United Nations

A/C.1/78/PV.20

General Assembly

Seventy-eighth session

Official Records

First Committee

20th meeting

Tuesday, 24 October 2023, 10 a.m.

New York

Chair: Mr. Paulauskas . . . . (Lithuania)

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

Thematic discussion on specific subjects and introduction and consideration of all draft resolutions and decisions submitted under all disarmament and international security agenda items

The Chair: The Committee will now continue its thematic discussion under the cluster “Conventional weapons”. Before I open the floor, I would like to remind all delegations to respect the time limit for statements during this thematic segment.

I give the floor to the observer of the Holy See.

Archbishop Caccia (Holy See): At the outset, my delegation recalls that all States parties to the Treaty on the Non-Proliferation of Nuclear Weapons share the obligation “to pursue negotiations in good faith ... on a treaty on general and complete disarmament”. Reaffirming that objective has become even more imperative amid the rapid global proliferation of armaments.

Most concerningly, the war in Ukraine has featured the widespread use of indiscriminate weaponry, namely, anti-personnel mines and cluster munitions. The Holy See calls for the immediate cessation of the use of such weapons, which endanger civilians, especially children, and contaminate our common home. As Pope Francis has stressed, concern for the moral implications of nuclear warfare must not be allowed to overshadow the increasingly urgent ethical problems raised by the use in contemporary warfare of so-called conventional weapons, which should be used for defensive purposes only and not directed at civilian targets. Indeed, the trail of devastation left by conventional weapons necessitates renewed action to limit their further spread, increase transparency on existing stockpiles and ensure that any use complies with international humanitarian law.

In undertaking such goals, the international community must always place the inherent dignity of the human person at the centre. In that regard, the Holy See renews its support for the United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All its Aspects, in which States expressed their determination to “enhance respect for life”, and looks forward to further progress on the programme for the fourth United Nations Conference to Review Progress Made in the Implementation of the Programme of Action next year. Similarly, my delegation supports the Secretary-General’s call for negotiations to conclude by 2026 a legally binding instrument to prohibit lethal autonomous weapons systems that function without human control or oversight. In the interim, the Holy See urges all States to refrain from developing such weapons, which can never be morally responsible subjects and violate the dictates of public conscience.

As armed conflict increasingly takes place in densely populated towns and cities, the use of explosive weaponry often proves indiscriminate, with unacceptable casualties among non-combatants and the destruction of infrastructure crucial to the survival of civilian populations. In response, the Holy See appreciates the adoption, in Dublin last November, of the Political Declaration on the Humanitarian

This record contains the text of speeches delivered in English and of the translation of speeches delivered in other languages. 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 AB-0928 (verbatimrecords@un.org). Corrected records will be reissued electronically on the Official Document System of the United Nations (http://documents.un.org).

Accessible document Please recycle

Consequences of the Use of Explosive Weapons in Populated Areas. The Holy See thanks the Government of Ireland for its leadership in that endeavour and hopes that the Declaration will shift military operations from a paradigm of collateral damage to one of intended protection, thereby minimizing the loss of life.

In conclusion, allow me to echo Pope Francis's message to the Security Council in June:

> "[F]rom an economic point of view war is often more enticing than peace, inasmuch as it promotes profit. But that is always for a few and at the expense of the well-being of entire populations. The money earned from arms sales is therefore soiled with innocent blood. It takes more courage to renounce easy profits for the sake of keeping peace than to sell ever more sophisticated and powerful weapons. It takes more courage to seek peace than to wage war (*S/PV.9346, p. 6*)".

The Chair: The Committee has heard the last speaker in its thematic discussion under the cluster "Conventional weapons".

The Committee will now begin its thematic discussion under the cluster "Other disarmament measures and international security".

Mr. Sirie (Indonesia): I am pleased to speak on behalf of the Movement of Non-Aligned Countries (NAM).

NAM notes the positive benefits of information and communications technologies (ICTs) and their contribution to development, and encourages States to implement norms, rules and principles for the responsible behaviour of States while advancing discussion on implementation mechanisms, as that will contribute to increasing stability and security in cyberspace.

On the other hand, NAM strongly rejects the cases of malicious use of new ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security. NAM calls for the intensification of efforts towards safeguarding cyberspace from becoming an arena of conflict and ensuring instead exclusive peaceful uses that would enable the full realization of the potential of ICTs to contribute to social and economic development.

NAM takes note the conclusions of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security in its 2013, 2015 and 2021 reports that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

NAM recalls that the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025, established pursuant to resolution 75/240, was the first inclusive mechanism established within the United Nations with the participation of all Member States acting on the basis of consensus.

NAM reiterates its determination for the success of the OEWG on Security of and in the Use of Information and Communications Technologies 2021—2025, established pursuant to resolution 75/240, which is currently the only inclusive mechanism taking into account the concerns and interests of all States, based on consensus and pursued within the United Nations with the active and equal participation of all States. NAM further notes the process of adoption of the OEWG's second annual progress report by consensus (see A/78/265).

NAM stresses that the development of any international legal framework to address issues related to the use of ICTs with implications for international peace and security should take into account the concerns and interests of all States and be based on consensus and pursued within the United Nations with the active and equal participation of all States. In that regard, NAM supports a single-track, State-led permanent mechanism under the United Nations, reporting to the First Committee. NAM supports the development of an open, inclusive, transparent, sustainable and flexible process that would be able to evolve in accordance with the needs of developing countries and in accordance with developments in the ICT environment. NAM further underscores that such a legal framework, together with a multilateral, inclusive institutional platform dedicated to international cooperation on safeguarding the peaceful uses of ICTs, would represent a major contribution towards increasing stability and security in cyberspace through the prevention of conflicts, thereby promoting the settlement of international disputes by peaceful means and the peaceful uses of ICTs. At the same time, NAM stresses as a principled position that nothing in that legal framework should affect the inalienable rights of States in the development and use of ICTs for peaceful purposes.

NAM rejects any unilateral measures not in accordance with the United Nations Charter and international law that impede the full achievement of economic and social development by the populations of affected countries and that hinder their well-being. NAM condemns the misuse of ICTs, including the Internet and social media, to incite and commit acts of terror. NAM underscores the importance of the capacity-building of Member States and confidence-building measures aimed at enhancing the stability and security of cyberspace.

NAM also emphasizes the importance of the observance of environmental norms in the preparation and implementation of disarmament and arms limitation agreements. Furthermore, NAM reaffirms that international disarmament forums should take fully into account the relevant environmental norms in negotiating treaties and agreements on disarmament and arms limitation.

NAM welcomes the adoption without a vote of resolution 77/45, on the relationship between disarmament and development. NAM further stresses the importance of the reduction of military expenditures, in accordance with the principles of undiminished security at the lowest level of armaments, and urges all States to devote resources made available therefrom to address new challenges to the international community in the fields of development, poverty eradication and the elimination of diseases that afflict humankind.

Under this cluster, NAM is presenting the following three draft resolutions and will welcome support of all States: “Observance of environmental norms in the drafting and implementation of agreements on disarmament and arms control” (A/C.1/78/L.6), “Promotion of multilateralism in the area of disarmament and non-proliferation” (A/C.1/78/L.7) and “Relationship between disarmament and development” (A/C.1/78/L.4).

Mr. Chindawongse (Thailand): I have the honour to deliver this statement on behalf of the Association of Southeast Asian Nations (ASEAN).

ASEAN aligns itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries.

ASEAN reaffirms its commitment to building an open, safe, secure, stable, accessible, interoperable, peaceful and resilient cyberspace that serves as an enabler of economic progress, enhanced regional connectivity and the improvement of living standards for all. At the same time, ASEAN recognizes the pervasiveness of cyberthreats that are ever evolving and transboundary in nature. Amidst widespread economic digitization and the proliferation of Internet-connected devices across ASEAN, we have become increasingly vulnerable to malicious activities in cyberspace that have the potential to undermine peace and security. In that regard, ASEAN believes that States need to work together to effectively respond to cyberthreats, minimize the risk of misperception and miscalculation by building trust and confidence, and harness the benefits of technology while recognizing that cybersecurity is a cross-cutting issue that requires the coordinated expertise of multiple stakeholders across different domains.

ASEAN emphasizes the United Nations central role in discussions on cybersecurity. In that regard, ASEAN reaffirms its support for the work of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 as a confidence-building measure and a forum for building and rebuilding consensus on that important issue. ASEAN therefore welcomes the consensus adoption of the second annual progress report of the OEWG at its fifth substantive session in July 2023 (see A/78/265). ASEAN is proud that ASEAN’s initiatives — in particular the ASEAN Regional Forum Points of Contact Directory on Security of and in the Use of Information and Communications Technologies and the matrix for the ASEAN Regional Plan of Action on the Implementation of Norms of Responsible States Behaviour in Cyberspace — have meaningfully contributed to international cyberdiscussions at the United Nations. We look forward to the establishment and operationalization of a global intergovernmental points of contact directory, as well as elaborating additional guidance, including a checklist on the implementation of norms, as outlined in the annual progress report.

ASEAN advocates that the OEWG remain the central platform for discussions on cybersecurity at the United Nations until the end of its mandate, and looks forward to further progress, including by building on the hard-won consensus that we have reached in the previous two annual progress reports. ASEAN appeals to Member States on the importance of preserving and maintaining consensus on the important matter of cybersecurity. We should also avoid creating parallel mechanisms and/or overlapping processes that would only further restrain the finite resources of the United Nations and its Member States. In that regard, ASEAN firmly believes that it is important to have a single-track process that will build on the consensus recommendations of the OEWG on regular institutional dialogue. ASEAN remains fully committed to engaging constructively with all partners towards that end.

Within ASEAN, cooperation on cybersecurity cuts across pillars and sectors guided by the ASEAN Digital Masterplan 2025 and the ASEAN Cybersecurity Cooperation Strategy 2021-2025, which were adopted by the ASEAN Digital Ministers in January 2022. ASEAN member States have made efforts to implement enhanced cybersecurity measures consistent with the 2021-2025 Strategy in view of the recent rise of global cybersecurity attacks and threats and in response to newer cyberdevelopments. At the same time, ASEAN is currently working on implementing the Asian Regional Action Plan on the implementation of the United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security, which was developed to ASEAN member States to identify areas that need further support to implement the norms, including capacity-building and international cooperation.

To strengthen ASEAN’s cybersecurity incident response capabilities, ASEAN has agreed to establish the ASEAN Regional Computer Emergency Response Team to facilitate the timely exchange of threat and attack-related information among ASEAN member States’ national computer emergency response teams.

As cybersecurity is a cross-cutting issue, the ASEAN Cybersecurity Coordinating Committee was established to strengthen regional collaboration and coordination in cybersecurity. The Committee comprises representatives from relevant sectoral bodies to strengthen cross-sectoral coordination on cybersecurity while respecting the work domains of the sectoral bodies.

ASEAN stresses the importance of international cooperation and capacity-building in the field of ICTs to enable States, especially developing countries, to effectively address cyberthreats and implement the 11 voluntary non-binding norms of responsible State behaviour in the use of ICTs. To that end, ASEAN initiated the implementation of the ASEAN Cyber Shield project from 2023 to 2026 to complement existing ASEAN capacity-building efforts, including the ASEAN-Singapore Cybersecurity Centre of Excellence in Singapore and the ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand, in supporting the common goal of enhancing the region’s capacities. ASEAN looks forward to working in tandem with the United Nations in that regard, especially through the ASEAN-United Nations Comprehensive Partnership.

Furthermore, ASEAN works with international partners to enhance international cooperation in the field of ICT security through platforms such as the ASEAN Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies. ASEAN also welcomes the progress made by the opening of the Defence Ministers Meeting (ADMM) Cybersecurity and Information Centre of Excellence and the ASEAN Defence Ministers Meeting-Plus Experts’ Working Group (EWG) on Cybersecurity. Notable achievements in recent years include the establishment of the Points of Contact and Technical Personnel Directory, the development of the compiled Glossary of Cyber Terminologies, the conduct of a tabletop exercise and the setting-up of the ADMM-Plus EWG on Cybersecurity portal.

To conclude, ASEAN reaffirms its commitment to becoming future-ready to enable economic progress, improve our way of life and ensure peace and security for all. We look forward to contributing constructively, together with members of the international community and relevant stakeholders, in advancing our shared goals of having a peaceful, secure, interoperable and resilient cyberspace.

Mr. Shen Jian (China): I have the honour to deliver this joint statement on behalf of Belarus, Burundi. Cambodia, Cameroon, Cuba, Dominica, Equatorial Guinea, Eritrea, Ethiopia, Guinea-Bissau, the Gambia, Kazakhstan, Kyrgyzstan, the Lao Peoples Democratic Republic, Nicaragua, Pakistan, Russia, Somalia, Syria, Vanuatu. Venezuela, Zimbabwe and my own country, China.

On the occasion of the second anniversary of the adoption of resolution 76/234, entitled “Promoting international cooperation on peaceful uses in the context of international security”, we, the sponsors of the resolution, reiterate that it is the inalienable right of all States to participate in the fullest possible exchange of equipment, materials and scientific and technological information for peaceful purposes. Against the background of a new era, bearing in mind the potential impact of scientific and technological advances on global security, the significance of peaceful uses is becoming ever more prominent in facilitating the economic and social development of Member States, in particular developing countries. We call on the international community to take concrete measures to ensure that the resolution is effectively implemented.

We welcome the political commitment and concrete efforts of Member States in promoting international cooperation on peaceful uses, as well as the progress made within multilateral frameworks and through bilateral channels. At the same time, undue restrictions on exports to developing countries of materials, equipment and technology for peaceful purposes persist. We reaffirm the importance of promoting international cooperation for peaceful purposes and the need to further deliberate that important topic within the framework of the United Nations in an open and inclusive way and utilizing relevant existing international, regional and bilateral mechanisms and arrangements in accordance with the resolution. We call upon Member States to continue dialogues on promoting peaceful uses and relevant international cooperation, including by identifying gaps and challenges, as well as ideas and opportunities for strengthening cooperation and exploring possible ways forward.

We will submit a draft resolution entitled "Promoting international cooperation on peaceful uses in the context of international security" to the General Assembly at its seventy-ninth session in 2024. We welcome the active participation of all States in the follow-up process.

The Chair: I now give the floor to the representative of the European Union, in its capacity as observer.

Mr. Karczmarz (European Union): I have the honour to speak on behalf of the European Union (EU). The candidate countries North Macedonia, Montenegro, Serbia, Albania, Ukraine, the Republic of Moldova, Bosnia and Herzegovina; the potential candidate country Georgia; and the European Free Trade Association countries Iceland and Norway, members of the European Economic Area, as well as Monaco and San Marino, align themselves with this statement.

Over the past decade, the international community has made it clear that the international rules-based order also applies to States' behaviour in cyberspace. All members of the General Assembly have repeatedly affirmed the evolving framework of responsible State behaviour in cyberspace, built upon the recognition that international law applies in cyberspace, adherence to voluntary non-binding norms of State behaviour, capacity-building and the enhancement of practical confidence-building measures to reduce the risk of conflict. Broad international consensus around those four elements is the foremost accomplishment of cyberdiplomacy in the past decade.

Russia's illegal, unprovoked and unjustified war of aggression has seriously challenged the international rules-based order, including in the cyberdomain. Destructive cyberattacks against Ukraine, often in conjunction with missile attacks, are unprecedented, with a spillover effect on the EU countries as well. Ukraine has, in the past year, not only suffered from more data-wiping malware than any country ever before, but also successfully prevented many of them, thanks to its extraordinary cyberdefence and resilience.

The changed threat environment in Europe induced by Russia's aggression against Ukraine, as well as other growing and evolving threats from States and non-State actors, have affected the way we as the EU approach malicious cyberoperations. We have strengthened our commitment to further revising and constantly improving cyberresilience within the EU and to developing further strategies on how best to address cyberthreats coming from all malicious actors.

While recognizing that States bear the primary responsibility to ensure international peace and security, other stakeholders have an essential role to play. The Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025, established pursuant to resolution 75/240, is an opportunity for the international community to exchange openly, inclusively and transparently on the responsible use of information and communications technologies by States in a manner that is consistent with international law.

We welcome the consensus reached in 2023 on the annual progress report of the OEWG (see A/78/265), and stress the need for the international community to continue its path to further strengthen security and stability in cyberspace. While the annual progress report could have gone further, it does outline multiple decisions and next steps that can be considered as concrete and actionable ways forward to strengthen the United Nations framework for responsible State behaviour and international law.

Much more is still to be achieved, notably to support the practical implementation of the outcomes of those discussions. The EU and its member States look forward to continuing to work with States and other stakeholders to take forward those efforts, in particular through an inclusive dialogue on the elaboration of a United Nations programme of action, building on consensus outcomes from successive United Nations groups of governmental experts and open-ended working groups, as well as the work of the current OEWG and the report of the Secretary-General.

The broad support for resolution 77/37 at last year's session of the First Committee, with 157 votes in favour, co-sponsored by a cross-regional group of 74 countries, reaffirmed the commitment of States to implementing the agreed normative framework through a permanent, inclusive and action-oriented mechanism. It clearly demonstrates a common aspiration of the vast majority of States to promote peace, security and stability in cyberspace through a permanent and cooperative platform that advances the exchange of knowledge and best practices, avoids duplication of efforts and assists in national and regional implementation efforts. Over 40 States, from all regional groups, have shared written submissions and the Secretary-General has issued a report (A/76/77) that offers valuable substance and recommendations for further inclusive discussions on the programme of action.

As set out in last year's resolution 77/37, this proposal is aimed at providing States with flexibility to address issues that would benefit from political discussions, information exchange and practical implementation. It will be State-driven, and it will also seek to enhance multi-stakeholder engagement, providing for regular consultations with relevant stakeholders, including the private sector, academia and civil society, to consider and provide their unique perspectives. Many non-State stakeholders are already driving initiatives with the aim of building trust and confidence between States and non-State actors, and their inclusion will result in more impactful outcomes and contribute to transparency, credibility and sustainability in the implementation of the framework.

Most importantly, the establishment of a permanent platform would allow the international community to focus its discussions on substance and the enhancement of cooperation and trust among States rather than recurring debates on future processes. We should not miss this opportunity to take our work forward in a stable environment, and the European Union and its member States fully support the corresponding resolution presented to the General Assembly to that end. To maintain a single-track process at the United Nations, we need a permanent mechanism to be established after the conclusion of the current OEWG 2021-2025, and its scope, structure and content should be built upon the discussions within the OEWG in 2024 and 2025.

Given the escalating nature of international cybersecurity threats, it is more important than ever to deepen our cybercollaboration with international partners and promote a shared understanding of how international law applies and how to further implement the United Nations framework of responsible State behaviour. For that reason, the EU supports draft resolution A/C.1/78/L.60, introduced by France, to establish a mechanism under the auspices of the United Nations as a flexible venue where United Nations Member States can engage in practical discussions on how best to secure cyberspace for all. We can only ensure an open, stable and secure cyberspace effectively if we collaborate, improve coordination and complementarity, break silos and create new, innovative methods to address malicious cyberbehaviour. Doing that is at the core of the EU's ambition.

Mr. Lagardien (South Africa): South Africa aligns itself with the statement delivered on behalf of the Movement of Non-Aligned Countries.

South Africa welcomes the consensus adoption of the second annual progress report (see A/78/265) of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025. That process has been important in building mutual trust and promoting peaceful cooperation among States. With regard to the many threats faced by States, South Africa believes that cooperative measures are needed to address those threats against information and communications technology (ICT) infrastructure.

Our participation in the Open-ended Working Group (OEWG) has been in good faith to ensure that the dialogue among States takes place under the auspices of the United Nations, a universal, multilateral forum that promotes the peaceful settlement of disputes. South Africa considers that maintaining international peace and security in cyberspace is a collective responsibility. We believe that States should use the existing 11 rules, norms and principles of responsible States' behaviour in cyberspace in their current incarnation while we consider the possibility of a broader framework for cooperation.

The second annual progress report provides us with two overarching confidence-building measures: the continued work on establishing regular institutional dialogue and the points of contact directory. We also see the OEWG and its consensus outcomes as a trust and confidence-building measure in itself, and we commend the Chair of the OEWG, Ambassador Burhan Gafoor, and his team for their efforts to ensure that we achieve tangible outcomes and that the process remains action-oriented. Discussion on the different formats of exchange of views among States on potential and emerging threats have shown us that the international community can remain constructively engaged during difficult political times. In that vein, South Africa supports proposals to establish a threats repository and a global cybersecurity cooperation portal. We trust that future sessions of the OEWG can further develop those ideas.

We believe that while the intergovernmental process would benefit from briefings by relevant experts from regional and subregional organizations, business, non-governmental organizations and academia, with due consideration given to equitable geographical representation, we feel that the Chair of the OEWG has used his convening powers to invite various stakeholders to share their views on the implementation of ICT security. The OEWG has therefore been able to engage as many diverse views as possible on its work.

As a developing country, South Africa has benefited from the exchange of views among States on the OEWG and we support the Chair and his proposed timetable to facilitate the process of agreeing on the future of our discussions as an international community. South Africa believes that it is vital for us to guard existing processes such as those, which have proven successful in difficult times.

Mr. Alqaisi (Jordan) (*spoke in Arabic*): At the outset, I would like, on behalf of the Group of Arab States, to reiterate the need to put an end to the war and the brutal Israeli aggression against the Gaza Strip. The Arab Group condemns that aggression in the strongest terms. Safe and sustainable access to essential humanitarian and medical aid must be ensured, as must an end to the forced displacement of Palestinians.

Turning to our thematic discussion today, the Arab Group associates itself with the statement delivered on behalf of the Movement of Non-Aligned Countries.

As for the issue of other disarmament measures, the Arab Group stresses that the solutions agreed upon in the context of multilateralism pursuant to the Charter of the United Nations provide the one and only sustainable path to address disarmament issues and international security. The Group calls on all Member States to reiterate and implement their individual and collective commitments within the international multilateral context. The Group reiterates its belief in the pivotal role of the United Nations in disarmament and non-proliferation matters.

The Arab Group expresses its concern over the increased tensions and military expenditures worldwide, a large portion of which could be allocated to promoting sustainable development and eradicating poverty throughout the world, especially in developing countries, including the Arab countries. The Group reaffirms the importance of following up on the programme of work adopted at the 1987 International Conference on the Relationship between Disarmament and Development, as well as on the effects of increased military expenditures on the implementation of the Sustainable Development Goals, pursuant to the 2030 Agenda for Sustainable Development.

The continued possession and modernization of nuclear arsenals pose a serious threat to international peace and security and to sustainable development. The Arab Group therefore underlines the need for the international disarmament forums to take relevant standards into account when negotiating treaties and conventions on disarmament and arms control. All States must contribute to ensuring full adherence to environmental standards while implementing such treaties and conventions.

Turning to cybersecurity, the Arab Group expresses its concern over the increased use of information and communications technologies (ICTs) in destructive activities that breach international peace and security, including those committed by terrorist and criminal organizations. The Group underscores the need for the United Nations to continue to develop binding rules that govern the responsible behaviour of States in that vital domain, commensurate with its rapid development. There is also a need to continue international cooperation and maintain the central role of the United Nations in those efforts.

The Arab Group stresses the importance of further international cooperation to promote the security of ICT. That would enhance the capacities of States to counter any sabotage attacks. Many reports issued by various groups of governmental experts and open-ended working groups have stressed such attacks. The Arab Group is keen to ensure the central role of the United Nations in promoting international standards regarding the safety and security of ICT and to continue cooperation with the United Nations in that domain, which has an impact on all vital facilities of various States. It has been increasingly used in sabotage activities that threaten international security.

In conclusion, the Arab Group emphasizes its readiness to actively participate in the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025. The Group welcomes the adoption by consensus of the second annual progress report of the Open-ended Working Group (see A/78/265) and looks forward to holding focused discussions on the different relevant proposals to support the developing countries in countering the increasing threats resulting from the use of ICT.

Mr. Sirie (Indonesia): Indonesia aligns itself with the statements delivered on behalf of the Movement of Non-Aligned Countries and the Association of Southeast Asian Nations. In that regard, I wish to add a few points in our national capacity.

My first remark concerns the importance of strengthening cooperative measures in the field of information and communications technology (ICT) security. Technology is often described as a double-edged sword, serving as a valuable tool but also posing significant risks. Yet, as we become more interconnected, cyberattacks emerge as a prime threat to digital infrastructure, causing service disruptions, data theft and fraud. In that regard, Indonesia emphasizes the need for cooperative measures among all Member States to ensure a safe, secure and stable cyberspace.

Indonesia reaffirms its support for the work of the Open-ended Working Group (OEWG) on on Security of and in the Use of Information and Communications Technologies 2021-2025, including its focus on capacity-building and confidence-building. That will assist countries in enhancing their capabilities in cybersecurity. For its part, Indonesia recently launched our National Cybersecurity Strategy in July. That will further enable our newly established National Cyber Security Agency and add to the legal framework to safeguard computer users, critical national infrastructure and cyberspace through legislation, such as the Law on Data Privacy of 2022 and the Law on Information and Electronic Transactions of 2008. Indonesia looks forward to continuing the discussion on furthering capacity-building on cybersecurity capability within the OEWG.

My second point concerns strengthening multilateral frameworks and norms on the use of ICT. In the current international security landscape, consensus-driven cooperation seems to be diminishing. We shall not let that happen in the sphere of ICT security. Such a trend would empower malicious actors to disrupt cyberspace safety, threatening international peace and stability. Therefore, given the precarious context of our international environment, Indonesia applauds the effort made by Member States to adopt the second annual progress report (see A/78/265) by consensus. With its inclusive and step-by-step approach, the OEWG has been able to become a platform that facilitates cooperation, transparency and confidence-building measures on the issue of ICT security. Indonesia also welcomes and looks forward to the implementation of the points of contact directory as one of the concrete and tangible outcomes of the OEWG. Therefore, it is imperative that we maintain the sanctity of the OEWG as an inclusive framework for managing cyberrisks, fostering good governance and practices within the cyberspace domains.

As we are midway into the OEWG mandate, I wish to echo statements made by delegations on a proposed draft resolution concerning the future mechanism to deliberate ICT security. It is important that we remain consistent with the common elements of the future mechanism, as agreed by consensus in the second annual progress report. We have to avoid the submission of competing draft resolutions on the same subject matter, which would lead to fragmentation in the work of the First Committee as it would result in parallel processes that would undermine the work of the OWG. Instead, we shall continue using the OEWG to discuss sustained cooperation, sharing best practices and capacities among countries to effectively address cybersecurity challenges, narrow the digital divide and facilitate unimpeded economic and social progress.

Mr. Hegazy (Egypt): At the outset, let me express our strong condemnation of the continued targeting of Palestinians in Gaza. We reiterate our calls for an urgent and unconditional ceasefire, and on Israel to immediately end its attempts to forcibly displace more than a million civilians in southern Gaza. It must also allow the unhindered access of humanitarian assistance to alleviate the ongoing human suffering of the Palestinian people.

Egypt aligns itself with the statements delivered on behalf of Movement of Non-Aligned Countries and the Group of Arab States, and wishes to make the following remarks.

Egypt reiterates that non-discriminatory, multilateral, legally binding instruments are the most effective measures for achieving sustainable progress in the area in the area of disarmament and international security. The continued commitment of all States to previously agreed undertakings and international law is a necessary condition for maintaining international peace and security and avoiding chaos — taking into consideration the rapid scientific and technological developments in several strategic fields that are domains with a direct impact on international security and have been left without clear internationally agreed rules to prevent them from turning into scenes for an arms race and armed conflicts — and for ensuring the reliable continuation and contribution of the relevant technologies to the development and welfare.

Cyberspace, outer space and the organization of artificial intelligence applications, including the area of lethal autonomous weapons, are prominent examples. The lack of progress in addressing the several security threats that arise in such domains is clearly due not to the lack of technical expertise on the part of the international community but to the continued misguided belief of some States that absolute dominance in such domains can be maintained. Those States thereby resist any efforts towards the development of equitable legal multilateral regimes prohibiting the malicious uses and weaponization of such technologies, which will lead to an arms race that no one can win.

We welcome the successful conclusion of the second annual cycle of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 and the adoption of its second annual progress report (see A/78/265) and the elements paper on the operationalization of the global points of contact directory, as well as other forward-looking recommendations that could pave the way to focused discussions on the outstanding issues and proposals within the scope of the OEWG.

The OEWG was presented with many creative ideas and constructive proposals, including regular institutional dialogue under the auspices of the United Nations, such as a possible United Nations programme of action on the use of information and telecommunications technologies in the context of international security that Egypt, along with France, has co-initiated since 2020 and developed with the support of a cross-regional group of States with the aim of complementing the work of the OEWG upon the conclusion of its mandate after 2025.

In that context, Egypt has submitted its national position on the future process for regular institutional dialogue on the website of the OEWG. We share the viewpoint that any future process on that topic must contain a distinct pillar on implementing the agreed framework and providing capacity-building to developing countries in that regard. Such a mechanism should serve as a flexible, action-oriented, single-track, permanent and consensus-based mechanism under United Nations auspices, as stipulated in paragraph 55 of the consensual second annual progress report of the OEWG. It should identify the possible gaps in the existing framework through the implementation of consensual outcomes, bolster international cooperation and assistance, and further elaborate the existing framework of norms, rules and principles, in addition to binding obligations.

In that context, we welcome the increasing support for focusing on implementing the existing agreed framework and developing it further. Moreover, we believe that we should continue to support the current OEWG towards the successful conclusion of its work and devote our efforts to reaching common grounds for the establishment of the future mechanism, building upon the work of the OEWG. In that vein, we encourage all delegations to avoid pre-empting the ongoing negotiations or prematurely imposing the establishment of parallel tracks not only under cluster 5 but also across the board. That trend will only lead to further division and stalemates.

Ms. Gomez Sardinas (Cuba) (*spoke in Spanish*): We support the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries. We also endorse the statement delivered by the representative of China on international cooperation for peaceful uses in the context of international security.

We reiterate Cuba's commitment to general and complete disarmament, which will make it possible to achieve a world free from weapons of mass destruction for the benefit of present and future generations. We call for the adoption of other disarmament and international security measures that will help us build a world of peace as soon as possible. We must reduce the vast amounts of money spent on militarization. That money, and the scientific and technological progress that are now devoted to financing the military-industrial complex and the development, production and updating of increasingly sophisticated weapons, would offer myriad benefits to humankind if it were used towards the fulfilment of the 2030 Agenda for Sustainable Development and the Sustainable Development Goals.

We, the Member States, must continue to work to preserve multilateralism as the basic principle for negotiations in the area of disarmament and arms control. We recall that such negotiations must comply with binding international environmental norms. We support the negotiation of legally binding initiatives to prevent the militarization of outer space and cyberspace and to ban lethal autonomous weapons systems.

Mr. Lagardien (South Africa), Vice-Chair, took the Chair.

We support the ongoing work of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, which enables Member States to discuss issues transparently, inclusively and on an equal footing. As proof of our commitment to that forum, we endorse the adoption by consensus of its second annual progress report (see A/78/265), although we had higher hopes, in particular for progress in the development of additional norms for responsible State behaviour in the area of information and communications technology (ICT) security. We must neither prejudge the outcome of discussions on the future mechanism for regular institutional dialogue, nor promote the proposed programme of action to the detriment of other national initiatives.

Information and communications technologies should be used not to make war but for exclusively peaceful purposes. We reject the hostile use of ICTs, either openly or covertly, to subvert the juridical and political order of States or to commit or incite acts of terrorism. We oppose the use of force as a legitimate response to cyberattacks.

We reject non-conventional means of war that the Government of the United States continues to use against Cuba and the vast resources it devotes to that purpose. We condemn the use of new ICTs and other digital platforms to destabilize our country, spread fake news and promote regime change. We are opposed to the manipulation of the Cuban Internet, in violation of internationally agreed norms in that regard. We call on the United States to immediately end the ongoing financial and commercial blockade against Cuba, which significantly limits access to and use of ICTs for the benefit of the Cuban people.

We are convinced that general and complete disarmament, in particular nuclear disarmament, is necessary and possible. Cuba will continue to promote the adoption of effective measures that will allow us to achieve that noble goal.

Mr. Pieris (Sri Lanka): Sri Lanka associates itself with the statement made by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries. I make this statement in my national capacity.

The third decade of the twenty-first century is essentially characterized by rapid advancement and revolutions in information and communications technology (ICT). We are indeed at a momentous time in the digital age and in a world reaping the benefits of information and communications technology. Today, ICT is intrinsically interlinked with the daily lives of us humans as never before. The virtual space that we inhabit daily is a testimony to the vital role that ICT has come to play, from States down to individuals. Having spread into all spheres of human activities, ICT has become an enabler of all those domains.

In my country, a programme called DIGIECON Sri Lanka 2023-2030 was launched in May, highlighting the great synergy between ICT and economic progress in Sri Lanka with a firm resolve for Sri Lanka's transformation into a digitally inclusive country. Encompassing a digital master plan and regulatory policy framework, along with a series of annual events, the programme is aimed at accelerating Sri Lanka's economy towards an inclusive digital economy by leveraging advanced technology-based solutions.

While heralding those frontiers and in spite of all its positive features, as with other forms of transformational technologies, cyberspace has also become a haven for various actors to indulge in criminal and terrorist activities, as well as for those with vested interests to spread hatred, intolerance and incitement to violence, particularly on social media. Unprecedented levels of vulnerabilities in terms of cyberattacks and other malicious activities targeting ICT services, thereby disrupting millions of lives at the push of a few buttons, have been witnessed in recent times.

Sri Lanka therefore supports the multilateral deliberations in the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025. It is the only inclusive mechanism pursued within the United Nations with the active and equal participation of all States. We welcome the adoption of its second annual progress report (see A/78/265) and the establishment of the global intergovernmental points of contact directory, and look forward to future deliberations of the OEWG. We also follow with interest the ongoing discussions in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

We emphasize that the use of such technologies should be in accordance with the purposes and principles of the Charter of the United Nations, international law and, especially, the principles of sovereignty, sovereign equality, non-interference in internal affairs, refraining from the threat or use of force in international relations, the peaceful settlement of disputes, respect for human rights and adhering to the well-established principles of peaceful coexistence among States. Enacting legislation, therefore, and taking steps to prevent illegal and criminal activities targeting individuals, industry or Government agencies is the primary responsibility of the States concerned, yet many developing countries, including my own, are grappling with capacity restraints,

Humankind’s creativity is well known. Its ability to self-destruct through its own creativity and pursuit of short-term self-interest is also well known, be it the malicious use of existing technologies or the invention of new technologies, such as artificial intelligence or lethal autonomous weapons systems. We can ill afford misadventures that imperil our very existence.

Ms. Lipana (Philippines): The Philippines aligns itself with the statements made by the representatives of Thailand, on behalf of the Association of Southeast Asian Nations, and Indonesia, on behalf of the Movement of Non-Aligned Countries (NAM). Let me deliver the following points in my national capacity.

We strongly support the NAM draft resolution A/C.1/78/L.4, on the relationship between disarmament and development, emphasizing the importance of aligning disarmament with global development goals. The draft resolution calls for reduced military expenditures and the redirection of resources towards economic and social development, bridging the gap between developed and developing nations. It underscores the symbiotic relationship between disarmament and development and the role of security in achieving peace and prosperity.

The Philippines fully supports the NAM draft resolution A/C.1/78/L.6, on environmental norms and disarmament, emphasizing the crucial link between environmental protection and global security, fostering responsible disarmament with a focus on environmental preservation. The Philippines joins NAM in highlighting the importance of multilateralism in disarmament and non-proliferation efforts, emphasizing the power of transparent negotiations and cooperation among States to preserve global peace and security.

On the security of and the use of information and communications technology (ICT), the Philippines fully supports the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025. We emphasize the positive impact of ICTs on development and the need for responsible State behaviour to ensure stability and security in cyberspace. The Philippines deplores the malicious use of ICTs that violates international law, and calls for collective efforts to safeguard cyberspace and promote its peaceful use.

We endorse the second annual progress report of the OEWG (see A/78/265). The Working Group, operating on a consensus basis and involving all members, has succeeded in producing action-oriented outcomes to build trust and confidence among nations on cybersecurity matters. The Philippines fully supports its continued success as the current mechanism addressing the cybersecurity concerns and interests of all United Nations Member States. We support the establishment of a single-track, State-led permanent mechanism under the United Nations reporting to the First Committee. The mechanism should be open, inclusive, transparent, sustainable and flexible to adapt to the evolving needs of developing countries in the dynamic ICT environment. We hope that we can all harmonize our efforts to that end and in our current and future deliberations of cybersecurity matters.

As we have been hearing throughout the informal consultations, competing draft resolutions are not helpful. They are divisive. In that regard, in the spirit of bridge-building, we have been and remain committed to helping to find a middle ground, and the Philippines will continue to engage with the proponents and interested delegations to work on a future mechanism that could enjoy the widest support possible.

On lethal autonomous weapons, the Philippines fully supports draft resolution A/C.1/78/L.56 on that issue. We commend the international community for recognizing the urgent need to address the challenges posed by autonomous weapons system, which raise humanitarian, legal, security, technological and ethical concerns. As we navigate the rapid development of those technologies, it is crucial to uphold international law and maintain humankind’s highest standards. The draft resolution’s inclusivity, considering diverse perspectives, ensures a comprehensive approach to addressing that critical issue. Mandating the Secretariat to prepare a comprehensive report that would consider technological advancements and involve various stakeholders demonstrates the international community’s commitment to upholding international law and safeguarding peace and security. The Philippines believes that the draft resolution will catalyse collective multilateral efforts to address the challenges posed by lethal autonomous weapons systems. We look forward to continued discussions and progress on that matter in the framework of the Convention on Certain Conventional Weapons.

In conclusion, the Philippines stands firm in its commitment to forging a future of security, development and responsible technology use. We pledge unwavering support for the principles of disarmament and sustainable development, embracing the power of multilateralism. Furthermore, we emphasize the need to safeguard the digital realm, ensuring the peaceful use of ICTs and maintaining cyberspace security.

Finally, we champion the international effort to address the ethical and security challenges presented by lethal autonomous weapons. Together, we can navigate those complex issues, upholding international law and humankind’s highest standards.

Mr. Sivamohan (Malaysia): Malaysia associates itself with the statements delivered by the representatives of Indonesia, on behalf of the Movement of Non-Aligned Countries, and of Thailand, on behalf of the Association of Southeast Asian Nations.

The unprecedented reliance of global society on information and communications technologies (ICTs) necessitates sustained attention to security considerations, which transcend national borders, while the increased use of ICTs has provided new opportunities to advance shared objectives. The risks and challenges posed by the malicious use of ICTs must be effectively addressed. In that connection. Malaysia commends the continued efforts of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025. We welcome the July adoption of the OEWG’s second annual progress report (see A/78/265), which provides a solid basis for the Group’s work in the year ahead.

We are pleased that Member States have agreed on elements for the development and operationalization of a global intergovernmental points of contact directory. Malaysia also looks forward to the OEWG’s additional focused discussions on, inter alia, ICT threats to critical infrastructure and critical information infrastructure, the mainstreaming of agreed ICT capacity-building principles and the application of international law in the use of ICTs.

Malaysia remains committed to participating actively in the work of the OEWG, which has proven to be a valuable forum for discourse on ICT security issues among all Member States, with contributions from relevant stakeholders. The integrity, effectiveness and credibility of the OEWG must be upheld even as we explore prospective formats of regular institutional dialogue for the post-2025 period.

It is reassuring to note that, as reflected in the OEWG’s second annual progress report, Member States have agreed in principle on common elements on which a future mechanism for regular institutional dialogue would be based. Those elements include

> “a single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee” (A/78/265, *annex, paragraph. 55 (a)*).

Member States have also

> “recognized the importance of the principle of consensus regarding both the establishment of the future mechanism itself as well as the decision-making processes of the mechanism” (*ibid., paragraph. 56*).

In that connection, Malaysia reiterates that parallel multilateral tracks should be avoided in key areas of disarmament and international security. That is a matter of particular concern to smaller delegations from developing countries, given constraints in terms of financial and human resources.

Against a backdrop of renewed major Power tensions and the prevailing trust deficit, the OEWG has delivered tangible results incrementally and through consensus. That is testament to the good faith in which all delegations have engaged in the process. Notwithstanding divergent views on specific issues under its ambit, it is clear that the OEWG itself constitutes a vital confidence-building measure. As we consider various proposals on the way forward, let us continue to work constructively to ensure the full realization of the OEWG’s potential, in accordance with its mandate. It is my delegation’s fervent hope that the OEWG will remain, until the completion of its term, a single-track, open and inclusive platform able to respond flexibly to Member States’ requirements in the rapidly evolving domain of ICT security.

Mr. In Den Bosch (Kingdom of the Netherlands): In addition to the statement delivered on behalf of the European Union, I would like to make the following remarks in my national capacity.

Information and communications technologies (ICTs) are significant drivers of sustainable development and can positively impact human lives. But the risk of those technologies being misused by State and non-State actors grows in tandem with our reliance on them. Therefore, it is crucial that we not only uphold but also strengthen the rules and norms applicable to the use of ICTs by States. We must harness the potential of digital technologies for economic and social development while ensuring the safety and well-being of societies and individuals.

To address those challenges, States have developed a cumulative and evolving framework for responsible State behaviour in the use of ICTs in the context of international security. That is no small feat. The framework has been the product of extensive negotiations and efforts to build trust among States and therefore enjoys the endorsement of all United Nations Members. The 2023 annual progress report (see A/78/265) of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 adds another important layer to that framework by reaffirming the applicability of international law to cyberspace and by making concrete progress on the establishment of a points of contact directory. The report provides concrete recommendations on the implementation of the norms for responsible State behaviour, further anchors the need for a gender perspective in addressing ICT threats, and encourages gender-responsive capacity-building. In that vein, the Netherlands will continue to support the participation of women in the Open-ended Working Group through the Women in Cyber Fellowship.

We welcome the work as set out in the report, including the further deepening of common understandings of how specific principles of international law apply in cyberspace. We also continue to support the Open-ended Working Group’s work on capacity-building to advance the implementation of the consensus framework. With a view to cementing the steps taken in the OEWG’s annual progress report, the Netherlands hopes that Singapore’s draft position to endorse the report will be adopted without vote.

The Netherlands supports the programme of action initiative to establish a permanent, inclusive and action-oriented mechanism after the conclusion of the current Open-ended Working Group in 2025. The programme of action should advance works towards two objectives — first, to continue the progress and development of the normative framework for responsible State behaviour on the basis of consensus; and secondly, to foster international cooperation to advance the implementation of that evolving framework. Those two objectives were also referenced in the conclusion of the Secretary-General’s report on the programme of action (A/78/76), which welcomes action-oriented proposals that advance the implementation of the normative framework and support the capacities of States in that regard.

In its contribution to the Secretary-General’s report on the programme of action, the Netherlands proposed a needs-driven mechanism to facilitate capacity-building within the programme of action that makes use of existing initiatives inside and outside the United Nations system. The proposal is a work in progress, and we will continue to engage on it with other Member States.

As regards advancing the programme of action initiative, the Netherlands strongly supports draft resolution A/C.1/78/L.60, submitted by France. The draft resolution sets out a clear timeline and objectives for the establishment of a future mechanism for regular institutional dialogue in 2026. It gives impetus to develop the mechanism further in the current Open-ended Working Group and takes a balanced approach to a possible future need for additional legally binding obligations.

In conclusion, the Netherlands looks forward to continuing the work of the Open-ended Working Group and to making tangible progress towards a more open, free, secure, interoperable and peaceful cyberspace.

Mr. Fausto Gonzalez (Mexico) (*spoke in Spanish*): Mexico attaches particular importance to our approach to the responsible and peaceful use of outer space. In this digital era, where the majority of human activities are interconnected through cyberspace, we must recognize that irresponsible behaviour in that sphere can lead to cyberattacks, geopolitical tensions and even conflicts.

That is why Mexico reiterates the urgent need to make sure that cyberspace remains open, free, stable, safe, accessible and resilient for everyone. As we see it, the need to ensure international law, including international humanitarian law, in cyberspace is undeniable. We are firmly committed to the rigorous implementation of norms and principles establishing responsible State behaviour in that area. In that effort, we see the need to balance cybersecurity concerns with protecting human rights and promoting development through the use of information and communications technologies (ICTs).

For developing countries, regulating cyberspace is not merely a question of security, but rather a prerequisite for the sustainable use of cyberspace in its broader sense. It is a tool that, if properly used and regulated, has the power to promote innovation, guarantee fair access to information, strengthen our digital economy and close existing inequality gaps in our world.

A long-standing concern that we share with many other States is the possibility of a race for offensive capabilities in cyberspace. It is alarming to think that nations or even private entities can develop advanced offensive capabilities that could potentially lead to destabilizing actions. In that regard, Mexico calls for a collective commitment to preventing cyberspace from becoming a new battlefield for rivalries.

The Chair returned to the Chair.

With that in mind, we reiterate our trust in multilateralism. We believe that the United Nations, in particular the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, are the ideal forum for continuing to address together the challenges that cyberspace and ICTs represent in the context of international security. We underscore the significant progress made in discussions in the Group, particularly in the adoption of the two annual progress reports and the establishment and operationalization of the global points of contact directory, including other measures to promote cooperation and confidence in cyberspace. It is particularly important for the Working Group to continue to promote understanding and dialogue and to avoid duplication of efforts to the detriment of all countries,

I conclude with an appeal that we continue to hold productive and constructive discussions that will lead to a standing mechanism for discussions on cyberspace. The mechanism must be inclusive and allow the participation of all relevant actors, as well as international cooperation, and it must ensure capacity-building based on the various regional and subregional needs. Discussions on developing a standing institutional mechanism on cyberspace that would consider the building of capacities and include norms of international law, rules and principles for responsible State behaviour, as well as confidence-building measures, must continue to be among the priorities of the Working Group. Mexico hopes that at future substantive sessions of the Open-ended Working Group, we will be able to consolidate even more recommendations aimed at guaranteeing peaceful and fair cyberspace for everyone.

Ms. Lukabyo (Australia): We all benefit from an open, secure, stable, accessible and peaceful cyberspace. The value of a rules-based cyberspace has never been more evident. Only a rules-based cyberspace can provide the stability and independence necessary for all countries to determine their own digital future and economic development.

However, never before has cyberspace been more contested. This year continues to bear witness to unacceptable instances of malicious cyberactivity in our own Indo-Pacific region and elsewhere, such as Russia's targeting of Ukraine's energy infrastructure. Cyberissues have become strategic foreign policy issues of urgent concern to all countries. We all bear a responsibility to work together and with industry, civil society and the technical community to manage the complex international security challenges in cyberspace and to focus our efforts on promoting peace and avoiding conflict.

Australia remains firmly committed to working collectively to address those challenges, including through the United Nations. The United Nations has a strong history of fostering international cooperation to understand emerging threats and reduce risks to international peace and security.

We again reaffirm our commitment to acting in accordance with the United Nations framework for responsible State behaviour in cyberspace, developed and agreed through the consensus reports of United Nations groups of governmental experts and open-ended working groups. Australia will continue to publicly share how it implements, interprets and observes the framework. Transparency breeds accountability, predictability and stability, and we therefore encourage all States to meaningfully implement and faithfully observe their commitments under the framework.

Australia is pleased that the recent fifth session of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 saw a high level of participation of women representatives and stakeholder engagement. Australia welcomes the OEWG's annual progress report (see A/78/265) and its unequivocal reaffirmation of the framework. We encourage all States to meaningfully engage with the next steps recommended in the report, particularly recommendations that States continue to engage in focused discussions on how international law applies in cyberspace.

Australia places great importance on consensus outcomes on cyberissues at the United Nations, as those issues are simply too important to be split across multiple fronts. Australia has long been an advocate for the establishment of a permanent United Nations mechanism to advance responsible State behaviour in cyberspace — a mechanism that is inclusive, transparent, democratic and consensus-based.

We welcome France's initiative to lead draft resolution A/C.1/78/L.60, on the establishment of a programme of action to advance responsible State behaviour in the use of information and communications technologies, positioning us to meaningfully address emerging threats to international security. Australia stresses that any new permanent mechanism would not compete with what has come before it. The mode and structure of United Nations cyberdiscussions have developed considerably since the first Group of Governmental Experts in 2004, which consisted of 15 State experts behind closed doors, to the ad hoc creation in 2018 of the open-ended working groups, which are open to all 193 United Nations Member States. The programme of action represents the next evolution in United Nations cyberdiscussions, building upon what has come before, and guarantees that those issues will be accorded the attention and importance that they merit into the future.

We must also work together to ensure the responsible development, deployment and use of artificial intelligence (AI) in the military domain. The military application of AI generates both new opportunities and potential risks. Australia will continue to actively engage in that emerging international agenda, including at next year's Summit on Responsible Artificial Intelligence in the Military Domain, to be held in the Republic of Korea. We commend the United States leadership on the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Australia will continue to work diligently with all Member States to build consensus on cyber and AI issues, founded upon a commitment to international law and norms of responsible State behaviour.

Mr. Vidal Mercado (Chile) (*spoke in Spanish*): Chile endorses the statement made by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries.

We believe that the malicious use of information and communications technologies (ICTs) not only affect the development and well-being of States and their levels of digitalization, resilience and infrastructure, but also represent a threat to international security. Similarly, cyberattacks and malicious activities in cyberspace may have a greater impact on certain groups and entities, such as the elderly, vulnerable persons and women and girls. The international community must therefore continue to work to generate consensus that will guarantee that our cyberspace remains free, open, accessible, stable, safe and peaceful. Chile believes that international law, in particular the Charter of the United Nations, provides the applicable normative framework for regulating responsible State behaviour in cyberspace, including international humanitarian law, international human rights law and the implementation of the 11 United Nations voluntary and non-binding rules.

We recognize the progress achieved in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, particularly with respect to the creation and building of capacities and the development of confidence-building measures. In that regard, I underscore the establishment of a United Nations global points of contact directory. We also highlight the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. We must be able to improve our capacities and generate forums for cooperation and the exchange of information, thereby promoting work with all interested parties, such as the private sector, civil society, academia and the technical community, among others. We also highlight the importance of closer regional ties and work with regional organizations in implementing the framework of the Open-ended Working Group.

There is no doubt that disarmament, non-proliferation and arms control can have a positive impact on human well-being, equality and justice, and in particular on development throughout the world, in particular the least developed countries, the small island developing States and landlocked developing countries. The vast amounts of military spending clearly could be put to better use. We must promote greater representation of least developed countries in multilateral forums discussing disarmament and international security.

Lastly, we appeal to all members to support the three draft resolutions put forward by the Non-Aligned Movement on this and other clusters, and we would also highlight draft resolution A/C.1/78/L.19, on youth, disarmament and non-proliferation. We believe that we must promote awareness among our young people of those pressing issues so that our leaders and decision-makers of the future will be informed and educated on those very sensitive issues, helping us to live in peace and build a better world. We also thank civil society, educational institutions and non-governmental organizations seeking to disseminate information on disarmament and international security.

Mrs. Hanlumyuang (Thailand): Thailand associates itself with the statements delivered on behalf of the Movement of Non-Aligned Countries and the Association of Southeast Asian Nations (ASEAN).

Cybersecurity is one of the most important matters in today’s interconnected world. The misuse of information and communications technologies (ICTs) has increasingly become a serious threat to international peace and security, as well as to humankind. It is imperative that we strive to promote an open, safe, secure, stable, accessible, interoperable, peaceful and resilient cyberspace. To achieve that, Thailand wishes to reiterate four important points, as follows.

First, Thailand reaffirms the importance of a rules-based cyberspace to prevent malicious acts and conflict in cyberspace. We reaffirm our long-standing position that international law, in particular the Charter of the United Nations, is applicable in the context of ICTs. Complementary to international law, 11 voluntary non-binding norms for responsible State behaviour in cyberspace serve as a very solid foundation for promoting trust and confidence among States. It is essential that States continue to forge an understanding of how international law applies in the context of ICTs and to identify where gaps exist. States must work together to elaborate additional guidance, including a checklist on the implementation of the norms.

Secondly, regular institutional dialogues that are open, inclusive and transparent serve as a necessary platform for discussion of the aforementioned issues. The dialogues could also be a venue for sharing best practices and enhancing capacity-building efforts. The current Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 remains a crucial framework for such discussion. We thank Ambassador Burhan Gafoor of Singapore for his exceptional chairmanship, which led to the successful adoption of the second annual progress report (see A/78/265) by consensus. Thailand welcomes the proposal on the establishment of a future mechanism to promote regular institutional dialogue on that issue, including the programme of action. We support a mechanism that is single-track, State-led, permanent and under the auspices of the United Nations.

Thirdly, Thailand underscores the vital role of confidence-building measures (CBMs) in fostering trust among States in cyberspace at all levels. Thailand welcomes the concrete outcome of the OEWG in the development and operationalization of a global, intergovernmental points of contact directory, which could facilitate secure and direct communications among States to help prevent and address serious ICT incidents and de-escalate tensions in situations of crisis. It is equally important to strengthen CBMs through regional efforts. For ASEAN, CBM-related initiatives and mechanisms include the ASEAN Cybersecurity Cooperation Strategy 2021-2025, the ASEAN Cybersecurity Coordinating Committee and the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies.

Lastly, Thailand recognizes the need for capacity-building programmes to assist States in enhancing their cyberresilience, as well as in the implementation of norms and international law. We encourage States in a position to do so to continue to support such programmes, which must be sustainable, politically neutral, transparent and demand-driven. In that regard, we would like to thank Japan for continuously providing support to the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok since 2018.

In conclusion, Thailand is committed to actively engaging with all parties to work towards bridging divergent views to build a safer, secure and stable ICT environment.

Mr. Saadi (Iraq) (*spoke in Arabic*): At the outset, the delegation of Iraq would like to align itself with the statements delivered by the representatives of Jordan, on behalf of the Group of Arab States, and Indonesia, on behalf of the Movement of Non-Aligned Countries.

The delegation of Iraq joins the calls for the Israeli entity to end its brutal shelling of unarmed civilians in the Gaza Strip. We stress the need for a ceasefire and delivery of humanitarian assistance to end the humanitarian suffering of the people in the Strip and their systematic forced displacement,

The ongoing possession, upgrading and growth of military arsenals and the rise in international and regional tensions are being met with an intensified arms race and global military spending, which collectively pose grave threats to international and regional peace and security. That is why we all have to take urgent and genuine measures to reduce such threats and promote international and regional peace and security in order to achieve the Sustainable Development Goals by 2030.

The delegation of Iraq stresses that promoting the universality of disarmament conventions and treaties, including those on disarmament of weapons of mass destruction, especially nuclear weapons, is the only guarantee for the non-use or threat of use of such weapons and for preventing their disastrous repercussions. Those arms are lethal and destructive for both humans and the environment alike. The agreed solutions reached by the United Nations in the context of multilateralism are the only sustainable guarantee for addressing issues of disarmament and international security. Consequently, there is a need to reiterate and implement individual and collective commitments made at the international, multilateral level. It is also important for the United Nations to play its pivotal role in disarmament and non-proliferation,

The delegation of Iraq expresses its growing concern about the increase of international and regional tensions in the international security environment. That has led to an increase in the use of information and communications technology (ICT) in activities that threaten regional and international and peace and security. In that regard, Iraq welcomes the adoption of the second annual progress report (see A/78/265) of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, established pursuant to resolution 75/240 of 2020, and welcomes also the exceptional efforts made by the Chairman of the Working Group, Ambassador Burhan Gafoor. We stand ready to fully support him and make every effort to ensure the success of future sessions in order to adopt recommendations that support all States, especially developing ones, and help them to address the challenges and risks emanating from the use of ICT, in addition to the growing threats in that field. That will contribute to the establishment of a secure and safe cyberspace accessible to all.

Mr. Ahmed (Pakistan): We are on the verge of a monumental step in human technological history, heralded by the advent of artificial intelligence (AI). AI’s inevitable march from algorithms to armaments also continues without adequate guardrails governing its design, development and deployment. We also stand at the cusp of a new arms race, where algorithms will be in the driving seat. As AI heads to the battlefield, it is reasonable to ask whether and to what extent humans will continue to control it and hold the off switch.

Those new technology-enabled military means and capabilities, in the absence of human control, can heighten nuclear risks, increase the likelihood of miscalculations and accidents and evoke asymmetric responses, thereby lowering the threshold for the use of force and armed conflict. In times of crisis, a low threshold for the use of force would be highly destabilizing. Those new tools also have the potential to reshape conflict dynamics, alter deterrence strategies, intensify arms races, introduce unforeseen escalation patterns and raise new risks in an already complex international security landscape.

While some States highlight the benefits drawn from the use of AI in the battlefield, it is equally important to highlight the overwhelming risks and potentially catastrophic consequences. The window of opportunity to act and enact guardrails is rapidly diminishing as we prepare for a technological breakout. A failure to address those serious risks to peace and security would also oblige States faced with existing asymmetries to defend themselves with the capabilities at their disposal. It is encouraging to see the growing number of regional initiatives and multilateral endeavours to address apprehensions surrounding AI's military capabilities. We also appreciate the Secretary-General's call for AI governance.

The response from the multilateral machinery has been rather modest and insufficient. The deliberations in the Convention on Certain Conventional Weapons (CCW) have primarily centred around the application of international humanitarian law and aim to address only lethal autonomous weapons systems (LAWS). They deal with neither the broader rubric of the development of AI in all its military applications, including their integration into existing domains, nor their security and stability impacts at the global and regional levels.

In the First Committee, a new draft resolution (A/C.1/78/L.56) has been introduced on LAWS by a group of countries for the first time. We believe that discussions on LAWS should continue in the groups of governmental experts of the CCW with the aim of developing international rules through a new protocol. Concurrently, other disarmament bodies can and should play a complementary role to address the broader issue of AI in military applications in a way that builds positive synergies, while avoiding duplication.

The scale of challenges resulting from the use of AI for military purposes, including in weapons systems, necessitates a multifaceted and holistic multilateral response. Pakistan has accordingly presented a working paper this year in the Conference on Disarmament with proposals to include an agenda item to deliberate the security and stability implications of military AI.

The weaponization of information and communications technologies (ICTs) and cyberspace poses formidable threats to peace, security and stability on both the global and the regional stages. The unique differences between the physical and cyber spheres, the extent and scope of the applicability of existing international law and its interpretation require the expedited consideration, elaboration and development of commensurate norms and rules to govern the use of cyberspace. The ongoing deliberations in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security have the potential to develop common understandings that can form the basis for further normative efforts to prevent cyberspace from becoming another domain of conflict.

We are also pleased to be part of the joint statement delivered by the representative of China on promoting international cooperation on peaceful uses in the context of international security. The right of all States to the peaceful uses of science and technology in accordance with their international obligations should be guaranteed in a non-discriminatory manner without any undue restrictions. Efforts for the regulation of dual-use material and technology should be pursued within the United Nations framework and in inclusive multilateral settings.

Mr. Moriko (Côte d'Ivoire) (*spoke in French*): My delegation aligns itself with the statement made by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries, and will make the following observations in its national capacity,

Although relatively recent, security threats linked to digital technologies are nevertheless among the most complex and alarming. Indeed, the hostile uses of cyberspace by State and non-State actors are on the rise and the forms that they take are rapidly evolving, sometimes with serious repercussions on every aspect of human life. The phenomenon has no spatial limits, which seriously jeopardizes global peace and stability and should be diligently remedied.

Transcending borders, any truly effective response to the challenge must also take place within an international and multilateral framework. It should, among other things, focus on the protection of critical infrastructure and critical information infrastructure, which are increasingly under sophisticated attack, causing major disruptions and financial damage and even threatening people’s lives. Particular attention must be paid to encouraging regional efforts to facilitate the exchange of experiences and good practices, such as the Cyber Africa Forum, held on 24 and 25 April in Côte d’Ivoire, which was devoted to protecting critical infrastructure from cyberthreats.

It is also important to work to prevent the use of cyberspace for terrorist propaganda, planning and logistics, particularly through the more effective implementation of the Christchurch Call to Action, aimed at eliminating terrorist and violent extremist content online, which my country signed in September 2019.

It is also essential to strengthen the framework for responsible State behaviour, established under the auspices of the United Nations, by accentuating our commitment to greater reflection within the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025. Progress in the deliberations within the Group are a cause for legitimate optimism for my delegation, which again this year joined the consensus around the second annual progress report (see A/78/265), based on a dynamic and tangible approach, including with respect to next steps.

My delegation welcomes in particular the establishment of a global, intergovernmental points of contact directory, the aim of which is to intensify the interaction and cooperation of States in order to increase transparency and predictability, thereby contributing to preserving international peace and security. My country also welcomes the ongoing discussions on the requirements and modalities for establishing a programme of action to promote responsible State behaviour in the use of ICTs in the context of international security. Côte d’Ivoire strongly supports the programme of action, which, building on the Working Group, would serve as an inclusive and action-oriented standing mechanism to respond to the need for the international community’s actions to constantly adapt to ever-changing security challenges.

My country particularly supports the concept of a renewed approach to capacity-building for States, especially for the most vulnerable. Such an approach would certainly have a beneficial impact on States’ ability to respond to cyberincidents. It is essential in order to strengthen the potential of all States to implement the framework of responsible behaviour with a view to consolidating its scope and building a peaceful, reliable and resilient digital environment. That is why my delegation, last year and again this year, has sponsored the draft resolution promoting that mechanism and urges a favourable outcome to discussions on its establishment.

Mrs. González López (El Salvador) (*spoke in Spanish*): Information and communications technologies (ICTs) are fundamental tools in today’s world, but their use inconsistent with the rules of responsible State behaviour in cyberspace and their violation of international law, particularly the Charter of the United Nations, pose serious challenges to international security.

El Salvador is fully aware of the increased use of cybermeans to threaten critical infrastructures, critical information infrastructure and global supply chains. Those threats require a serious discussion on the regulation of responsible behaviour, international law in cyberspace and measures to promote confidence, capacity and institutional dialogue. Those discussions are taking place in the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, in which my country participates constructively. We believe that the Group does critical work in establishing common understandings and finding convergences on cyberspace.

Despite the progress that El Salvador has made in cyber and digital matters, conceptually we support the future progress of those discussions under a permanent and inclusive format under the auspices of the United Nations. For that reason, we have presented our national views and participated in consultations to provide elements on the scope, structure and content of a future programme of action on responsible State behaviour in cyberspace.

At this session, the First Committee has heard an increasing number of representatives refer to the international security implications of emerging technologies, in particular artificial intelligence (AI). My country has spoken emphatically in relevant forums about the risks associated, for example, with generative artificial intelligence and machine learning, while we see significant opportunities to improve our cybersecurity systems through the use of AI. We call for an AI approach to cybersecurity and not a cybersecurity approach to AI.

We urge the regulation and promotion of the risk-based use of AI and the holding of in-depth discussions on governance models for that technology, as well as ongoing analysis of potential threats and challenges with implications for international security. Furthermore, it is relevant to highlight that the use of AI in the field of security goes beyond autonomous weapons systems, encompassing a new dimension focused on automation and not solely on autonomy. We call for a holistic consideration of AI, since the nature of the technology, its applications and uses affects all aspects of human life, even those not directly related to security. That technological dependence is rapidly deepening and requires substantive discussion.

In the First Committee, El Salvador has addressed the cross-cutting gender approach as a crucial tool in understanding the different experiences of women and men in security matters. Cyberspace is no exception. It is undeniable that gender-based violence can be aggravated by the use of ICTs.

Finally, El Salvador attaches great importance to the participation of many actors in those processes. The challenges in cyberspace require the active collaboration of civil society, non-governmental organizations, regional organizations, academia and industry. We therefore urge Members to continue to work with the valuable contributions of those actors in our deliberations.

Mr. Muhith (Bangladesh): Bangladesh aligns itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries. Allow me to share my national position.

The rapidly changing global security landscape, driven by fast-evolving technologies, undeniably emphasizes the necessity for diverse disarmament measures beyond conventional frameworks. The rapid advancement of technology, particularly in the fields of artificial intelligence (AI), autonomous weapons systems, biotechnology and cybercapabilities, has revolutionized not only our daily lives, but also the global security landscape. Those innovations have unlocked unlimited potential for human advancement and economic growth. However, they have also introduced new dimensions of risk, demanding innovative disarmament solutions.

Bangladesh is deeply concerned about the development of military AI capabilities and the emergence of quantum technologies, particularly those related to weapons systems, which have exposed the inadequacies of existing governance frameworks. Our foremost responsibility is to harness AI for peace, not conflict. Therefore, we emphasize the urgent need for comprehensive frameworks to govern AI and emerging technologies effectively so as to ensure their responsible, effective and ethical use.

We firmly believe that cyberspace must be considered a global public good that should benefit everyone everywhere, without any discrimination. To take advantage of the enormous benefits of digital technologies, the international community must develop a secure, safe, trusted and open information and communications technology (ICT) environment, underpinned by the applicability of international law to cyberspace, well-defined norms of responsible State behaviour, robust confidence-building measures and coordinated capacity-building. Our only hope for a free, secure, stable, accessible and peaceful ICT environment is through multilateralism, and we underscore that the United Nations should play a leading role in the development of international cybernorms.

In that regard, Bangladesh considers the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 to be the central and inclusive mechanism within the United Nations. We reaffirm our constructive engagement towards the success of the OEWG and welcome the consensus adoption of its two consecutive annual progress reports. In line with the second annual progress report (see A/78/265), we support the establishment of a single-track, State-led, permanent mechanism within the United Nations. We also support the establishment of an open, inclusive, transparent, sustainable and flexible process that can effectively address the evolving needs of developing countries in the dynamic ICT landscape.

We are of the view that in absence of a globally accepted norms structure, the principles of the Charter of the United Nations and relevant international law should apply to cyberspace in maintaining peace and stability. In Bangladesh, we are investing in promoting a robust cybersecurity culture across Government and society. We have put in place the necessary frameworks, policies and strategies, including the recent Cyber Security Act 2023, and are continuously building upon them. We seek international cooperation in our efforts, particularly in capacity-building and confidence-building measures,

Bangladesh attaches great importance to mainstreaming and preserving relevant environmental norms in the international legal regime concerning disarmament and arms control. The applicability or relevance of such legal norms to disarmament on the seabed and in outer space should be subject to further informed research and analysis. Education is fundamental in promoting understanding of the humanitarian and economic consequences of armament. Bangladesh underscores the significance of disarmament and non-proliferation education. We appreciate the valuable work carried out by the United Nations Institute for Disarmament Research and emphasize the need for enhanced, predictable resources to support the Institute in expanding and managing its knowledge base for the benefit of all Member States.

To conclude, we must put people at the centre of our disarmament efforts and ensure disarmament that saves lives today and tomorrow. Let us continue to work together to ensure a more secure world.

Mr. Eustathiou de los Santos (Uruguay) (*spoke in Spanish*): Uruguay shares the concerns of many Member States about increased malicious information and communications technology (ICT) activities, particularly those impacting the vulnerability of sectors related to critical infrastructure, health care, security and defence. Such malicious activities are a real and growing problem and require greater cooperation among States and between the public and private sectors in order to protect the integrity, functions and availability of cyberspace.

In Uruguay, we are working to strengthen our National Centre for Computer Security Incident Response by enhancing its response and monitoring activities so as to minimize the time required to detect and respond to incidents, reduce risks and generate significant savings for the country. In order to address those real and potential threats, Uruguay believes that it is essential for us to continue to work towards increased cooperation and capacity-building, bearing in mind the differences among countries as we address malicious ICT use. We believe that the main objective of capacity-building is to guarantee the safe, effective and significant participation of all States in cyberspace in order to take advantage of the sustainable development opportunities it offers. That being said, cooperation mechanisms, such as traditional North-South, South-South and triangular cooperation, will generate specific technical assistance actions for capacity-building, including those aimed at implementing the 11 United Nations norms for responsible State behaviour in cyberspace.

Uruguay reaffirms the relevance of exchanges of national good practices in preventing digital threats. My country has engaged in such exchanges with a number of countries of our region through our Government agency on ICT. We also recognize the key role of the United Nations in implementing confidence-building measures and promoting their implementation worldwide, as was recently underscored in the reports of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (A/76/135) and the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025.

Technological developments must go hand in hand with solid institutions, a framework that recognizes human rights and a legally secure and trustworthy environment. As societies, we have not only shared obligations, but also rights and opportunities. The joint implementation of a normative framework must be carried out in a coordinated fashion, taking account of the opinions of all Members and based on a human-centred approach to cyberspace.

In that regard, our country has put forward a comprehensive, ongoing agenda that we call Uruguay's Digital Agenda, in which we consider the regulatory framework and promote greater awareness thereof, in cooperation with all stakeholders involved. For us, digital transformation goes hand in hand with legal certainty. That is why we are promoting the normative changes necessary to take account of technological progress, prioritizing improvements in administrative procedures, mechanisms for the exchange of information between public and private entities, and digital business management.

My delegation believes that when we adopt regulatory frameworks, we must focus on accessibility, copyright, consumers' rights, fair competition, data protection, security, transparency and cyberspace, and promote adherence to relevant international standards and conventions .

Ms. Muigai (Kenya): Kenya aligns itself with the statements delivered by the representatives of Nigeria and Indonesia on behalf of the Group of African States and the Movement of Non-Aligned Countries, respectively. I will make additional remarks in my national capacity.

We thank the Permanent Representative of Singapore, Chair of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, for the briefing he will soon deliver. We commend the remarkable progress achieved by the Open-ended Working Group under his stewardship and we anticipate continued tangible outcomes in that crucial area.

In this digital era, the pervasive influence of technology shapes our increasingly interconnected global society. Indeed, the rapidly advancing digital age is correspondingly redefining our perception of security and our way of life, including our conduct of diplomacy. Striking the elusive equilibrium between innovation and preventing malicious intent is paramount but herculean. Indeed, it demands a collective global effort through a multilateral approach.

In that regard, our principal task is clear — to define the rules, norms and principles of responsible behaviour among States for our security and the use of information and communications technologies. Given the rapid technological advancements, the imperative for an environment of accountability where cybersecurity is upheld and global digital collaboration is nurtured responsibly is an urgent necessity. In undertaking that overarching task, we need to consider the initiatives of States that have made significant innovations and pioneered digital safety advancements. We encourage those States to be magnanimous in sharing relevant information and best practices in support of other countries to develop their own cybersecurity infrastructure.

The United Nations must also proactively support nations in enhancing digital capabilities and addressing the repercussions of the digital revolution, including the misuse of artificial intelligence, big data and social media. In that regard, cooperation and coordination in capacity-building should be pursued and strengthened through the utilization of existing specialized multi-stakeholder agencies and organizations, such as the Global Forum on Cyber Expertise. Crucially important too is the continuous study and understanding of the ever-evolving landscape of cyberthreats. By having insights into existing and potential threats in the sphere of information security, we can invest in preventive and pre-emptive measures through cooperation, collaboration and coordination.

In its quest to secure its digital space, Kenya has, among other things, established the National Kenya Computer Incident Response Team, implemented national public key infrastructure and recently inaugurated the National Computer and Cybercrimes Coordination Committee, comprising relevant ministries and agencies with a fully fledged secretariat to ensure the effective implementation of decisions.

In conclusion, Kenya's delegation underscores that regular institutional dialogue, as outlined in our mandate, is paramount to ensuring not only that every nation's voice is heard, but also that we collectively learn, act and grow together. Let our shared goal be an inclusive digital space that is safe and secure for current and future generations.

Mr. Gusmão de Sousa (Timor-Leste): As a developing State, Timor-Leste shares with many States the benefits and threats of information and communications technology (ICT) to the nation-building and development processes of the country. That includes the maintenance of peace and security, based on respect for the national sovereignty of all Members and under the operation of regulations on the peaceful use of ICT, as set forth in the Charter of the United Nations.

The recent coronavirus disease pandemic has shown us the importance of having strong resources in the domain of ICT security. We need to pay particular attention to the needs of developing countries in terms of the implementation of the existing rules and in their further development. The increasing development of ICT, together with emerging threats in cyberspace, will cause damage that may harm our lives. As a small State, Timor-Leste believes in the important role of this multilateral platform, as it has provided better space for dialogue among all to tackle divides between countries and make sure that all can benefit from the advantages that ICT will bring to us.

As a new country embarking in the digitalization process of the nation, Timor-Leste remains concerned by the growing threat of cyberattacks on critical infrastructure and critical information infrastructure. Developing States are still facing different challenges in responding to cyberthreats. Timor-Leste therefore believes that coordination and cooperation and the sharing of best practices through bilateral, regional and multilateral platforms will support and strengthen national structures. In that regard, we are of the view that the previous Group of Governmental Experts and Open-ended Working Group (OEWG) complemented each other in their work and presented dynamic platforms to strengthen cooperation and engage on the issue of cybersecurity.

We also take this opportunity to commend the work of Singapore in steering the work of the current Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, and we wish to emphasize its central role in the discussion around ICT and international peace and security under the auspices of the United Nations. We welcome the adoption of the 2023 annual progress report (see A/78/265) and the establishment of the global points of contact directory, as we are currently establishing our internal procedures for that process.

On the future regular institutional dialogue mechanisms, Timor-Leste welcomes the proposal for the elaboration of a future programme of action on cybersecurity, as we see it as a possible framework that is inclusive, open, transparent and effective under the auspices of the United Nations. Nevertheless, we wish to emphasize that the OEWG remains the appropriate forum to elaborate the programme of action and its establishment, as it is an inclusive mechanism that reflects the interests of all States. We are also of the view that if the POA is to be embraced by all, it should focus on confidence-building measures, especially for developing countries in addressing their needs, such as in capacity-building, to enable all and reinforce the implementation of established norms, including in addressing legal gaps in the applicability of international law to cyberspace. We accordingly welcome further discussions on the proposals, including specific details, such as organizational matters, for our preparation.

We wish to stress the need to strengthen multilateral cooperation to keep pace with the rapidly evolving security landscape, including developments in cyberspace. We share the view that confidence-building measures are critical tools for promoting trust and preventing conflicts. In that connection, we reaffirm our commitment to the disarmament machinery and emphasize the equal participation of women in the disarmament machinery.

We also wish to align ourselves with the statement delivered by the representative of Indonesia on behalf of the Non-Aligned Movement and highlight the importance of ensuring that the use of information, communications and technology is fully in accordance with the purposes and principles of the Charter of the United Nations and international law. Timor-Leste attaches great importance to the upholding of the international legal regime concerning disarmament and arms control. Its applicability to cyberspace is important in maintaining peace and stability. As our Government is investing heavily in the digitalization process, we are currently establishing the necessary framework, strategy and policy in the cyberspace domain. Along that line, we seek the cooperation of all in our efforts, particularly in the capacity-building process.

Lastly, we are of the view that engagement with the relevant sectors, such as the private sector, will assist States, especially developing ones, in understanding the nature of the threats and in cooperating and adequately addressing them, which will enrich that process.

Ms. Rodríguez Mancia (Guatemala) (*spoke in Spanish*): The international environment is characterized by threats to peace, frequent acts against world security and scourges affecting the most vulnerable in our societies. Despite that, the development of information and communications technologies (ICTs) is advancing by giant steps, focusing our attention on the need to improve our understanding and strengthen our national capacities and cooperation in cyberspace. Cyberspace has become a critical domain for global activities because of its civil and dual-use nature. It has also been used by criminal groups and terrorists on more than one occasion. Its protection through responsible State behaviour is therefore essential to guaranteeing international peace and security.

It is particularly disturbing that a number of States are developing ICTs for military purposes, which has made the use of those technologies in future conflicts between States increasingly likely. Such activities represent a complex of conditions that call for the participation and cooperation of all sectors of our countries to develop the technical and legal frameworks to strengthen cyberspace globally and nationally. That is why my country fully believes in the need to continue to promote capacity-building as an essential component of cooperation among States in promoting confidence-building measures in the area of ICT security. I reiterate the importance of full transparency and support for the exchange of information and the dissemination of good practices at the subregional, regional and international levels.

My delegation underscores the fact that the applicability of international law to the behaviour of States in cyberspace, voluntary non-binding norms for the behaviour of States in peacetime, and the implementation of confidence-building measures remain critical, as is the need to highlight the gaps among countries in terms of cybersecurity and defence. My country is particularly interested in efforts to build capacities with a view to creating a more equitable cyberspace, which will help to maintain balance in the context of international security.

Guatemala has adopted a national cybersecurity strategy, the main purpose of which is to strengthen our country's capacities, creating the environment and conditions needed to ensure participation, development and the exercise of the human rights of individuals in cyberspace. In addition, over the past year Guatemala has made considerable progress in developing cybersecurity law. My country has the honour of being an observer of the Council of Europe Convention on Cybercrime, which is aimed at addressing digital and Internet criminality by harmonizing legislation among countries, improving investigation techniques and promoting cooperation among States.

That is why we welcome the second annual progress report (see A/78/265) of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025. We highlight the importance of draft resolution A/C.1/78/L.60 to promote a programme of action to advance the establishment of a standing mechanism for responsible State behaviour in the use of ICTs in the context of international security, which Guatemala supports. In that regard, we take note of the Secretary-General's recommendations in the New Agenda for Peace, proposing the establishment of an independent, multilateral accountability mechanism on the malicious use of cyberspace by States.

Finally, we remind all States that ICTs must be used for peaceful purposes and for the well-being of humankind, promoting the sustainable development of all countries, whatever their level of scientific and technological development.

Mr. Varem (Estonia): Estonia aligns itself with the statement that was delivered by the observer of the European Union. In addition, we would like to highlight the following points in our national capacity.

Preventing and managing threats to international peace and security, including threats deriving from the malicious use of cyberspace, is of the utmost importance to Estonia. Threats in the use of information and communications technologies (ICTs) are evolving and intensifying, highlighting the increasing concerns for national and international security. Malicious cyberincidents may have devastating effects on economic and social development targets and critical infrastructure, as well as direct implications for international stability.

In particular, Russia's illegal and unprovoked invasion of Ukraine has showcased how cyberoperations are employed to support military objectives and have become part of military operations. During Russia's aggression, Ukrainian governmental authorities, critical infrastructure, local Government, the security and defence sector and private companies have been targeted in cyberspace. The malicious cyberoperations have also demonstrated a dangerous spillover effect, underlining the cross-border character of cyberthreats.

Estonia strongly condemns such malicious cyberoperations. We underline that international law — including the Charter of the United Nations in its entirety, international human rights law and international humanitarian law — is fully applicable to State behaviour in cyberspace. The United Nations Member States need to join forces to strengthen the international rules-based order and adhere it to it in cyberspace as well. We recall that any use of ICTs by States in a manner inconsistent with their obligations under the framework of responsible State behaviour undermines international peace and security and trust and stability among Member States.

Estonia values highly the work of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 and welcomes the agreement on the annual progress report (see A/78/265) in July. Despite the challenging geopolitical situation, the consensus report underscores the increasing interest of United Nations Member States in deepening the discussions on the framework of responsible State behaviour. Estonia has found deliberations on threats, norms, international law, capacity-building and future institutional dialogue to be very useful for clarifying national and regional perspectives and also building the global commitments on cyberstability.

United Nations Member States have repeatedly called for a permanent United Nations mechanism on cyberissues in the context of international security. Estonia continues to support the establishment of an inclusive, single-track and action-oriented programme of action after the current OEWG ends in 2025, as outlined in resolution 77/37. We appreciate the fact that the upcoming OEWG meetings will offer additional options for collectively shaping the programme of action.

Finally, we would like to reiterate the importance of harnessing the expertise of the multi-stakeholder community. We value opportunities for the meaningful, regular and substantial participation of the private sector, civil society and academia in the OEWG sessions. Estonia invites States and other stakeholders to continue engaging in constructive exchanges to share, to listen and to work towards enhanced global cyberresilience.

Ms. Nam (New Zealand): New Zealand is committed to advancing responsible State behaviour in a free, open, peaceful and secure cyberspace. Technological developments in cyberspace have the potential to make the world a safer place and can contribute to sustainable development, prosperity and economic growth. Equally, however, cyberspace has increasingly become a vector for new and emerging threats that are inconsistent with international peace and security. That includes the deployment of ransomware, the targeting of critical infrastructure and the malicious use of cyberactivity that is now increasingly occurring in the context of armed conflict.

New Zealand places importance on working collectively to meet those challenges and to promote responsible State behaviour online. In that regard, we welcome the consensus on the second annual progress report (see A/78/265) of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 during its fifth substantive session in July.

New Zealand notes, as we and many others have done before, that cyberspace is not a lawless space and that international law applies online as it does offline. New Zealand has been heartened to see States continuing to share their national perspectives on the application of international law. That includes States sharing views on the applicability of international humanitarian law and international human rights law. We emphasize again our position that the Charter of the United Nations in its entirety is applicable and essential to maintaining peace, security and stability in cyberspace, and that States can and should expect to be held accountable for malicious cyberactivity that is contrary to the Charter and international law.

We welcome the proposal for a United Nations programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. We continue to make a lot of progress in the Open-ended Working Group and our discussions have revealed many issues that we collectively need to address. We see that a permanent, inclusive, flexible and adaptable mechanism for regular institutional dialogue will be needed after the conclusion of the current OEWG to continue the implementation of the framework for responsible State behaviour and further facilitate work on a range of issues, building on the outcomes from successive groups of governmental experts and open-ended working groups.

We welcome and support draft resolution A/C.1/78/L.60, put forward by France, which provides a clear and transparent pathway for all Member States to consider the development of the future mechanism's scope, structure, content and modalities in a way that complements the current OEWG.

Finally, we also reiterate the importance of multi-stakeholders, including industry, academia and civil society, in addressing the numerous challenges posed in cyberspace. Those challenges cannot be surmounted by Governments alone. Non-governmental stakeholders continue to provide a vital perspective and valuable expertise to international cybersecurity discussions, and we continue to welcome and encourage dialogue with all relevant stakeholders.

Mr. Ogasawara (Japan): We have been witnessing a growing threat in cyberspace due to an increased number of incidents involving the malicious use of information and communications technologies (ICTs), such as malware attacks, cyberoperations against critical infrastructure and cryptocurrency theft. There are no borders in cyberspace. That is why international cooperation is an absolute necessity for all of us.

In that context, Japan attaches great importance to the current Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 as an inclusive platform under United Nations auspices. We commend the leadership of the Singaporean Chair and his team and welcome the adoption of the second annual progress report (see A/78/265) in July, as well as the substantial progress we have collectively achieved, such as the establishment of the global points of contact directory.

We must promote the rule of law in cyberspace. The cyberdomain is not a lawless space. International law, including the Charter of the United Nations and international humanitarian law, is applicable in cyberspace. Given the rapidly changing nature of the ICT environment, our priority should be focused on engaging in further concrete discussions on how existing international law applies. We look forward to more concrete and substantial discussions on that important topic, including in the intersessional meetings of the OEWG.

Capacity-building is another priority area. Japan has been closely collaborating with the Association of Southeast Asian Nations, the World Bank and other international partners to enhance regional and global capacity-building efforts in the field of ICT. The global round table on ICT security capacity-building, scheduled for May 2024, will provide a great opportunity for all Member States to exchange views on practical capacity-building measures, with a wide participation of relevant stakeholders.

Regarding the regular institutional dialogue, we thank the cross-regional main sponsors for submitting draft resolution A/C.1/78/L.60, on the programme of action (POA) proposed by France. Japan believes that this flexible, inclusive and single-track POA proposal can ensure a seamless transition to a new, action-oriented, permanent mechanism after 2025, where we can further develop the achievements of the OEWG. We sincerely hope that the draft resolution, the outcome of our collective efforts, will be adopted with the broad support of Member States.

As the only country that has ever suffered the use of atomic bombs during war, Japan attaches primordial importance to our efforts in disarmament and to non-proliferation education. At the tenth Review Conference of the Parties to the Treaty on the Prohibition of Nuclear Weapons in August last year, Prime Minister Kishida Fumio announced the establishment of the Youth Leader Fund for a World without Nuclear Weapons as part of our efforts under the Hiroshima Action Plan that he presented at the conference. The primary goal of the programme is to bring future leaders from nuclear-weapon States and non-nuclear-weapon States alike to Japan to learn first-hand the realities of nuclear weapon use. It is also aimed at creating a global network of diverse international cohorts of future leaders and other key actors from Governments, civil society, education, academia, media, industry and other sectors.

The tragedies of Hiroshima and Nagasaki must not be repeated. Raising awareness of the experiences lived in Nagasaki and Hiroshima after the use of nuclear weapons should underpin our collective efforts towards a world without nuclear weapons. Japan considers it its duty to pass those experiences on to future generations and across borders.

Mr. Van der Haegen (Switzerland) (*spoke in French*): Malicious cyberoperations by State and non-State actors have increased continuously in recent years, both in peacetime and in armed conflict. The war against Ukraine is an example of that development, and not the only one. Cyberattacks conducted by criminal actors against companies or private individuals, against critical infrastructure or directly against States, as the attack on Costa Rica demonstrated, are exponentially on the rise. Those challenges can be met only through respect for the agreed framework of responsible State behaviour in cyberspace, as confirmed and reaffirmed by the consensus reports of the groups of governmental experts and open-ended working groups and endorsed by all States in the General Assembly.

Switzerland welcomes the adoption of the second annual progress report (see A/78/265) of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025, as it embodies a solid basis for the future work of the Group. We particularly welcome the opportunity to pursue the discussion on the applicability of international law, including international humanitarian law, in cyberspace. We also welcome the strong emphasis on protecting critical infrastructure and critical information infrastructure from ICT threats and the recommendation for further focused discussions on that topic. Recent cyberincidents and the current geopolitical situation have shown that the protection of critical infrastructure, in particular medical and health-care facilities, are of the utmost importance. In that context, Switzerland believes that the OEWG should focus on the improved understanding, promotion and implementation of the existing 11 voluntary norms before developing new ones.

We thank the Chair of the OEWG for submitting draft decision A/C.1/78/L.13, which highlights the adoption of the annual progress report and the schedule of meetings. Switzerland fully supports the draft decision and the procedural and practical approach. We must also underscore that Switzerland has serious reservations over draft resolution A/C.1/78/L.11, submitted by the Russian Federation on that issue, as it seems redundant and would duplicate the text introduced by the Chair of the OEWG. The draft submitted by the Russian Federation also raises substantive issues, in particular because it does not build upon consensus language, adopts a pick-and-choose approach, makes no reference to the consensual framework and attempts to adapt the mandate of the OEWG. That could call into question the important progress made so far in the current OEWG. In such circumstances, Switzerland would not be in a position to support the draft.

Switzerland supports the ongoing discussions on the establishment of a United Nations programme of action (POA) on cybersecurity POA within the OEWG. We believe that the POA is best suited to become the new regular institutional dialogue once the current OEWG has finished its work in 2025. That is why we are a co-sponsor of draft resolution A/C.1/78/L.60, submitted by France, Colombia, Senegal and the United States, which will help to advance those discussions.

Before concluding, I would like to highlight the many challenges that we are facing in the light of rapidly advancing technological progress. The implications of artificial intelligence, as well as other areas of science and technology, including life sciences, are highly salient at this session of the First Committee. Going forward, those developments should become a focus of the Committee and we should ensure that it adopts a resolution that connects the different strands of arms control and disarmament with emerging technologies and that examines the complex synergies of science and technology and their impact on international peace and security.

Ms. Page (United Kingdom): The United Kingdom is committed to advancing a free, open, peaceful and secure cyberspace that enhances collective security and supports global development. That requires all States to uphold and implement the existing commitments agreed at the United Nations, namely, the framework for responsible State behaviour in cyberspace and the applicability of existing international law to cyberspace, including the Charter of the United Nations, in its entirety.

Despite those agreements, some States continue to act irresponsibly. Russia has used cyberoperations as part of a long-running campaign of hostile and destabilizing activity against Ukraine. Those attacks have real-world impacts. We are deeply concerned that the draft resolution submitted by Russia attempts to reinterpret these consensus agreements for its own narrow self-interest and in doing so undermines the framework we have collectively built here together.

Patterns of malicious cyberactivity continue to evolve. The United Kingdom has experienced increased targeting of our democratic institutions, processes and values. We will respond robustly to hostile acts against our critical national infrastructure, including by bolstering our defences through the Defending Democracy Taskforce and new powers under the National Security Act of Parliament.

The impact of ransomware on critical national infrastructure has the potential to undermine international peace and security, and we therefore welcome references to that in the second annual progress report (see A/78/265) of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025. This year, the United Kingdom, in coordination with international partners, sanctioned 18 ransomware cyberactors. We will continue to impose costs on those who harm us and hold malicious actors accountable.

Furthermore, the United Kingdom is particularly concerned by the irresponsible use of commercially available advanced cybercapabilities. That growing market encompasses a wide variety of products and services, including commercial spyware. Within a domestic and international legal framework that safeguards human rights, commercial cybertools can be used responsibly by law enforcement services to prevent serious crime and terrorism. However, their misuse can undermine human rights and threaten our collective security and the stability of cyberspace. That is a complex challenge requiring the engagement of a range of sectors. The United Kingdom and France are working closely together to develop a multi-stakeholder response and we look forward to further cooperation with all Members on this.

The United Kingdom recognizes the work of the OEWG, including the careful balance reached in its consensus annual report. We are committed to playing our part in implementing and supporting others to engage in responsible behaviour in cyberspace. That includes funding £32-million worth of capacity-building efforts this year and engaging in constructive debate to further States' common understandings of how international law, including international humanitarian law, applies to cyberspace.

The United Kingdom supports draft resolution A/C.1/78/L.60, submitted by France, to establish a permanent, action-oriented, inclusive mechanism after the conclusion of the OEWG in 2025, which would build on consensus outcomes, including those reached within the OEWG. Such a mechanism would provide continuity to States' discussions on information and communications technologies in the context of international security and enable the implementation and further elaboration of the United Nations framework for responsible behaviour in cyberspace.

Finally, I should like to say a word on multilateral export control regimes, which are a critical part of the non-proliferation system. As well as contributing to international security, they provide a level of assurance of end use, giving States the confidence to transfer technology and facilitating exports around the world. We are concerned by the continuing efforts by some States to undermine and discredit those crucial regimes.

Mr. Ghorbanpour Najafabadi (Islamic Republic of Iran): The Islamic Republic of Iran extends its heartfelt condolences to and firm solidarity with the enduring nation of Palestine. We strongly condemn the grievous atrocities committed recently by the Israeli regime in Gaza, which have so far led to more than 5,000 deaths, more than 60 per cent of them children and women. That bloodshed and indiscriminate bombardment should be stopped immediately and humanitarian aid should be delivered without hindrance.

My delegation associates itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries.

Against the backdrop of significant surge in cyberattacks, with a reported increase of up to 50 per cent in 2022, the Islamic Republic of Iran emphatically reiterates its unwavering stance on the utilization of cyberspace and the information and communications technology environment. We firmly believe that those invaluable assets, akin to a common heritage of humankind, must be harnessed exclusively for peaceful objectives, and it is imperative for States to collaborate while adhering meticulously to pertinent international law.

In line with that principled standpoint, Iran has been actively engaged in intergovernmental negotiations under the auspices of the United Nations. Our involvement is driven by a profound commitment to safeguarding the rights of all parties involved. In accordance with the foundational resolution 75/240, the guiding principle of working methodology of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025 is consensus. That entails respecting the perspectives of every single Member State. The essence of consensus must be upheld and promoted, as it underpins the deliberations of the Group.

With the adoption of the second annual report of the OEWG (see A/78/265), accompanied by a comprehensive collection of statements elucidating the positions of Member States, including Iran, we perceive that the further advancement and ultimate success of the OEWG depend fundamentally on forging a substantive consensus. As we have underscored previously, the voluntary participation of Member States in consensus or the decision not to obstruct it should not be taken for granted. Consequently, it is incumbent upon us to diligently consider and integrate the viewpoints and contributions of all Member States into the outcomes of OEWG.

In that vein, it is essential that we review previous documents of the OEWG, including the Chair's summary and the 2021 annual progress report (see A/77/275), which substantially identified outstanding issues. Those documents should serve as a foundation for constructive negotiations and the bridging of divergent viewpoints. We wish to emphasize that if we aspire for the OEWG to effectively function as a confidence-building measure, we must be vigilant in addressing the concerns and interests of all Member States. Failure to do so would erode the essential confidence and trust that the OEWG enjoys. Those qualities are invaluable to its mission.

In the light of the evolving realities, it is crucial to acknowledge that certain States, notably the United States, have not only engaged in the militarization of cyberspace, but have also conducted multiple cyberattacks. The Israeli regime in particular has launched a series of cyberattacks against Iran, with the notorious Stuxnet being a stark example. We unreservedly condemn those actions and implore the international community to hold the perpetrators accountable for their actions. Regrettably, Iran has recently found itself falsely and baselessly implicated in an alleged cyberattack. We categorically reject and caution against any unfounded claims rooted in fabrications.

Mr. Getahun (Ethiopia): My delegation associates itself with the statements delivered on behalf of the Movement of Non-Aligned Countries and the Group of African States.

The contribution of information and communications technologies (ICTs) to peace, growth and development are enormous and well recognized. For those contributions to have a positive and lasting impact, upholding the principles of responsible behaviour of States in using ICTs for only peaceful purposes is extremely critical. Despite the growing use of ICTs in industry, the threats arising from their use for criminal purposes are also increasing. That, we believe, is detrimental to our collective efforts to utilize those technologies to ensure peace and stability and achieve our strategies, and must therefore be addressed in a timely and swift manner.

Ethiopia works with others for the success of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, which is currently the only inclusive mechanism. The equal participation of all States in consensus-based outcomes is critical to its successful completion. In that regard, Ethiopia supports the view that a State-led process reporting to the First Committee is the best approach. In a similar vein, we believe that regional platforms are also important to reaching the needed consensus. Hence, we share the view that developments in the use of cyberspace in the context of international security could be discussed inductively from the subregional and continental levels to the global level, which would help to build the confidence at all.

We emphasize that developing countries need capacity-building programmes on technical, legal and related matters of ICTs pertinent to the peaceful use of cyberspace. In that regard, it is critical that the United Nations system and regional organizations play a key role in providing capacity-building support to enable developing countries to enhance their capacities at all levels and benefit from the use of ICTs to achieve their development objectives. Such capacity-building support is also instrumental for confidence-building measures, with the aim of enhancing the stability and security of cyberspace.

Ethiopia is intensively working to utilize ICT capabilities to enhance rapid economic and social changes and build a more prosperous society. We have formulated policies and legislation with the aim of promoting and leveraging the utilization of ICTs and made progress with regard to institution-building to tap the potential of ICTs and meet our development objectives. Ethiopia is committed to contributing to and benefitting from the implementation of the global digital compact agenda to strengthen digital cooperation through an open and inclusive process. We fully support the promotion of digital solutions through access to and use of digital public goods to achieve the Sustainable Development Goals and work towards bridging the digital divide.

In our efforts to develop the ICT industry and in effectively addressing cyber-related problems, we have encountered various challenges, including a lack of financial resources, a low level of digital skills and skills in adopting digital public goods. In our pursuit to effectively and sustainably use ICTs to address our multifaceted development challenges, we therefore call on the international community to provide demand-driven support to enable us to tackle the bottlenecks surrounding the use of ICTs.

In conclusion, Ethiopia underlines the importance of securing peace, security and the stability of the information and communications technologies environment, and reiterates its commitment to working with all to achieve that objective.

Mr. Berard Cadieux (Canada): Canada would like to address two issues consequential to international peace and security: responsible State behaviour in cyberspace and the importance of applying a gendered perspective in disarmament matters as the rule, not the exception.

Canada welcomes the cumulative and evolving framework for responsible State behaviour in the use of information and communications technologies (ICTs), elaborated through the consensus report (see A/76/135) of the Group of Governmental Experts (GGE) on advancing responsible State behaviour in cyberspace in the context of international security and in the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025, as well as its 2022 and 2023 annual progress reports (see A/77/275 and A/78/265, respectively).

The framework is instrumental to peace and security and to building a common understanding of how States should behave in cyberspace. We are therefore concerned that a small number of States, including some that played a key role in developing it, are now calling into question the solidity of the framework. We recall that through the 2015 (see A/70/174) and 2021 GGE reports, the international community agreed by consensus on a set of comprehensive voluntary norms on responsible State behaviour in cyberspace, and States also agreed that international law applies in cyberspace. Those norms and international law are appropriate means to guide what States can and cannot do in cyberspace. We welcome ongoing discussions in the Open-ended Working Group on the implementation of norms and on how international law applies.

Practical confidence-building measures and capacity-building are two other key elements of the framework for responsible State behaviour in cyberspace. Since 2015, Canada has committed over $30 million to cybercapacity-building projects around the world and works with various organizations to promote an open and secure Internet. We recognize that more work is needed and look forward to deepening our discussion in the coming years.

(*spoke in French*)

Canada believes that the United Nations membership needs to establish a permanent forum to advance pragmatic, action-oriented discussions at the conclusion of the current mandate of the OEWG. Canada is therefore co-sponsoring the programme of action proposal at this session of the First Committee. The programme of action is the best forum to concretely advance the implementation of the agreed normative framework, including through support for targeted capacity-building activity. The programme of action will also provide an inclusive forum for all Member States to engage on those and all cybersecurity-related issues, while benefiting from the expertise of the private sector, civil society and academia.

With an eye to inclusivity, Canada reaffirms that securing an open Internet requires investments in gender equity and an understanding of the gendered impact of cybersecurity issues. We acknowledge the work done by the OEWG to highlight the diverse contributions of women, the posting of documentation on the OEWG portal, and the ongoing Women in Cyber Fellowship programme. We look forward to building on the programme in future United Nations work on cyberspace.

Gender perspectives are not just vital in cyberspace, but are also key to our work across the disarmament machinery. Gender mainstreaming helps to create effective, long-lasting initiatives that help address the world's most pressing security threats. One way of doing that is to collect and share age and gender-disaggregated data on the impact of weapons. Canada is encouraged by the increasing gender representation in United Nations forums, including this Committee. However, the gender imbalance remains, and we are thus missing essential voices and perspectives at the table — voices and perspectives that are needed for the development of effective non-proliferation and disarmament policies and programmes.

In conclusion, closing the gender gap is a prerequisite to creating a more inclusive, peaceful and prosperous world. Canada is therefore steadfast in its commitment to working with all stakeholders to advance gender considerations in all aspects of international security.

Mr. Shen Jian (China) (*spoke in Chinese*): The international landscape in cyberspace is currently complicated, grave and characterized by the formation of blocs, militarization and fragmentation. This year marks the twenty-fifth anniversary of the launch of the information security process at the United Nations. From the groups of governmental experts to the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security, the information security at the United Nations started from scratch and expanded in scale, with significant achievements, including the confirmation of the principles of sovereignty in cyberspace and the maintenance of peace in cyberspace; the development of 11 norms for the responsible behaviour of States in cyberspace; the observation and implementation of the framework for responsible State behaviour; and the newly established global intergovernmental points of contact directory. Those hard-won achievements have played an important role in maintaining peace and stability in cyberspace.

The successful experiences over the past 25 years have demonstrated that the only way to address challenges and realize joint development and common prosperity is to uphold peace, cooperation and inclusiveness while rejecting conflict, confrontation and exclusiveness. Maintaining the peaceful nature of cyberspace is our only option. We should put peace and cooperation at the centre of our policies and demonstrate our willingness to seek peace and development through cooperation, reject cyberconflicts and cyberwarfare, and enable cyberspace to be a place full of digital opportunities instead of a new battlefield of big-Power rivalry.

Global cyberspace governance requires the equal participation and joint decision-making of all countries. We need to strongly uphold the centrality of the United Nations on information security issues, respect the authority of the OEWG as the only process for information security under United Nations auspices, and join hands to make long-term arrangements for the future institution on information security.

In the digital era, we need to take the initiative to address the emerging challenges of information security and work hard on the real and urgent problems affecting all countries. The second annual progress report of the OEWG recognizes that

> "[c]onsidering the growth and aggregation of data associated with new and emerging technologies, States also noted the increasing relevance of data protection and data security" (*A/78/265, annex, paragraph. 17*).

China has proposed a global initiative on data security that provides an effective solution to global data security. It could serve as the foundation for our future discussions. Faced with risks and challenges in cyberspace, China would like to work with all parties, uphold solidarity and cooperation, and make joint efforts to build a community with a shared future in cyberspace.

Artificial intelligence (AI) is a new area of human development that has created huge opportunities for socioeconomic development and is also accompanied by unpredictable risks and challenges. The governance of AI, a common task faced by all countries of the world, bears on the future of humankind. Recently, China released the Global AI Governance Initiative, calling on all countries to enhance exchange and cooperation and work together to prevent risks. We should develop AI governance frameworks based on broad consensus so as to make AI technologies more secure, reliable, controllable and equitable. Previously, China also released position papers on regulating the military applications of AI and on strengthening the ethical governance of AI.

China advocates a people-centred approach and such visions as AI for Good, with emphasis on development and ethics first. We believe that AI should always develop in a way that is beneficial to human civilization. We should work together to prevent and fight the malicious use and abuse of AI technologies by terrorists, extremists and transnational organized criminal groups. All countries, especially major countries, should adopt a prudent and responsible approach to the research, development and application of AI technologies in the military field and refrain from seeking absolute military advantage and undermining global strategic balance and stability.

China advocates the implementation of tiered and categorized regulation to ensure that the relevant weapons systems are always under human control. In the light of the dual-use nature of AI technology, while strengthening regulation and governance we need to ensure the rights of all countries to peaceful uses. China opposes drawing ideological lines or forming exclusive groups to impede other countries from developing their AI. We also oppose setting up barriers and disrupting the global AI supply chain through technological monopolies and unilateral coercive measures.

China actively supports discussions to establish an international institution to govern AI within the United Nations framework and to coordinate efforts to address major issues concerning AI development, security and governance.

Mr. Christoglou (Greece): Greece aligns itself with the statement delivered by the observer of the European Union and would like to contribute a few remarks in its national capacity.

Malicious behaviour in cyberspace has intensified in recent years, including a sharp surge in cyberattacks targeting critical infrastructure, supply chains and intellectual property, as well as a rise in ransomware attacks against businesses, organizations and citizens. Cyberattacks have also evolved as a means in armed conflict, becoming one of the most important threats to peace and security of our time. With that in mind, Greece strongly supports the work that has been accomplished at the United Nations, which has notably addressed the application of national law in cyberspace. It has established both norms of responsible behaviour and confidence-building measures. Building on that work contributes to advancing peace and stability in cyberspace and benefits all countries.

Greece also welcomes the 2023 annual report (see A/78/265) of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021-2025, most notably the recommendation calling on States to engage in discussions regarding the scope, structure and content of a programme of action to advance responsible State behaviour in cyberspace. We strongly believe that the establishment of a permanent, inclusive and action-oriented mechanism would provide a strong basis for the continuation of the two most important aspects of our work: the implementation and further development of the framework of responsible State behaviour in cyberspace.

Greece is fully committed to further discussions at the United Nations on issues of cybersecurity and we reaffirm our willingness to engage positively in an effort to make constructive progress, as evidenced by our active participation in the recent OEWG process since its inception.

The meeting rose at 12.55 p.m.