, we would like to thank you, Madam President, for convening this meeting on a topic with almost infinite ramifications that calls on us to reflect, inter alia, on how to adapt the work of the United Nations to overcome the challenges posed by the use of digital technology to the maintenance of international peace and security. We are also grateful to this morning's briefers — Under-Secretary-General DiCarlo, the Director of Advox, and Professor Druet of McGill University — for their excellent analyses and proposals.

If we look at things head-on, we must proceed from the principle that the use of digital technology, first

and foremost, must be used to defend human rights and democracy. The two aspects are inseparably linked. In that regard, Mexico reaffirms its commitment, which it has maintained throughout the years, to a free, open, stable and secure cyberspace in which international law, including international human rights law, international humanitarian law, international criminal law and other legal precedents establishing, for example, the right to privacy, is fully applicable. We recall the agreements that we have already reached and are under way at the intergovernmental level, especially in the area of cybersecurity, through the reports of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. Similarly, it is incumbent on us to recall other processes under way, including the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Innovative solutions to current challenges in peacekeeping need to be sought, in particular through strengthening digital technological capacities in peace operations and special political missions, as was mentioned earlier in today's briefings. The use of technology can contribute very constructively to improving early-warning detection of emerging threats, preventing humanitarian crises and human rights violations and strengthening the measures necessary for protecting and supporting civilians and civilian infrastructure, including combating arms trafficking and mine-clearance activities.

New technologies show particular promise in areas, such as medical-care support, including the provision of timely, routine and emergency mental-health and psychosocial care. Both peacekeepers and civilians affected by humanitarian crises can benefit from the flexibility and accessibility afforded by telemedicine. Moreover, we have seen that the use of renewable energy technologies can enhance the safety and security of United Nations personnel and the effectiveness and sustainability of missions. In the face of the growing environment of misinformation, which was highlighted earlier, the use of social networks is key to strengthening relations between peacekeeping missions and the communities in which they operate. For that reason, the provisions of resolution 2589 (2021) and presidential statement S/PRST/2021/17, in which the Security Council acknowledged that technology could help peacekeeping missions better understand the environments in which they operate, are absolutely essential and should enable us to improve the way we collect, analyse and share information.

Similarly, we take note of the Secretary-General's Strategy for the Digital Transformation of United Nations Peacekeeping with regard to new technologies and information and follow-up on the Action for Peacekeeping Plus initiative. The implementation of the Strategy requires greater coordination between the United Nations system and stakeholders on the ground, as well as cooperation with regional organizations, the private sector, civil society and, of course, academia.

At the most United Nations Peacekeeping Ministerial conference recent United Nations Peacekeeping Ministerial Conference, Mexico endorsed the initiative put forward by the Republic of Korea on technology and medical capacity-building in peacekeeping. The initiative has three objectives — maximize the use of available technologies to better understand situations and provide early warning; respond to disinformation in conflict situations and improve cybersecurity intelligence and promote capacity-building in the area of data and information analysis.

Lastly, resolution 75/316, endorsed by Mexico in the General Assembly, underscored the impact that rapid technological change will have on achieving the 2030 Agenda for Sustainable Development and, therefore, on international peace and stability. We underscore the importance of the Road Map for Digital Cooperation and the information contained in the report *Our Common Agenda* (A/75/982).

Mr. Agyeman (Ghana): At the outset, I would like to thank the United States for convening today's briefing on the use of digital technologies in maintaining international peace and security.

I also thank Under-Secretary-General Rosemary DiCarlo for her insightful briefing, as well as Nanjala Nyabola, Director of Advox, the Digital Rights Project of Global Voices, and Dirk Druet, Adjunct Professor at the McGill University Centre for International Peace and Security Studies, for their additional perspectives.

In recognizing the pervasive nature of digital technologies globally, Ghana shares the view that such technologies can play an important role in maintaining international peace and must therefore be leveraged

to enhance our collective security. We believe that cognizant of the demands of national sovereignty and territorial integrity, digital technologies, which overcome territorial barriers, can be used in strengthening preventive diplomacy objectives, through enhanced situational awareness, in activating early warning, detecting emerging threats and bridging societal differences, as disparate views and positions are mobilized into a constructive and coherent whole for reinforcing peace objectives.

In situations of conflict management, we also see the benefits that digital technologies can bring in analysing risks, improving the lead time required for protecting civilians and civilian infrastructure, and the rigour it provides in better defending the mandates of peace support operations and enhancing the safety and security of uniformed and other personnel. Digital technologies can also strongly support peacebuilding efforts and the rebuilding of societies fractured by war.

Ghana believes that the immeasurable benefits that digital technologies can provide in strengthening efforts for the maintenance of international peace and security can better accrue only if there is a common understanding of the normative framework that underpins such an enhanced and complementary approach in leveraging the available modern tools in pacifying our world. Indeed, we are aware that despite the benign nature of digital technologies, they can also exacerbate global insecurity if not used responsibly. They can deepen mistrust if perceptions persist in strained and fragile societies that exogenous forces are manipulating the will of a population towards values that may be foreign to those societies.

We also note the malicious manner in which digital technologies have been used, in some instances by State and non-State actors to misinform and manipulate populations, threaten and harass individual activists and journalists and fuel discrimination in ways that subvert national unity and coherence. The way such technologies have been used in recruiting and radicalizing people into terrorist groups, organizing terrorist attacks and financing terrorist activities is also of great concern.

Against the backdrop of the great potential of digital technologies in reinforcing the available tools for the maintenance of international peace and security, but mindful of its negative consequences, we would like to highlight a few additional points. As previously indicated, the use of digital technologies for the maintenance of international peace and security must proceed from a point of convergence and on the basis of principles that respect national sovereignty and promote universal values. In that regard, we believe that the United Nations has an indispensable role to play in enhancing the positive impact of digital technologies on global peace. For instance, building upon the commitments in the Secretary-General's Strategy for the Digital Transformation of United Nations Peacekeeping, which aims to embrace the opportunities offered by digital technologies, will enable missions to adapt to changing conflict dynamics and take advantage of increased efficiencies. Furthermore, lessons learned by the Department of Political and Peacebuilding Affairs in mediation efforts during the coronavirus disease pandemic using digital technologies can offer an acceptable path in constructing enduring frameworks for such engagements with wider populations for the cause of peace.

Secondly, the capacity of national Governments to enhance their cybersecurity space should be at the heart of developing a robust framework for the use of digital technologies. The malicious use of digital technologies by terrorists and extremist groups and the trend towards cyberwarfare require that vulnerable countries, such as some in Africa where fragilities exist, obtain the required support to strengthen their digital capacity, in line with the African Union's Digital Transformation Strategy for Africa (2020-2030). Such capacity-building efforts should include the gathering, processing, use and analysis of new technologies and their impact on security. In that regard, the supportive role of the Counter-Terrorism Committee Executive Directorate is commendable, and we welcome more such efforts.

Thirdly, States also have a critical role to play in enacting policies that prevent the misuse of cyberspace with elements that, inter alia, encourage investments in critical national infrastructure, promotes responsible media content and facilitates the early detection, investigation and prosecution of offenders. States ought to make good their commitment to the Charter of the United Nations by respecting international human rights law in a manner that ensures that personal data collected, stored, processed, used, transferred and disclosed upholds and protects the privacy of individuals. Furthermore, we welcome measures that encourage companies to uphold international human

rights law and business standards, based on the United Nations Guiding Principles on Business and Human Rights.

Fourthly, cognizant of the effectiveness of regional arrangements in preventing conflicts through early-warning mechanisms and in building peace in post-conflict settings, we strongly urge the strengthening of digital-technology partnerships between global multilateral systems and regional bodies. We encourage support for the implementation of existing treaties, such as the Budapest Convention and the African Union Convention on Cybersecurity and Personal Data Protection, otherwise known as the Malabo Convention, and believe that early-warning mechanisms, such as those of the Economic Community of West African States and the African Union, can be further deepened through strong global support.

Moreover, support for regional platforms for intelligence and information-sharing could further enhance the early detection of the expansionist agenda of terrorist networks, including in West Africa and in relation to their online activities. Additionally, action to cut off terrorism financing must be sustained and enhanced, including in the spaced-out economy, where cryptocurrencies have become a medium of choice for financing terrorist activities. While the collaboration between the Intergovernmental Action Group against Money Laundering in West Africa and West African national financial intelligence centres has produced significant outcomes, its actions would continue to require deepening.

Before concluding, I would like to mention Ghana's commitment to enhancing the use of technologies for peaceful purposes through actions that have been undertaken to strengthen the domestic information and communications technology ecosystem. In addition to the institutionalization of a national cybersecurity awareness month aimed at elevating the whole-of-society awareness of cyberthreats, the operationalization of sectoral computer-emergency-response teams in key institutions, such as the National Communication Authority, the Central Bank and the National Information Technology Agency, have enhanced the resilience of the cyber-ecosystem across online services, the financial sector and Government business. We therefore advocate a whole-of-society approach in developing resilience in the peace-and-security nexus, including partnerships with the private sector, civil society organizations and the technology giants, whose increasing role has to be made to serve the public good. Also, women and the youth are critical agents of change and will remain crucial to enhancing the positive impact of technologies on global security.

With a commitment to the collective objective of enhancing all available tools, Ghana believes that multilateral and regional initiatives can effectively harness technologies for the objectives of global peace and security.

Mr. Nebenzia (Russian Federation) (*spoke in Russian*): We wish to thank our briefers for their briefings.

Digital technologies have transformed the world and become an integral part of its economic, political and social processes. There were hopes that they would become an engine of economic and social progress and that they would simplify communication and help humankind make the transition to a new digital stage of development.

During the coronavirus disease pandemic, it was thanks to information and communication technologies (ICT) that jobs and the unity of the world divided by quarantine were preserved. Government-provided public services, including the work of hospitals, banks and the financial sector in general, schools and other institutions critical to society, became almost entirely linked with ICT. It is no exaggeration to say that humankind is far more dependent on ICTs today than at any time in its history.

But the hopes that ICT would be an unequivocal force for good have not been fulfilled. The culprit is not technology, but the fact that it has been used to achieve geopolitical goals and to impose hegemony. That is the case not only in the physical environment, but also in the online environment.

In recent years, the manipulation of information has assumed threatening proportions. A whole army of pseudo-investigators from non-governmental organizations has emerged which, at the behest of Western Governments, are churning out biased so-called investigations that are in fact generating and disseminating numerous fakes and uncorroborated information from open sources to tarnish countries whose are inconvenient to the West. A notorious example of that is the White Helmets and Bellingcat. They have distinguished themselves for gross fabrications in the interests of Western propaganda on the Syrian chemical

dossier, the Malaysia Airlines Flight MH-17 story and many other high-profile issues. Experts have repeatedly caught them red handed, so to speak, pointing out the inconsistencies in their conclusions, which have nothing to do with professional, independent investigative journalism and are reached in violation of all the most basic principles.

We are deeply troubled by a new trend: an information war is being fought not just in a manner that is completely divorced from reality, but also with the goal of distorting it and completely superseding it. The truth is being pushed aside by an intense flow of information and ideologically charged spam, so as not to give the audience the slightest opportunity to gain access to objective information.

An egregious example of that is the information unleashed by the Western media, under the direction of their Governments, concerning the deaths of civilians in Bucha, in which case the Russian military was blamed. All objective facts and evidence were swept under the rug, and outright fakes were instead disseminated. Under pressure from the facts, even the Western media were eventually forced to admit that many peaceful residents of Bucha died not from gunshot wounds, as Ukraine claimed, but from obsolete artillery shells that had been used by the Ukrainian armed forces when they bombed that city. Now they are using new fakes to shift focus from the evident responsibility of Ukraine's armed forces for the provocation. Similarly, they are also silent about the attacks on Kramatorsk, after an investigation revealed evidence that clearly shows the involvement of the Ukrainian armed forces.

In recent months, the work of the collective Western Ministry of Truth, or more accurately the Ministry of Lies, has reached a zenith. A campaign of disinformation and manipulation of public opinion that is unprecedented in its scope and intensity has been unleashed against Russia. The Western media, which were already not known for their objectivity, have finally turned into a mouthpiece for crude State propaganda as well as fake-news factories.

The ICT giants, which have monopolized the sphere of social networks and video hosting, are not behaving any better. Digital platforms have finally thrown off their masks and are no longer trying to hide their political bias. They are blocking any accounts whose content is at odds with the agenda dictated by the Western elites. The Meta corporation has explicitly allowed hate speech and calls for violence against Russians and Russian speakers on its platforms.

States that call themselves a "community of democracies" are in fact engineering true cyber-totalitarianism. They want to create a world in which they — and they alone — will have complete control over the information flows and determine what is true and what the audience needs to read and see. Any alternative point of view is immediately branded as disinformation and propaganda, and inconvenient facts are cast aside. Russian television channels are being shut down, Russian journalists are being expelled, and access to Russian websites is being blocked. Is that the so-called freedom of access to information? We hope that is what the organizers of today's meeting meant by abuse of restrictions on access to Internet resources under the pretext of ensuring national security.

The Russophobic information attack has been directed by its initiators against various spheres of activity, including those that are completely unrelated to politics, such as education, culture and sports. That is a flagrant violation of the basic principle of the inadmissibility of discrimination on the basis of ethnicity. In addition to the information aggression aimed at people's minds, a campaign has been orchestrated to undermine the ICT infrastructure itself through the organization of computer attacks. In Kyiv, the creation of a cyberarmy was recently announced, and there was open acknowledgement of such cyberattacks against Russian and Belarusian targets. Moreover, the Western sponsors of the Kyiv regime not only did not try to prevent it, but also deliberately cultivated that army of hackers without a thought about the consequences. The relevant tasks, as we are aware, were recently advanced by NATO as part of the Locked Shields cybersecurity exercise in which the Ukrainian armed forces are participating.

In April, Washington announced a $10 million reward for anyone who could justify the theory that Russian intelligence was allegedly involved in cyberattacks on the United States. Our repeated calls to address the issues through the competent agencies were ignored.

Western Governments deliberately engage hacker groups and often ordinary users in launching cyberattacks. Tools and detailed instructions on how to stage computer attacks are published in the public domain, and mass agitation on organizing hacker

attacks against Russian infrastructure is carried out on social networks.

Against that background, we were not surprised that Nina Yankovic, born in western Ukraine and known for leading the information campaign on whitewashing neo-Nazism in Ukraine and spreading information about Russia-gate, which never existed, was appointed to head the so-called Disinformation Governance Board at the United States Department of Homeland Security from 27 April this year. It recently became clear that she was directly instructed by Trump's rival in the election, Hillary Clinton. Even in the United States itself, such blatant cynicism caused a scandal. Yankovic had to resign, and the project has been suspended for the time being. However, we have no doubt that it will be revived in one way or another insofar as, apart from promoting fakes and disinformation, our Western colleagues have almost no diplomatic methods left at their disposal.

Alongside the West's pumping of Ukraine with conventional weapons, there is a parallel uncontrolled distribution of cyberweapons and techniques for their use. Practical skills are being acquired by a huge number of people. According to Zelenskyy, there are more than 300,000 fighters in his so-called cyberarmy.

An uncontrollable cyberarmy is being created. After developing skills under Member States' command in Ukraine while attacking Russia, it will not stop there. It is not a regular army. Experts know all too well how difficult it is to track down hacker activity, identify its source and suppress it. Hackers mobilized by Member States will spread around the world, posing a threat to citizens of Western countries, among other things.

The militarization of the digital space carried out by the West greatly increases the threat of a direct military clash, especially since the regime in Kyiv is actively mastering provocations in the information space according to Western techniques. However, their consequences could be even more horrendous. Computer attacks on critical infrastructure can lead to real and large-scale human casualties, not to mention the risk of misidentifying the perpetrator in the case of false-flag attacks, which are much easier to organize in virtual space than in real life. In such a case, the risks of unintentional escalation and the mutual exchange of cyberstrikes would increase manifold.

The Kyiv regime's reckless actions could lead to a full-scale confrontation in cyberspace that would involve other countries. NATO has already extended the right of collective self-defence under article 5 to information space. The responsibility for such an escalation will fall entirely on Western countries, which are encouraging the recklessness of the Kyiv leadership.

Faced with such a threat, we will certainly fight back against any attempts to undermine Russia's information security. But I once again urge Council members to think about the danger of dragging the world into a confrontation in cyberspace, which is no less dangerous than the use of weapons of mass destruction. We have been trying to prevent such a scenario for more than two decades.

Let me recall that Russia was the first to raise the issue of international information security at the United Nations back in 1998 and have it included in its agenda on a standing basis. We insisted that the United Nations set up negotiation platforms, first expert ones and then ones open to all Member States. At each of those stages, we had to overcome the strongest resistance from our Western colleagues, who claimed that they could manage without the United Nations. How they do without the United Nations is well known to the world.

We are seeking an international commitment that all States should undertake not to use ICTs for military purposes. We demand the demilitarization of the information space. All these years, we have been proposing specific draft international instruments — a universal concept for ensuring international information security and, on behalf of the Shanghai Cooperation Organization, a draft code of responsible conduct in that area.

What about our Western colleagues? All these years, they have been openly building up their offensive cyberpotential and developing rules for its use. Suffice it to recall the cynical *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which regulates in detail how to so-called humanely conduct cyberwarfare.

Which one of us has therefore been preparing for cyberwarfare all these years — Russia, which called for a ban on the use of ICTs for political and military purposes and is ready to assume the corresponding obligations, or Western countries, which repeatedly rejected all those initiatives in order to keep a complete free hand in the information space?

The digital sphere must not be allowed to become an area of geopolitical confrontation. This is an

existential question for humankind. Now more than ever, there is a need for a responsible discourse aimed at the development of practical solutions. It is our duty to support it regardless of the political climate. We call for a depoliticized discussion on all aspects of ensuring international information security in a specialized forum under the auspices of the General Assembly — the Open-ended Working Group. We believe that our meeting today does not replace the activities of that Group in any way.

Mrs. Nusseibeh (United Arab Emirates): The United Arab Emirates would like to thank the United States for organizing this meeting on an issue of increasing importance that the Security Council should address together beyond specific conflicts and very much in its own right, in the view of the United Arab Emirates. We also thank Under-Secretary-General DiCarlo, Ms. Nyabola and Mr. Druet for their really insightful briefings today.

Digital technologies advance at a dizzying speed. Let us think back to 1989, when the World Wide Web was created. By the end of the next decade, Larry Page and Sergey Brin had invented Google. Little did we know at the time that that new idea, coming from a garage in California, was going to change our lives forever. Fast-forward a decade, Google was in everyone's smart phone, and it was an indispensable part of work and life, bringing about enormous progress and change.

Let us now imagine the same warp speed on the nefarious side of technology happening today, as we heard, under our watch. For example, ongoing advancements in digital technologies are multiplying the possibilities of what devices such as drones are able to do. In the near future, it will be possible that swarms of drones, utilized by terrorist groups, could carry out cross-border attacks, using facial technology and other features enabled by artificial intelligence, without the possibility of attribution to either a State or a non-State group. How will States, including those around this table, respond to such an attack in the future legally and in accordance with international humanitarian law.

To prevent that dystopian future, we need to take urgent action now in the United Nations, the Security Council and other forums. What is clear is that we should not expect meaningful answers to emerge from the political and ethical debates that have been raging for more than two decades and that have not caught up with the technologies that are now ubiquitous and that have the potential to be utilized in such destructive ways.

There is no doubt that digital technologies bring their fair share of risks and challenges, particularly as that force multiplier for terrorist groups. But, as we also heard, that is not the whole story.

Digital technologies can also be peace enablers, as we heard today. For example, natural disaster warning systems, relying on the latest technologies and data, allow us to predict extreme weather events, such as droughts, hurricanes and floods, and pre-position aid accordingly. Successive anticipatory action programmes in Somalia have helped communities to address devastating water shortages and droughts. Thanks to such technologies, the Office for the Coordination of Humanitarian Affairs and other partners have been able to mitigate the loss of livelihoods and the decline in food consumption, ensure access to water and keep children in school, where they belong. Proper information puts the international community in a better position to respond to climate security threats. It saves lives and helps prevent fragility from becoming a trigger of instability.

As we consider the dual nature of digital technologies, it is time for the Council to move beyond admiring the problem and to discuss specific ways in which the Council can leverage technological innovations to contribute to sustainable peace and security. Today the United Arab Emirates would like to address five specific issues.

First, as others have mentioned, terrorist and extremist groups such as Da'esh, Al-Qaida and many others must not be allowed to use the Internet to propagate their agendas and manipulate social media and its billions of users. Technology companies have increasingly invested in detection tools based on artificial intelligence and human moderation teams to remove such content from their platforms. However, it has been clear to Governments for a while that business as usual is not enough, because terrorists and extremists continue to radicalize and recruit online. This problem is by no means limited to developing countries. The perpetrators of a number of recent high-profile hate crimes against religious and ethnic minorities in much of Europe and the United States have been radicalized through these online platforms, as were countless Da'esh recruits around the world. So although we have seen progress in recent years

strengthening regulatory and legislative frameworks to protect users from terrorist and extremist content, we obviously need to fast-track these efforts, since the international normative framework is not catching up. This responsibility lies not only with the technology companies but also with Governments.

Secondly, we must address the pernicious effects of online disinformation and misinformation campaigns using social media platforms, including on peace operations and humanitarian activities. These should be safeguarded. We have seen instances where peacekeepers and humanitarian relief workers, who are already putting themselves in harm's way to protect civilians, become further imperilled by the spread of misinformation and disinformation against them. Effective responses to fighting disinformation are needed at multiple levels, including through the use of the private sector via rules and regulations, fact-checking, the labelling of information and media literacy campaigns. The suggestions made today by the briefers that the United Nations should scale up its capacity and ability in that regard should be welcomed.

Thirdly, we should leverage digital technologies to strengthen the protection of civilians against harm. For example, in the physical world, medical and certain humanitarian actors use the red cross or red crescent emblems to signal their specific protection under international humanitarian law. As those actors are facing new digital threats from attacks on their digital backbones, we should start considering whether there might be a digital emblem to clearly signal that medical and humanitarian actors must never be targeted, online or offline. That emblem should not only reinforce the idea not only that those networks need to be protected but also that there should be accountability for any violations and that international law applies here.

Fourthly, digital innovation is having an impact on the physical world, multiplying the possibilities of what devices such as drones can do. I mentioned this at the beginning of my remarks. Commercially available drones can now fly faster, travel further, carry larger payloads and leverage artificial intelligence and other tools to operate without manual control. And drones do not just operate in the air. On 3 March 2020, as I briefed the Council, the Houthi terrorist group used a remotely operated drone boat laden with explosives to attack an oil tanker off the coast of Yemen. Had it been successful, the attack would have had devastating effects — not only on the tanker and its crew, but on the environment, on global supply routes and on local communities along the Yemeni coast that depend on the sea for their livelihood. We are in a Hobbesian state of nature regarding the use of technology by super-empowered non-State actors. Inaction is not an option because when there is no regulation, we are only encouraging proliferation.

It is clear today by the evidence shown and other reports that terrorist groups and non-State actors increasingly have access to such technologies. We strongly condemn their use to conduct cross-border attacks, target civilians or civilian infrastructure, in violation of international law. But that threat will only grow more dangerous as technology advances, and it must be addressed in the United Nations. Governments should enhance coordination, support capacity-building measures and exchange good practices and guidance to counter that threat.

Finally, we have talked about the importance of digital technologies to protect humanitarian actors. Let us now talk about their role in scaling up humanitarian action. Digital innovations such as artificial intelligence, predictive analytics, digital cash transfers and blockchain technology can improve humanitarian operations. These emerging technologies not only help humanitarian actors anticipate and prepare for crises but also enable them to move more quickly and efficiently when such crises arise.

As we consider digital innovation, let us not forget the digital divide. An estimated 37 per cent of the world's population — almost 3 billion people — have never used the Internet. The divide remains wide, and it disproportionately impacts women and girls. Only 19 per cent of women in the least developed countries are using the Internet — 12 per cent less than men. Inequality in the physical world is clearly being replicated in the digital world. As we think of how innovation can help us amplify our impact, let us prioritize those who have yet to see the dividends of technological developments that are now commonplace in other parts of the world.

As an early champion of frontier technologies, the United Arab Emirates is leveraging their benefits domestically and abroad. That is why, four years ago, we championed the establishment of the Secretary-General's High-level Panel on Digital Cooperation, which reflected our belief that digital technologies can positively contribute to global peace and security.

We actively supported implementation efforts and are encouraged to see the idea of establishing a global digital compact in the Secretary-General's *Our Common Agenda (A/75/982)*. We all need to further champion this multilateral work.

The United Arab Emirates will continue to work with all gathered here and all stakeholders to ensure that the world benefits from digital technologies as a key enabler to bring about more resilient, equitable and inclusive societies.

Mr. De Oliveira Marques (Brazil): Brazil thanks the United States presidency for organizing today`s briefing on the impact of digital technologies in maintaining international peace and security. We also express our appreciation to Under-Secretary-General Rosemary DiCarlo, Ms. Nyabola and Mr. Druet for their insightful presentations.

The process of digital transformation brings great benefits and opportunities for humankind, including for building peace and understanding and for empowering underrepresented and vulnerable groups.

The coronavirus disease pandemic has shown society the great benefits of the use of digital technologies, which have proved to be efficient tools to keep daily life possible, with the restrictions imposed by the threat of the virus. Education, trading and banking systems, among many others, have been able to adapt existing technologies to the sudden new reality. The Council and the United Nations system depended on them to continue to hold meetings, and today we have even gotten used to the idea of listening to briefers who are not able to attend a meeting in person. Of course, those benefits have not been enjoyed equally everywhere, due to persistent inequalities in the access to information and communication technologies. Tackling that digital divide remains an important task of the international community.

As we are well aware, the same digital technologies that have revolutionized our lives by allowing the generation, storage, dissemination and access to vast amounts of information have often been misused by Governments and non-State actors. Today's discussion has touched upon some of those challenges, which are diverse in nature and therefore require different modalities of State responses.

The General Assembly has recognized that international law, in particular the Charter of the United Nations, is applicable to States' activities in cyberspace and is essential to maintaining peace and stability, respecting human rights and promoting an open, secure, peaceful and accessible digital environment. International human rights law and international humanitarian law must be respected online as well as offline. We also underline the importance of adhering to the voluntary, non-binding norms for the responsible behaviour of States in cyberspace endorsed by the General Assembly, including through protecting critical information infrastructure supporting essential services to the public.

To address the challenge of disinformation, Governments and societies must adopt broad strategies. Educational campaigns and open debates to raise awareness, as well as cooperation between public and private actors such as social media companies can help tackle the misuse of digital platforms for the purpose of incitement to violence and terrorism.

International cooperation regarding the use of digital technology has greatly improved our capacity to identify common threats, including from non-State actors such as terrorist groups. As technologies evolve, we can also use them more efficiently to improve the transparency and agility of the Security Council. We should encourage the use of new technologies to provide women, young people and civil society with greater access to peace processes and peacebuilding and peacekeeping initiatives.

United Nations peacekeeping operations should make use of existing digital technologies to their full potential in order to improve the implementation of their mandate. I would like to highlight the importance of new technologies for strategic communications in peacekeeping missions. Strategic communications act as enablers and have a multiplier effect across all mandated areas, notably in relation to the protection of civilians and the women and peace and security agendas. Furthermore, they are crucial in addressing misinformation and disinformation that might hinder mandate implementation and threaten the safety and security of peacekeepers.

Mr. Biang (Gabon) (*spoke in French*): I thank you, Madam President, for taking the initiative to convene this meeting, which gives us the opportunity to consider the impact of digital technologies on the maintenance of international peace and security. In recent times, the issue has become more and more prominent on the

international peace and security agenda. I would like to thank Under-Secretary-General Rosemary DiCarlo, as well as Ms. Nyabola and Mr. Druet, for their enlightening briefings.

The theme at the heart of our discussions today reminds us more than ever that technological progress has pushed back the limits of our physical world into the infinity of the digital and the cybernetic. That implies, on the one hand, an expansion of our possibilities at all levels, including in the maintenance of international peace and security, yet, on the other hand, a reconfiguration and recalibration of the threats to them.

Now more than ever, peacekeeping relies on a robust ecosystem of technology and innovation that not only strengthens conflict management and prevention tools but also promotes better situational awareness, improves mission support and facilitates an enhanced implementation of United Nations peacekeeping mandates, often in complex environments.

Technological progress also contributes to the reinforcement of the security of peacekeepers and civilian populations and allows for improved preventive actions, particularly in the humanitarian field. The use of unmanned aerial vehicles and point analysis systems are increasingly becoming the preferred means of observing and anticipating movements in hard-to-reach areas such as battlefields, in order to obtain reliable information for more timely and efficient responses.

It is clear that the world is at a tipping point towards the robotization and digitization of our societies, our governance — both national and global — and, in particular, our rights and obligations. Unfortunately, that technological mutation is not exclusively advantageous. It is accompanied by consequences and sources of concern, like any science that is not draped in a mantle of consciousness.

Often considered as a force multiplier, technological progress also reveals itself as a factor of exacerbation in situations of conflict. Indeed, hate speech, radicalization, incitement to discrimination and violence in all their forms, disseminated via the Internet and social networks and of which women and youth are the primary vulnerable targets, have today become preferred vehicles of terror, fear and the perpetuation of crises.

The manufacturing of more powerful and more sophisticated weapons, refined by technological progress, brings with it an amplified capacity for nuisance and dehumanization, which must be subjected to a strict legal and ethical framework at the risk of being a real danger to humankind. The sad spectacle of armed and terrorist groups that freely acquire increasingly sophisticated weapons and new technologies to strengthen their power of destabilization in several regions in Africa recalls the need for peacekeepers, as well as the regular forces of the countries concerned, to also have access to the latest technologies.

The viability of those States in the grip of such negative forces and the survival of the populations concerned, caught in a terrible vice between the impotence of States with decadent authority and the torments inflicted by armed groups with an agenda of terror and chaos, are at stake. It is crucial that peacekeeping forces have access to technological equipment that is commensurate with the scale of emerging threats and adapted to the challenges that must be met, particularly in asymmetric armed conflicts against terrorist groups.

We share the conviction that it is necessary to encourage technological innovation and progress in the field; to maximize the potential of existing and new technologies to improve the ability of our peacekeeping missions to effectively carry out their mandates; enable peace operations to detect, analyse and address threats to civilians, peacekeepers and humanitarian and political missions in a timely and integrated manner; and, finally, ensure a more responsible use of digital technologies by peace operations while respecting human rights wherever they are at risk.

My country supports the Strategy for the Digital Transformation of United Nations Peacekeeping, as well as the United Nations Strategy and Plan of Action on Hate Speech.

Gabon remains firmly committed to the peaceful and responsible use of technology for the maintenance of international peace and security and calls for the strengthening of triangular cooperation, which is essential, inter alia, for the implementation of resolution 2518 (2020), on the safety and security of peacekeepers.

In conclusion, I would like to stress the importance of mobilizing at the international, regional and national levels to achieve optimal governance of the digital space and technological progress and to make it a

genuine catalyst for the mandates of United Nations peace missions and major instruments for international peace and security.

Ms. Juul (Norway): I would like to thank the briefers for their very interesting statements. I also thank the United States for facilitating this important discussion within the Security Council.

Over the past year the Council has engaged, in different formats, in discussions on technology and security, from the Arria Formula meeting on emerging technology and security held in May 2021 by the Permanent Mission of China to the open debate in June, when Estonia put cybersecurity on the Council's agenda for the first time (see S/2021/621). This is a timely continuation of those discussions.

Emerging and evolving digital technologies present great opportunities in a number of areas. Indeed, without digital technology, the Security Council itself would not have been able to function during the initial stages of the coronavirus disease pandemic. At the same time, digital technologies may also raise concerns and challenges. When used for malicious purposes, there is no doubt that they can pose a threat to international peace and security. Today's discussion is therefore at the core of the mandate and the responsibility of the Council.

Digital technologies are brought about and used not only by States. That underlines the importance of cooperation between States and other stakeholders. We need to cooperate with all those that develop and use technologies, including with academia and non-governmental organizations. Only by working together can we make sure that new technologies help us move forward in a direction that benefits us all. The United Nations forms an important global platform for such interaction.

The misuse of digital technologies can affect peace and security globally, for example, through Internet shutdowns or the massive spread of disinformation. Norway is concerned that the evolving misuse of the digital domain can bring about consequences that may escalate tensions, including human rights violations and abuses. Wilful restrictions on access to the Internet, in full or in part, represent but one type of misuse. The spread of targeted disinformation through digital technologies represents another — one that often limits people's access to reliable information at times when it is needed the most.

Nevertheless, we should not underestimate the positive effects of digital technologies. They can help promote inclusion in decision-making processes by allowing access for groups that have traditionally been excluded, such as women and minority groups, including through the use of video-teleconference in the Security Council itself to facilitate the participation of more and diverse civil society briefers.

Disinformation also remains a challenge in many areas, including posing a risk to our own United Nations peacekeeping missions, for example, when false information is spread to create a more hostile environment among the communities that the peacekeepers are deployed to help. Yet the best defence against disinformation is a free, independent and professional media sector. It is essential that the media are free to convey important information, ask critical questions and report on human rights violations and abuses. Supporting independent and pluralistic media and ensuring the safety of journalists can therefore also help reduce tensions and prevent conflict.

I thank you once again, Madam President, for placing this issue on our agenda. I look forward to this being a continuing discussion on how we can prevent and counter disinformation and other challenges resulting from the misuse of digital technologies, without losing sight of the immense benefits that such technologies offer to the maintenance of international peace and security.

Mr. Roscoe (United Kingdom): I thank you, Madam President, for this discussion today. We are also very grateful to the briefers for their contributions, as they illustrated that technology is changing how we monitor, understand and respond to conflict and humanitarian crises around the world.

It is clear that, first, technology can play a role in actually preventing the outbreak of conflict. If we can see risks in advance, then we can and should act before a crisis hits. Timelier decision-making enables early and preventive action, which is an area that I believe the Security Council should explore more, in conjunction with the Secretariat. It is also why we are working with others and industry to develop artificial-intelligence-driven conflict-prevention models.

Secondly, during conflict itself, accurate situational awareness for United Nations peacekeepers on missions is essential. Combining digital technologies,

such as remote monitoring with improved intelligence, surveillance and reconnaissance processes, can enable peacekeeping and monitoring missions to improve their understanding of threats and vulnerabilities on the ground. If we can get those drones described by our colleague from the United Arab Emirates to help peacekeepers instead of attack people, we can make progress.

Thirdly, technology also enables greater accountability. As we heard today, including from our brilliant briefers, social media enables greater accountability; it empowers people to tell the world about the conflicts, as they experience them, and ensures that the world knows what is happening on their terms. That means that the truth, including evidence of mass atrocities or violations of international humanitarian law, cannot be hidden by those who wish to hide them.

As we also heard today, technology is being used by States and other actors to suppress human rights and spread disinformation and as a tool in conflict. We see some States attempt to hide the truth by blocking access to social media or independent media sites. As others have noted, we saw that last year when the military junta shut down the Internet in Myanmar. We also see authoritarian regimes using surveillance technology to monitor and persecute their own citizens, denying them their human rights. Technology can also be used by those seeking to destabilize, and that is particularly true in the context of Russia's invasion of Ukraine, where Russia has conducted cyberattacks and, as we have reported, used an online troll factory to spread disinformation and manipulate public opinion about its illegal war.

Fortunately, technology can also help us combat disinformation. Russia tried once again today to claim that the bodies of victims lying in the streets of Bucha were a "staged provocation" by Ukraine. They suggested that the Ukrainian forces had undertaken that staged provocation after they retook the town. But satellite imagery proved that the bodies in the streets of Bucha had been there for several weeks, making it clear that they were killed during the period when Russian forces occupied the town.

Today, rather than talk of a staged provocation, we were spun some new nonsense about obsolete artillery. That is another Russian tactic to attempt to distract and confuse us and obfuscate. Layers of contradictory and competing lies are pushed out so that people are confused and do not know what to believe. But no one should be fooled by this. We look forward to the International Criminal Court undertaking a full investigation so that we can know the truth about what happened in Bucha, based on real evidence. Hopefully, indictments will flow from that.

Combating misinformation and defending media that are committed to reporting the truth online are critical to the proper functioning of the international system. Therefore, when the Russian delegation bemoans the fact that it is sanctioned on social media or that its State propaganda outlets are blocked, it should not be doing so. In the digital space, as in all spaces, we must strive to protect the truth from this new doublespeak.

In conclusion, we need to work together, including with civil society organizations, the private sector and other communities, to realize the benefits of, as well as counter the risks associated with, digital technologies. That will involve adapting institutions and upholding norms that are rooted in high standards, human rights and democratic values. The Council must ensure that existing frameworks and international law remain our guiding principles, as we do that. And if we succeed in doing that, we can ensure that digital technologies are a force for good and a transformative opportunity for sustaining peace and development.

Mr. Flynn (Ireland): I thank our briefers.

As we have heard today, technology is a positive force for good in our lives but can also be a powerful weapon for fomenting violence and conflict. Cyberattacks, cybercrime and the abuse of technology to spread disinformation are severely damaging trust, while advances in modern technology are contributing to the changing nature of conflict. Hate speech can be spread and amplified within minutes, thereby polarizing communities, undermining democracy and fuelling intolerance and violence across the globe.

There are countless examples of such risks. Russian State-controlled media has cultivated disinformation narratives in an attempt to create a pretext for its illegal unjustified war in Ukraine. As the war continues, so do the Russian Federation's efforts to distort reality and deny its brutal aggression on the ground.

In Myanmar, as we have heard from others, the curtailment of Internet access prior to the coup signalled the subsequent erosion of fundamental freedoms, repression, surveillance and brutal violence. In Ethiopia, we have seen the misuse of technologies to

oppress human rights defenders, conduct surveillance on activists, spread hate speech and incite tensions through social media. In many other cases, new technologies are being misused to threaten the security and integrity of States, target critical infrastructure, interfere in democratic processes and curtail human rights.

While the proliferation of digital technologies presents new risks and challenges, it also has the potential to play a vital role in support of peace. From Colombia to Libya, we have seen how digital technologies have supported greater inclusivity, promoted engagement in peace processes and complemented face-to-face interactions. They can and should facilitate and broaden the participation of women, youth and minorities. Ireland welcomes the work of the Mediation Support Unit and Innovation Cell of the Department of Political and Peacebuilding Affairs in that regard. However, those efforts must take note of the particular risks faced by those groups in online spaces, as well as the global gender digital divide.

We encourage all around the table to be more open to the positive role that technology can play in conflict prevention and in addressing global challenges such as climate change. Capacity-building, confidence-building measures and initiatives, including the programme of action for advancing responsible State behaviour in cyberspace, which Ireland was proud to co-sponsor, are central to such efforts.

Technology can also act as a force multiplier in peacekeeping missions, offering our peacekeepers greater situational awareness and improved data analysis capabilities. Those critically important enablers improve safety, security and operational efficiency, thereby enhancing mandate implementation. That is why implementing the Strategy for the Digital Transformation of United Nations Peacekeeping is so important.

It is precisely during times of armed conflict that we must vigorously defend the right to freedom of expression, online as well as offline, and access to information — freedoms essential to the promotion of lasting peace, understanding the nature of conflict and ensuring accountability. Today I pay tribute to the private citizens, journalists and human rights defenders in Ukraine who are using digital technologies to share harrowing stories from the front lines, often at great personal risk. They are working tirelessly to collect, verify and preserve digital evidence of the attacks, in the hope that it will be used to hold those responsible to account.

It is beyond question that international law, including international humanitarian law and international human rights law, applies in cyberspace. Our approaches to digital technologies must be grounded in human rights, the rule of law and democratic values.

Ireland supports a free, safe, secure, inclusive and accessible cyberspace. We know that digital technologies do not exist in a vacuum. It is clear that non-State actors play a leading role in driving technological innovation. The active and meaningful participation of civil society, including human rights defenders, women's groups, technical experts, academia and the private sector in our work to identify solutions to shared challenges is critical. Ireland also strongly encourages the Peacebuilding Commission to consider the impact of digital technologies, both positive and negative, in its discussions and advice.

In conclusion, investing in the potential of digital technologies is investing in peace. When it comes to the use of digital technology, Ireland firmly believes that multilateralism, responsible State behaviour, transparency and human accountability are key to building and maintaining the trust that underpins international peace and security.

The President: I shall now make a further statement in my capacity as the representative of the United States.

Let me start by thanking all of my colleagues today for engaging in a very constructive dialogue about the role that digital technologies play in advancing international peace and security. Unfortunately, Russia chose to be unconstructive by launching into baseless attacks to intentionally spread the exact kind of disinformation we are here today, in part, to talk about preventing and addressing.

I will not go down the rabbit hole of Russia's conspiracy theories. Instead, we will work together in future with other members of the Council to continue these important conversations in the weeks and months ahead. I would again like to thank the briefers for their contributions today. I would also like to thank all of my colleagues.

I now resume my functions as President of the Council.

The meeting rose at 12.35 p.m.