United Nations

A/C.1/77/PV.19

General Assembly

Seventy-seventh session

Official Records

First Committee

19th meeting

Monday, 24 October 2022, 3 p.m.

New York

Chair: Mr.Pieris .... (Sri Lanka)

The meeting was called to order at 3.05 p.m.

Agenda items 90 to 108 (*continued*)

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

The Chair: The First Committee will continue its thematic discussions under the cluster “Other disarmament measures and international security”. Delegations wishing to exercise their right of reply will be able to do so once the Committee exhausts the list of speakers for the cluster. Time permitting, the Committee will begin its consideration of the cluster “Regional disarmament and security” this afternoon.

Before I open the floor, I would like to remind all delegations that during the thematic segment, statements are limited to five minutes when speaking in their national capacity and seven minutes when speaking on behalf of several delegations.

Mr. Lagardien (South Africa): South Africa aligns itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

South Africa supported the 2021 outcomes of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and the first Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs). It is, however, important to remain united behind a single process, and we look forward to the work of the fourth and fifth sessions of the second Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. In that vein, we congratulate Member States for having adopted by consensus the 2022 annual progress report of the Open-ended Working Group (see A/77/275) and look forward to reaching a common understanding on security of ICTs.

South Africa remains concerned about the growing threat of cyberattacks on critical infrastructure and information infrastructure. While we believe that we should confront such threats through greater cooperation and the development of best-practice mechanisms, our efforts should support national priorities and efforts to identify and designate such infrastructure. States, especially developing countries, are at varying levels of risk, given the varying capacities of States to respond to the threats posed by malicious acts in cyberspace. In that context, South Africa values the importance of both the implementation and the further development of existing norms. My delegation prioritizes implementation, which in our view will contribute to a better understanding of the gaps in existing norms, if any, thereby informing the need for new norms to be developed. Implementation is also an opportunity to identify effective practices and capacity-building requirements.

South Africa welcomes efforts towards the development of a programme of action as part of the work of the OEWG. We are confident that through our discussions on security of ICTs in the Open-ended

Working Group, we can reach a common understanding of the threats and vulnerabilities of States that will need to be addressed in such a programme of action. While South Africa has long supported its development, we believe that the OEWG remains the appropriate forum to elaborate such a programme of action and its establishment. We therefore recall the recommendation contained in the annual progress report of the OEWG for it to further elaborate the programme of action with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, which would, inter alia, support the capacities of States in implementing commitments in their use of ICTs.

We also believe that the engagement of all relevant actors, including civil society and the private sector, to understand the nature of such threats and to cooperate and adequately address, across all of society, the threats posed by both State and non-State actors, would enrich this process driven by Member States.

Mr. Röethlin (Austria): Austria fully aligns itself with the statement delivered on behalf of the European Union (see A/C.1/77/PV.18). In our national capacity, we wish to add the following points.

Since the previous dedicated debate on this cluster, in 2019, the importance of cybersecurity has increased considerably. Unfortunately, we have also seen the tremendous harm that irresponsible and illegal behaviour in cyberspace can cause. A case in point is the illegal cyberattacks accompanying the Russian invasion of Ukraine, which affected not only Ukraine but also other countries through its spillover effects.

We therefore welcome the increased attention given by the United Nations to the topic of cybersecurity and welcome the important work carried out by the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies, which completed a successful first year of its deliberation with the adoption of a progress report (see A/77/275), which the Committee will hopefully welcome by consensus. The report and its recommendations lay the foundations for the future work of the Group. We welcome the active engagement of various stakeholders in the OEWG, but also regret that a large number of important stakeholders from industry, academia and civil society were barred from participating in its work due to unsubstantiated vetoes. We cannot work on cybersecurity without interacting with the stakeholders who decidedly shape it.

Austria will continue to advocate for an open, free, stable and secure cyberspace based on the full applicability of international law, including international humanitarian law and international human rights law, and guided by the framework for responsible behaviour of States in cyberspace, adopted by consensus.

More remains to be done, especially when it comes to the exact scope of the applicability of international law, capacity-building and confidence-building measures. We will continue our efforts to that end in the OEWG and hope that the existing good practices in those areas can be examined — for example, by including exchanges with regional organizations in the framework of the OEWG. We are convinced that a programme of action can be an ideal vehicle for making progress in the implementation of the normative framework, which is why we are supportive of the draft resolution (A/C.1/77/L.73) on the programme of action submitted by France.

We are encouraged to see that the draft resolutions under this cluster cover important aspects of the work in disarmament and international security that have been neglected for too long. I will briefly touch on two issues here.

First, we welcome the important and increased work undertaken by the Office for Disarmament Affairs in recent years in the field of disarmament education. In times of increased global tensions, it becomes ever-more important to pass on information about our work. That will build awareness and will help us raise the next generations of experts doing vital work on disarmament affairs.

Secondly, the past years have seen the world grapple not only with armed conflict, but also with a global pandemic and the ever-more acute consequences of climate change. Yet the resource allocation between these three poles of crisis has not been equal. We would like to repeat our call from last year that we need to move away from the dangerous misconception that security can be ensured only by military armament. The non-military crises we are witnessing should be a wake-up call to lead us to a broader understanding of security and to better integrate disarmament instruments and measures into all efforts to build and maintain security.

Mr. De Martin Topranin (Italy): Italy aligns itself with the statement made on behalf of the European Union (see A/C.1/77/PV.18) and wishes to add the following remarks in its national capacity.

Technology development and scientific progress are critical for the well-being of humankind and have to be seen as an instrument to promote peace and sustainable growth. Information and communications technologies (ICTs) and the Internet are among the greatest human achievements of all time, offering unprecedented opportunities. Working on disarmament and security, we have the great responsibility of ensuring the proper framework for those developments and preventing any dangerous or negative use.

International cooperation is crucial to achieve that goal, and we need to improve dialogue, transparency and confidence-building measures in order to promote a better understanding of the common challenges we need to face. Italy remains committed to the concept of cyberstability, supporting the efforts of the international community leading towards a cyberspace based on the applicability and respect of international law in its entirety, beginning with the Charter of the United Nations, international humanitarian law and international human rights law.

We fully support the ongoing work of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies, and we welcome the successful conclusion of its third substantive session, with the consensual approval of an annual progress report. We therefore fully support the draft decision presented by Singapore, on behalf of the Chair, to adopt such a report (see A/77/275) by consensus. As staunch supporters of multilateralism and working methods that guarantee inclusivity and build upon existing acquis, we believe that upcoming discussions on that issue need to be fully exploited. Institutional dialogue needs to be orderly, predictable and inclusive in order to be able to make constructive progress and be time-conscious and financially efficient.

It is important to recognize that, together with the intensification and evolution of ICTs, threats have also increased. That is another important topic on which the OEWG should intensify its work, especially when it comes to the cyberresilience of digital infrastructure and to the threats posed by the use of cyber in armed conflict. Those issues are particularly pressing in the current challenging geopolitical environment and after Russia’s unprovoked and unjustified war of aggression against Ukraine.

That brutal act has served to highlight the reliance of critical activities in connected societies on digital infrastructure, telecommunications infrastructure in particular, and related vulnerabilities. Italy therefore underscores the importance of protecting digital infrastructure against malicious interference and calls on all actors to prioritize support for the resilience of information, communications and telecommunications infrastructure. That is essential to guaranteeing access to the global Internet, which underpins access to information, including life-saving information and businesses.

We are committed to increasing the cyberresilience of digital infrastructure, improving and sharing awareness of cyberthreats and expanding our coordinated cyberresponse in line with our cyber and national security frameworks and existing and future cooperation and partnership initiatives.

The cyberdomain has proved to be a very dynamic context, and we believe that further action is needed in order to translate our discussion into something tangible that improves international cooperation on cybersecurity. In that vein, Italy supports the proposal of establishing a programme of action on advancing responsible behaviour in cyberspace as a necessary initiative for an action-oriented agenda (A/C.1/77/L.73). That should and will be an inclusive process, driven by the States Members of the United Nations. We believe that, at this delicate juncture, we need to come together and give an operational dimension to our institutional dialogue.

We therefore fully support the cyberprogramme of action and salute it as a very sensible, inclusive and balanced project that can provide us with an operational dialogue focused on implementation, building on our acquis. Speaking of action, let me underline that capacity-building is crucial for a safe and secure cyberspace.

Mr. Shin (Russian Federation) (*spoke in Russian*): I would like to begin my statement by saying that we would like to once again emphasize that the Russian Federation consistently promotes a unifying agenda in the area of arms control, disarmament and non-proliferation. We submitted draft resolution A/C.1/77/L.66, entitled “Strengthening and developing the system of arms control, disarmament and non-proliferation treaties and agreements". We hope that it will be adopted by consensus and will have a positive effect on constructive cooperation on the entire range of issues concerning international peace and security.

With regard to agenda item 94, on the initiative of the Russian Federation and with the overwhelming support of the States Members of the United Nations, the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) for the period 2021 to 2025 was created in 2020. The OEWG is the only mechanism for negotiations on those matters in the United Nations system. The value of that format allows all States, without exception, to participate directly in the decision-making process on issues that affect national security and discuss all relevant initiatives of States on a truly democratic, open and transparent basis.

In that context, we welcome and share the views in support of the OEWG expressed by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18), the representative of the Philippines on behalf of the Association of Southeast Asian Nations (see A/C.1/77/PV.18), the representative of Belize on behalf of the Caribbean Community (see A/C.1/77/PV.18) and the representative of Iraq on behalf of the Group of Arab States (see A/C.1/77/PV.18), as well as the readiness of those entities to continue constructive work within that format.

The first year of the work of the OEWG ended with the consensus adoption of its annual progress report on 29 July (see A/77/275), which contains important provisions that allow for the creation of a basis for the development of an international legal regime for regulating the use of ICTs and developing inter-State cooperation in that area. The Russian Federation believes that it is essential not only to consolidate the success already achieved but also to focus the OEWG on holding further constructive negotiations in order to agree on specific measures to strengthen peace and security in the information space and to address issues with regard to digital development.

To that end, Russia submitted draft resolution A/C.1/77/L.23/Rev.1, entitled "Developments in the field of information and telecommunications in the context of international security," previous iterations of which have been submitted annually by Russia since 1998. Draft resolution A/C.1/77/L.23/Rev.1 is universal, non-confrontational and non-politicized. It complements draft decision A/C.1/77/L.54, submitted by Singapore, which endorses the annual progress report of the OEWG, and it welcomes the efforts made by the Chair of the Group, which we fully support. Draft resolution A/C.1/77/L.23/Rev.1 is based on the provisions of previously adopted General Assembly resolutions, as well as on the consensus reports of the first and current OEWGs. The objective is to safeguard the Group as the key negotiation platform dealing with the entire range of issues of international information security under the auspices of the United Nations and to prevent its fragmentation into parallel formats that duplicate one another. That is the aspiration of the broader international community, and the Group represents its achievement.

Draft resolution A/C.1/77/L.23/Rev.1 confirms the previous consensus agreement to further elaborate all national initiatives on security in the use of ICTs within the OEWG. It contains specific proposals on capacity-building in the use of ICTs and also confirms the need to decide on the future format of regular institutional dialogue on those matters on a truly universal basis, within the existing Group. Moreover, any such mechanism should be launched solely upon the conclusion of the work of the OEWG in 2025. We must give the Group a chance to fully realize its potential in the remaining three years of its mandate.

The adoption of draft resolution A/C.1/77/L.23/Rev., which Russia submitted,1 is especially crucial this year, because a group of States has submitted a draft resolution (draft resolution A/C.1/77/L.23) that essentially proposes creating an alternative format to the OEWG one. We view that as another attempt to hijack the Group's activities in order to politicize the negotiations and impose on the international community a premature decision on the format of future work in that area. We believe that approach is unacceptable. It contradicts logic and the interests of the overwhelming majority of countries. We call on the States Members of the United Nations to support draft resolution A/C.1/77/L.23/Rev.1, which aims to continue to preserve and protect the current format of the OEWG. A vote in favour of draft resolution A/C.1/77/L.23/Rev.1 is not a vote for Russia, it is a vote for continuing constructive inter-State interaction and results-oriented negotiations in the interest of strengthening peace, security and stability in the information space.

Mr. Aidid (Malaysia): Malaysia associates itself with the statements delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries and by the representative of the Philippines on behalf of the Association of Southeast Nations (see A/C.1/77/PV.18).

Rapid developments in the area of information and communications technologies (ICTs) have undoubtedly resulted in invaluable opportunities for peoples across the world, promoting socioeconomic growth and cross-border interaction in various fields. ICT platforms played a key role in facilitating the continued operation of public and private entities at the national, regional and international levels throughout the period of the coronavirus disease (COVID-19) pandemic, thereby mitigating the immense disruption costs to global society. Our contemporary reliance on ICT, which is unparalleled in human history, is a stark reminder of the nature of the attendant challenges and the importance of taking collective action to address them. As we tackle the multifaceted impact of the COVID-19 pandemic, we must ensure the optimal use of our scarce resources in the domain of ICT security. Particular attention should be paid to the needs of developing countries in terms of both the implementation of existing rules, norms and principles and the global discourse concerning their further development.

The increasing complexity and sophistication of emerging threats in cyberspace provide cause for concern. We must remain vigilant against any malicious use of ICTs, particularly against critical infrastructure and essential services. Continued dialogue and action through multilateral platforms are essential if we are to bridge development divides and take full advantage of ICTs. In that regard, Malaysia underscores the central role of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) for the period 2021 to 2025, and welcomes the adoption of its 2022 annual progress report (see A/77/275). As a universal platform, the OEWG provides a forum for all Member States to, inter alia, further develop the rules, norms and principles of responsible behaviour of States, as well as their means of implementation. The OEWG also affords Member States an avenue for sustained engagement with stakeholders who are integral players in the development, functioning and security of ICT platforms.

Last year, Malaysia was pleased to co-sponsor resolution 76/19, which among other things underlines Member States' support for the current OEWG and its mandate. The adoption of that resolution without a vote was a welcome development, signifying the common commitment of the United Nations membership to addressing ICT issues under a single platform, after several years of fractious argument over different mechanisms. At the current session of the First Committee, we have unfortunately witnessed recommendations by various delegations concerning the underlying intention and substantive merit of proposals put forward by others. That is a pattern with which we are regrettably familiar. Malaysia fervently hopes that the parties concerned will make every effort to engage constructively with each other and prevent the unravelling of the hard-won consensus, which — however fragile— has helped advance the work of the OEWG. It is evident that all parties recognize the value of the OEWG and the imperative of preserving its integrity and credibility. Like many others, Malaysia firmly believes that the OEWG is the body best suited to addressing the challenges at hand in the field of ICT security. We will continue to participate actively in meetings of the OEWG, which is itself a critical confidence-building measure that must be allowed to realize its full potential, in accordance with its mandate.

Mr. Li Song (China) (*spoke in Chinese*): I take the floor to outline China's position on peaceful uses and information and communications technology security. The peaceful use of science and technology, as well as the international cooperation thereon, are the inalienable right of all countries. Regrettably, for many years, the rights of developing countries to the peaceful use of science and technology and to international cooperation without discrimination have been far from guaranteed. The final document of the Movement of Non-Aligned Countries summit held in Baku clearly identified the unreasonable restrictions that developing countries continue to face on the export of materials, equipment and technology for peaceful purposes. China believes that the call of the countries of the Non-Aligned Movement should be responded to, and that the legitimate rights of developing countries for the peaceful uses of science and technology should be respected and the undue restrictions on such uses should be addressed as soon as possible.

Last year, the General Assembly adopted resolution 76/234, entitled “Promoting international cooperation on peaceful uses in the context of international security”, which initiated the dialogue on peaceful uses and relevant international cooperation. Pursuant to that resolution, the Secretary-General collected opinions from all parties and submitted a report (A/77/96) that enjoyed very broad participation and received the most input among all the reports on disarmament issued last year, fully demonstrating the broad-based will to engage in, and the urgent need for, dialogue on the issues concerned. Once again this year, China submitted a draft resolution on that topic (A/C.1/77/L.56). While adhering to the purpose and core concept of last year’s resolution, we have taken on board all parties’ proposals to the fullest extent, and we aim to continue the dialogue process in the framework of the General Assembly and to provide a platform in which all parties may discuss relevant issues, challenges and opportunities for cooperation.

Some countries are concerned that China’s initiative seeks to disrupt the existing non-proliferation export control regime. That is complete nonsense. The confrontation over the draft resolution on peaceful uses was not provoked by China, and it should not continue during this session. Rather, the dialogue process established under United Nations auspices, as provided for by the draft resolution, should serve as a bridge for communication and dialogue between the non-proliferation export control regime and the developing countries. I would like to stress that non-proliferation and peaceful uses are not enemies; rather, they should be partners that go hand in hand. China calls on the developing countries to give greater support to the draft resolution, urges Western countries not to obstruct the dialogue process within the United Nations framework and calls on the Member States of the United Nations to take concerted efforts to promote, in a balanced manner, both peaceful uses and non-proliferation — two objectives that are not mutually exclusive.

Currently, the global cyber security landscape is evolving profoundly, with a huge deficit in cyber and digital governance, coupled with prominent factors of instability and uncertainty in cyberspace. China believes that all parties should put the public good of the international community before their own geopolitical self-interests, put unity and cooperation before divisions and confrontation, practice true multilateralism and jointly develop and observe consensus-based international rules governing cyberspace. All countries, in particular the major countries, should fulfil their international obligations earnestly, commit to building a peaceful, secure, open and cooperative cyberspace and jointly observe, rather than merely implement, the United Nations framework for responsible State behaviour in the use of information and communications technologies. Countries should refrain from introducing ideological differences into cyberspace, from politicizing, instrumentalizing and weaponizing science, technology, economic and trade issues, from fragmenting the Internet and from destabilizing the industrial supply chains.

The future of cyberspace should be jointly planned by all countries, whether through the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security or the Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies. The consensus among countries is that there should be only one cyber security process at the United Nations. This year, the Open-Ended Working Group (OEWG) successfully produced its first annual progress report (see A/77/275), which is no small feat given the current circumstances and demonstrates the trust and confidence of all parties in the Working Group.

All parties should welcome the Working Group’s current robust momentum and respect its authority as the only information and communications technology security process at the United Nations, in line with its mandate established under resolution 75/240, and should engage in discussions on future institutional dialogues in the framework of the Working Group. All parties should refrain from attempting to build a new programme of action outside the Group and should prevent the duplication of United Nations cyber security process from proceeding on parallel tracks. China will work with all parties to make full use of the Working Group’s mechanism, strengthen communication and exchanges and jointly build a cyberspace that is more fair, reasonable, open, inclusive, secure, stable and vibrant.

Ms. Lõhmus (Estonia): Estonia aligns itself with the statement delivered on behalf of the European Union (see A/C.1/77/PV.18), and I would also like to highlight some points in our national capacity.

Estonia considers efforts to prevent and manage threats to international peace and security emanating from the malicious use of cyberspace to be of the utmost importance. Since February, we have witnessed Russia's brutal aggression against Ukraine, in which Russia has been using, alongside its kinetic warfare, malicious cyberoperations against Ukraine's critical infrastructure and essential services, as well as disinformation campaigns. Russia's malicious cyberoperation against the satellite KA-SAT network caused a significant impact in terms of indiscriminate communication outages and disruptions across private and public entities in Ukraine. The attack also affected several third countries, demonstrating the dangerous spillover effect of cyberattacks.

Estonia strongly condemns such malicious cyberoperations and sees them as a deliberate disregard of the United Nations framework of responsible State behaviour. In that regard, we reiterate 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. As reflected in the Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021 consensus report, which was endorsed by resolution 76/135, Member States agreed that States should not conduct or knowingly support any information and communications technology activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Estonia values highly the work of the Open-Ended Working Group and welcomed the adoption of its annual progress report (see A/77/275) in July 2022. Despite the severe geopolitical situation, that report sends an important signal on the need and willingness of the United Nations membership to further discuss the development and application of norms of responsible State behaviour. We encourage States to continue constructive discussions towards reaching a mutual understanding on how to effectively mitigate cyberthreats and contribute to building global cyberresilience. In order to move forward with discussions on the implementation of the agreed framework of responsible State behaviour and support capacity-building efforts, Estonia expresses its strong support for the establishment of a permanent, inclusive and action-oriented programme of action. We therefore support draft resolution A/C.1/77/L.73, which aims to start the work of the programme of action after the mandate of the OEWG concludes in 2025 and to build on the work of the latter, as well as the work of the previous OEWG and that of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.

Finally, we underline the inherent multi-stakeholder nature of cyberspace and welcome further cooperation with the private sector and civil society. The high level of expertise and the diverse views of different stakeholders allow discussions on cybersecurity in the United Nations to be better informed. Estonia deems it essential that the members of the multi-stakeholder community be given an adequate opportunity to express their opinions during the upcoming OEWG discussions.

Mr. Molla (Bangladesh): Bangladesh aligns itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

The disarmament discourse continues to be redefined by rapid technological advancements, including emerging weapon technologies, artificial intelligence and biotechnology. In particular, the revolution in information and communications technology (ICT) and the Internet have fundamentally changed our way of life. While human life is being revolutionized by digital connectivity, the risks it poses to international peace and security cannot be underestimated. We must therefore remain alert in detecting malicious uses of technology that could jeopardize our collective security.

Cyberspace must be considered as 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 ICT environment that is underpinned by the applicability of international law to cyberspace, well-defined norms of responsible State behaviour, robust confidence-building measures and coordinated capacity-building. Cybersecurity is a matter of international peace and security, and it therefore requires close international cooperation. The Secretary-General also identifies cyberwarfare as a key strategic risk in his report *Our Common Agenda* (A/75/982). No single country can respond to the threat of cyberattacks alone. Member States must therefore create a climate in which all States are able to enjoy the full benefits of cyberspace. Our only hope for a free, secure, stable, accessible and peaceful ICT environment is through multilateralism. We underscore that the United Nations should play a leading role in the development of international cyber norms.

Bangladesh considers the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security, which was established by resolution 73/27, as an important and inclusive mechanism within the United Nations. We reaffirm our constructive engagement for the success of the current OEWG and welcome the consensus conclusion of its first annual progress report (see A/77/275), which we believe will serve as a road map for our future discussions. We support draft decision A/C.1/77/L.54, submitted by Singapore. We also acknowledge the work of previous Groups of Governmental Experts and their reports, which contain important recommendations to promote an open, secure, stable, accessible and peaceful ICT environment.

In the absence of a globally accepted norms structure, we support the application of the principles of the Charter of the United Nations and relevant international law to cyberspace in order to maintain peace and stability. In Bangladesh, we are investing in promoting a robust cybersecurity culture across the Government and society. We have put in place the necessary frameworks, policies and strategies 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 in the seabed and outer space should be subject to further informed research and analysis.

Bangladesh reiterates the importance of disarmament and non-proliferation education. Education plays a fundamental role in fostering understanding on the humanitarian and economic consequences of armaments. We wish to put on record our appreciation for the continued useful work being done by the United Nations Institute for Disarmament Research. We stress the need to ensure enhanced and predictable resources for the Institute to deliver on its mandates and thereby help expand and manage its knowledge base for the general consumption of all Member States.

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

Mr. Diack (Senegal) (*spoke in French*): Senegal aligns itself with the statement made by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

We are pleased to participate in this thematic debate on other disarmament and international security issues. My delegation would like to take this opportunity to share its views on some of the issues on the agenda of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) for the period 2021 to 2025, including the implementation of international law, confidence-building measures, capacity-building and the establishment of a regular dialogue under the auspices of the United Nations.

With regard to the implementation of international law, Senegal notes that certain issues, such as the adoption of a new international legal instrument or the maintenance of positive international law to govern cyberspace, have yet to be resolved. In that regard, we believe that further discussions are necessary to avoid misunderstandings and promote a better understanding of how international law should apply to cyber activities. Senegal considers that two issues deserve particular attention.

The first issue relates to the application of international humanitarian law. It should be noted that the application of international humanitarian law should not be interpreted as a legitimization of war in cyberspace, but rather as a strict observance of the principles of necessity, distinction, humanity and proportionality in all cyberactivities carried out in the context of armed conflict.

The second issue concerns the application of countermeasures in response to cyberattacks, including collective countermeasures. In that connection, it is imperative to reach a clear consensus to ensure a balance between recognizing the legality of such countermeasures, in particular to protect countries lacking technological expertise, and controlling their use so that they do not cause conflicts in cyberspace. In pursuit of those discussions, we are in favour of resorting to the expertise of relevant institutions, such as the International Law Commission.

With regard to confidence-building measures, Senegal welcomes the proposal to establish a global directory of national points of contact and supports the recommendation in the first annual activity report of the OEWG to hold more focused discussions on the directory's operationalization. In order to promote information-sharing, it would be pertinent to work on modelling and standardizing State contributions, including contributions to the report of the Secretary-General on developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies (see A/77/92) and to the United Nations Institute for Disarmament Research Cyber Policy Portal. Such a model could include the provision of information on cybersecurity policies, legal frameworks, administrative structures and cyberthreats, as well as specific needs for responses to cyberthreats.

Nevertheless, we must always bear in mind the technical difficulties faced by some States. Hence the relevance of capacity-building as a major challenge, especially for developing countries. Senegal is aware of that and has adopted a national cybersecurity strategy that defines five strategic objectives: strengthening the legal and institutional framework for cybersecurity; protecting critical information infrastructures and State information systems; promoting a culture of cybersecurity; capacity-building and enhancing technical knowledge in cybersecurity; and participation in regional and international cybersecurity efforts.

Our country has endeavoured to adapt the legal framework for the use of digital technology and its institutional architecture, in particular through the creation of its central technical service for the security of coding and information systems, a special division for combating cybercrime and a commission for the protection of personal data. The same applies to the strengthening of training in computer security. Several training institutions have been established, in particular the Institut Professionnel pour la Sécurité Informatique and the Regional Oriented National Cybersecurity School in Dakar, as a result of our cooperation with France. In pursuit of those efforts, Senegal remains committed to all relevant legal instruments, including the African Union Convention on Cyber Security and Personal Data Protection, adopted in Malabo; the Council of Europe Convention on Cybercrime, signed in Budapest; the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; and directive C/DIR/1/08/11, of 19 August 2011, of the Economic Community of West African States on the fight against cybercrime.

With regard to the establishment of a regular dialogue under the auspices of the United Nations, my delegation welcomes the United Nations programme of action on cybersecurity and draft resolution A/C.1/77/L.73, on its implementation. We welcome the fact that the consultations on that draft resolution took into account concerns including the recognition of the OEWG as the primary United Nations mechanism on cybersecurity, the conduct of the discussions on the programme of action in the context of the OEWG and the fact that, once operational, the programme of action will take into account the consensus outcomes of the OEWG.

My delegation is convinced that cybersecurity measures should not be enacted to restrict digital development or to hinder innovation and development opportunities offered by offered by ICTs. As a means of preventing and combating the malicious uses of cyberspace, those measures must have as their sole purpose promoting an accessible, safe, peaceful and prosperous digital environment that leaves no one behind, in accordance with Target 9.c of the Sustainable Development Goals.

On all those issues, Senegal reiterates its determination and commitment within the Open-ended Working Group, which is the only framework for frank and constructive discussions on cybersecurity.

Mr. Zlenko (Ukraine): Ukraine aligns itself with the statement delivered by the observer of the European Union (see A/C.1/77/PV.18) and would like to make the following statement in our national capacity.

The rapid development of information and communications technologies (ICTs) progressively led to the reformatting of the Internet space. Nowadays it is no longer a comfortable platform for communication, but also a real weapon that is becoming more and more dangerous in the hands of hackers, criminals and some State actors and their proxies. Unfortunately, despite the existing legal norms and institutional mechanisms established to combat cyberattacks at national, regional and international levels, the advantages of the modern digital world are often abused, with cyberattacks on the rise having become a new method of warfare.

Ukraine is a State in which cyberattacks have become one of the major elements of the external attempt to undermine our sovereignty since 2014. Throughout the period from 2014 to 2021, Ukraine faced an unprecedented number of cyberoperations against vital objects of our critical infrastructure, most notably involving the launch of the NotPetya malware cyberattack in June 2017. Most of those attacks were carried out by hacker groups controlled from the Russian Federation. Since the beginning of Russia's full-scale military aggression against Ukraine, on 24 February 2022, cybercriminals have attacked the Government and local authorities. Also among the main targets are commercial and financial institutions, the security and defence sector, the energy sector and the transportation industry — precisely all the infrastructure that serves the livelihood of the population. In fact, Ukraine became the first country in the world to become a participant in a full-fledged cyberwar. Since the Second World War, humankind has never faced such serious challenges as it has since Russia attacked our country. For cyberspace, war is a completely new challenge. During eight months of the war, the Government Computer Emergency Response Team of Ukraine registered more than 1,000 cyberattacks.

Despite Russia's military aggression, Ukraine is further strengthening its cybersecurity system, with the material and advisory assistance of its partners. The national cybersecurity system put in place by the cybersecurity strategy of Ukraine is based in the Ministry of Defence, the State Service of Special Communications and Information Protection, the Security Service of Ukraine, the National Police of Ukraine and the National Bank of Ukraine. It ensures collaboration among all Government agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civil groups, businesses and other stakeholders. The purpose of the current cybersecurity strategy of Ukraine, established for the period 2021 to 2025, is to create conditions for the safe functioning of cyberspace, its use in the interests of individuals, society and the State. The document is based on the principles of deterrence, cyberresilience and interaction.

At the international level, we emphasize that particular attention should be given to the elaboration of unified standards in combating cyberthreats, sharing best practices, building mutual trust in the field of cybersecurity, preventing the use of cyberspace for political, terrorist and military purposes and providing financial and technical assistance to enhance national capacities to withstand cyberthreats, mitigate risks and strengthen resilience. In addition, the issue of ensuring accountability in cases of the identification of a particular State or State actors behind the preparation or targeted malicious use of ICTs or the dissemination of lies for hostile purposes is especially important. After all, international efforts made in that domain are simply in vain if there are no reliable mechanisms to detect, punish and bring to justice the individuals and relevant States responsible for coordinating and financing illicit activities in global cyberspace.

As one of the co-sponsors of draft resolution A/C.1/77/L.73 that fully supports the establishment of a programme of action to advance responsible State behaviour in cyberspace, which is aimed at establishing a permanent inclusive action-oriented mechanism within the United Nations, we share the key goals of that initiative of ensuring support for States in the implementation of the framework for responsible State behaviour in cyberspace and increasing dialogue in cooperation with relevant stakeholders. In that regard, our delegation strongly supports draft resolution A/C.1/77/L.73, submitted by France.

Mr. Khaldi (Algeria): The imperative of building and maintaining international peace, security, cooperation and trust among States in the information and communications technology (ICT) environment has never been so clear. In fact, the evolving threats emanating from the malicious use of information and communications technologies, as well as the increasing number of cyberattacks on the critical infrastructure of States, are deeply alarming and require a collective response. In that context, Algeria cannot stress enough the vital importance of ensuring that the use of ICTs fully respect the purposes and principles of the Charter of the United Nations and international law — 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 and human rights law — and remain in compliance with the principle of peaceful coexistence among States.

Algeria is encouraged by the positive progress reflected in the successful conclusion, in 2021, of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of international Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. The consensual adoption of their final reports generated positive momentum in the multilateral efforts on ICTs in the context of international security and provided a significant foundation to pursue our deliberations in that domain. In that vein, Algeria supported and welcomed the launch, under United Nations auspices, of the new Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications technologies, which was established pursuant to resolution 75/240, under the chairmanship of Singapore, as the only inclusive mechanism, based on consensus, with the active and equal participation of all States. Algeria therefore remains convinced that the current OEWG represents a significant milestone in international cooperation towards establishing an open, secure, stable, accessible and peaceful ICT environment. Much remains to be done, but the new OEWG again offers a unique forum in which to not only develop a better grasp of the critical issues related to the evolving threats emanating from the malicious use of ICTs, but also continue working collectively to overcome those challenges.

While we reiterate our strong support for the new OEWG and our intention to continue working constructively with all Member States for its success in 2025, we welcome the adoption of the OEWG’s first annual progress report by consensus in July 2022 (see A/77/275). We sincerely hope that consensus spirit will prevail during the remaining sessions of the OEWG, which constitute an important confidence-building measure. We also hope that regional and subregional organizations will continue to play an important role in advancing that process forward.

The international community’s ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. Therefore, building and strengthening the capacities of States in that domain is an urgent necessity.

To that end, Algeria considers that the current OEWG must be able to determine, before the end of its mandate, the appropriate mechanisms to ensure the provision of assistance and cooperation by States and the private sector to developing countries, upon their request. Such assistance should also include financial resources, capacity-building programmes and technology transfer in ICT areas while taking into account the specific needs and particularities of each recipient State.

At the same time, the current OEWG remains the best platform to discuss and develop all relevant initiatives of Member States aimed at maintaining peace and security in cyberspace.

Finally, my delegation associates itself with the statements delivered earlier on behalf of the Movement of Non-Aligned Countries and the Group of Arab States under this cluster (see A/C.1/77/PV.18).

Ms. Page (United Kingdom): The United Kingdom is committed to advancing responsible State behaviour in a free, open, peaceful and secure cyberspace.

Over many years, States have consistently expressed concern that ICTs can be used for purposes that are inconsistent with international peace and security, and that the use of information and communications technology (ICT) in future conflicts between States is becoming more likely.

That is a reality. Today we see Russia — a permanent member of the Security Council — using sophisticated cybercapabilities and information wars to undermine international peace and security. We have also begun to see States using cybercapabilities in other conflicts around the world.

The United Kingdom welcomes the inclusion of a clear and historic reference to the applicability of international humanitarian law in the first consensus annual progress report of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies. The world must stand together to promote the application and observance of international humanitarian law in both the physical and virtual worlds.

It is right that the Chair of the Open-ended Working Group submitted a decision to provide a pathway to consensus adoption of the OEWG’s annual progress report. We call on all States to support that approach and stay true to the good work that we have done together in the first year of the OEWG.

However, though we support the output of the current OEWG, we cannot overlook the challenges that we face in the process of making progress together.

The United Kingdom is a responsible cyberpower, committed to upholding our shared framework for responsible State behaviour in cyberspace through positive action.

First, when States abuse the framework, we will say so. In the last eight months, we have attributed multiple disruptive attacks against Ukrainian critical national infrastructure to the Russian State, and we have seen reckless cyberactivity enabled by the Democratic People's Republic of Korea, Iran and China. That sort of activity has real-world impacts. Cascading effects on critical infrastructure can be escalatory and have potentially devastating security, economic, social and humanitarian consequences.

We have also seen politically motivated Internet shutdowns and restrictions, as well as disruption of mobile communications, during recent protests in Iran. Restricting people's access to the Internet undermines their ability to exercise their human rights, including the freedoms of expression and association, and their ability to hold Governments to account. We call on all responsible State actors to end such malign activities.

Secondly, where we can support implementation of the framework and protect all States from malicious activity in cyberspace, we will do that, too. We are pleased to see the OEWG take an important step towards supporting Member States' shared goal of upholding responsible State behaviour in cyberspace by establishing a global points of contact directory.

Finally, the United Kingdom, like others, will continue to elaborate and share our own understanding of the framework, most recently in our further statement in May on how existing international law applies to State activity in cyberspace. That is another important foundation of our future work together.

With so many issues to address, it is clear that regular institutional dialogue is needed on this topic. That dialogue will continue to develop over time but must be securely anchored in the baseline consensus framework. We therefore welcome the French draft resolution (A/C.1/77/L.73) providing a clear and transparent pathway for all Member States to continue to discuss a possible future cyberprogramme of action within the OEWG and through contributions to a Secretary-General's report.

Such a dialogue must find a balance between providing Member States the support that they need to implement the framework and addressing threats to international peace and security in cyberspace, which are real and escalating. We cannot lose sight of new and emerging challenges to peace and security in cyberspace.

The United Kingdom is committed to going deeper into discussions with all stakeholders in order to find elusive consensus on complex issues. We have much work ahead of us. Through positive and practical action, we can address the mismatch between States' actions and their commitments to implementing the framework of responsible State behaviour and address threats to international peace and security in cyberspace.

Finally, let me say a word about missile technology 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. The United Kingdom is concerned by the continuing efforts by some States to undermine and discredit those crucial regimes.

Mr. Albai (Iraq) (*spoke in Arabic*): At the outset, the delegation of Iraq would like to associate itself with the statement delivered on behalf of the Group of Arab States and the statement delivered by the representative of Indonesia on behalf of the States members of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

The delegation of Iraq stresses that the promotion of the universality of disarmament conventions and treaties, including those that have to do with weapons of mass destruction, foremost among which are nuclear weapons, is the only guarantee of the non-use or threat of use of those weapons so as to avert the catastrophic consequences that could result from the use of such lethal weapons, which have a destructive capacity for both humankind and the environment.

The agreed international solutions set out in the multilateral framework provide the only sustainable guarantee for addressing issues of disarmament and international security. There is a need, therefore, to reiterate and implement individual and collective commitments in the context of the international multilateral framework. There is also a need for the United Nations to play a pivotal role in the field of disarmament and non-proliferation.

Iraq expresses its growing concern over the current spiralling regional and international tensions in the international arena. That has contributed to the increased use of information and communications technology (ICT) in activities that threaten regional and international peace and security. The United Nations must therefore continue to develop binding rules that control the responsible behaviour of States in that field, which is of the utmost importance. The United Nations must also continue to develop controls in that area in a manner commensurate with the relevant rapid developments.

There is also a need to continue international cooperation while preserving the central role of the United Nations in such efforts. As such, Iraq welcomes the adoption by consensus of the first report of the Open-ended Working Group established by resolution 75/240, of 2020.

Iraq expresses its full support for and readiness to make every effort to ensure the success of the fourth and fifth sessions, scheduled to be convened next year, in a manner conducive to adopting recommendations to support developing countries in facing the challenges and dangers resulting from the use of ICT, in addition to the increased threats in that field.

Mr. Gunaratna (Sri Lanka): Sri Lanka aligns itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

In this interconnected sphere of the Internet, we are equally safe and equally vulnerable, despite our differing capacities. It is said that technology is a useful servant but a dangerous master. Information and communications technology (ICT) were proven to be an essential development partner in many sectors during the coronavirus disease pandemic. The rapid transformation of education delivery is of special note in that regard with respect to mitigating any major rollback of achievements in that sector.

The global pandemic also transformed the traditional functioning of governments and organizations, permitting services to be provided remotely. Unfortunately, with those developments, cyberattacks have emerged as a leading vulnerability of critical digital infrastructure, resulting in disruptions to the delivery of essential services, the theft of sensitive data and fraud.

In order to enable countries to embrace the full potential and benefits of the use of ICTs, Sri Lanka reiterates the importance of all Member States taking cooperative measures to ensure cybersecurity. It is necessary to intensify global efforts to set international standards and develop cyber-risk management frameworks to establish good governance and a regulatory environment within cyberspace. Here Sri Lanka notes with appreciation the work of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies.

Nationally, Sri Lanka is implementing the nation’s first information and cybersecurity strategy, which has identified the importance of establishing a partnership-based approach to ensuring cybersecurity. Sri Lanka has continued to strengthen its legal framework to protect computer users, critical national infrastructure and cyberspace by introducing the Computer Crimes Act, the Payment Device Fraud Act, data-protection legislation and the Electronic Transaction Act. Sri Lanka is currently finalizing its cybersecurity bill.

The misuse of ICTs by any actor for any purpose is to be condemned. In the age of information, the misuse of that resource for malicious purposes harms all structures — social, economic and political — and becomes more a tool of divisiveness than a bridge that brings the world and our peoples closer. The implementation of norms, rules and principles of responsible behaviour and compliance with treaties, agreements, obligations and commitments in that field, therefore, is essential to ensuring a safe and secure cyberspace and contributing towards international peace and security.

In connection with the deteriorating international security context, we are seeing a reduction of consensus-driven cooperation and the direction of future road maps in this sphere, which is regrettable and to the detriment of all States. That will only lead to the greater misuse of cyberspace by terrorists, violent extremists and other malicious actors aiming to disrupt the safety of the users of that space and threaten international peace and stability.

Sri Lanka therefore underscores the importance of continued cooperation, the sharing of best practices and capacities among countries to effectively address cybersecurity challenges, reduce the digital divide and enable unimpeded economic and social progress. Let us not, in our collective failure to come together, bring to life the words of Albert Einstein, spoken before the Internet age, to the effect that it had become appallingly obvious that our technology had exceeded our humanity.

Mr. Hovhannisyan (Armenia): Armenia is committed to supporting the efforts of the international community in mitigating the risks and countering the threats stemming from the use of information and communications technology (ICT).

The crisis caused by the coronavirus disease pandemic highlighted the growing potential of ICTs in ensuring the proper and continuous functioning of Governments and the delivery of public and social services. However, ICTs were also utilized to incite discrimination, identity-based hatred and disseminate extremist ideology and violent practices. The growing use of social networks to spread animosity, encourage hate crimes on ethnic and religious grounds and glorify their perpetrators, in particular when promoted at the State level, constitutes a dangerous trend that if not addressed could lead to grave breaches of international humanitarian law and international human rights law.

The fourth Global Forum against the Crime of Genocide, entitled “Prevention of genocide in the era of new technologies”, to be held in Armenia on 12 and 13 December, will focus on the potential of innovative technologies in the prevention of atrocity crimes and the risks stemming from their weaponization, as well as the application of digital tools and platforms as early-warning mechanisms to prevent violence and conflict.

We would like to reiterate that the principles and norms of international law in their entirety should become the basis for responsible State behaviour in cyberspace.

Regional organizations have an important role in implementing the framework for responsible State behaviour in the use of ICTs. In that regard, Armenia values the continuous efforts undertaken in the framework of the Organization for Security and Cooperation in Europe (OSCE) aimed at enhancing transparency, predictability and stability in the use of ICTs, as well as the full implementation of OSCE confidence-building measures to reduce the risks stemming from the malicious use of ICTs.

We underscore the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies. In studying existing and potential threats in the sphere of information security, it is important not to overlook the implications of the malicious use of ICTs for the enjoyment of human rights, in particular the right to seek, receive and impart information and ideas regardless of frontiers.

Armenia supports the activities of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies as an inclusive and transparent platform for advancing the dialogue between Member States and other stakeholders on the implementation of the rules, norms and principles of the responsible behaviour of States. The OEWG is designed to address the applicability of international law in the ICT sphere, identify ways to prevent and counter threats in the sphere of information security and promote confidence-building measures and capacity-building. The annual progress report of the OEWG forms a good basis for further advancing the discussions among Member States. We look forward to constructive, results-oriented deliberations during its fourth substantive session, to be held in March 2023.

Ms. Subhashini (India): At the outset, I convey warm Diwali greetings to all.

India is pleased to introduce under this cluster draft resolution A/C.1/77/L.59, entitled “Role of science and technology in the context of international security and disarmament”, which addresses the felt need of States for enhanced international cooperation in the peaceful uses of science and technology.

The draft resolution recognizes that scientific and technological developments can have both civilian and military applications and that progress in science and technology for civilian applications needs to be maintained and further encouraged. The draft resolution is mindful of the need to regulate the transfer of technologies for peaceful uses in accordance with the relevant international obligations to address the risk of proliferation by States or non-State actors.

It highlights the importance for Member States to continue efforts to apply developments in science and technology for disarmament-related purposes as well as to engage with experts and the relevant stakeholders from industry, academia and civil society to effectively address the challenges involved.

India is grateful to the Secretary-General for having submitted the updated report A/77/188, as mandated by resolution 76/24, of 2021. We are pleased that that resolution was adopted by consensus and had the support of almost 40 Member States as sponsors and co-sponsors last year.

As a developing country, India supports enhanced international cooperation in and the promotion of peaceful uses of science and technology through the relevant means, including technology transfer, the sharing of information and the exchange of equipment and materials. At the same time, India believes that it is imperative that international transfers of dual-use goods and technologies and high technology with military applications be effectively regulated, keeping in mind the legitimate defence requirements of all States and non-proliferation concerns.

The rapid developments in various disciplines, including biosciences, material sciences, artificial intelligence and the application of data to new and emerging technologies provide significant benefits and may also pose challenges to peace and security. India recognizes the need for an interdisciplinary approach to understanding their implications as well as to formulate appropriate responses to mitigate their adverse impact.

India supports and actively participates in discussions relating to emerging technologies in various multilateral forums of the United Nations and specialized agencies and within the framework of the international treaties to which India is party.

India is committed to promoting an open, secure, stable, accessible and peaceful ICT environment. The malicious use of cyberspace by terrorists and for criminal purposes and the interconnected nature of the ICT domain necessitate a collaborative, rules-based approach and work to ensure its openness, stability and security.

In that regard, India supports the action-oriented work of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies, chaired by Singapore. We welcome the consensus adoption of the 2022 annual progress report of the Group, which provides a solid foundation for the work of the Group for the coming year.

The OEWG, during its tenure, should remain the main platform for all intergovernmental deliberations on ICT issues related to its mandate. We strongly discourage the creation of formal parallel processes until the completion of the OEWG's work.

Recognizing the disparity among Member States in cyberpreparedness to tackle various cyberthreats and the need to enhance their capabilities, India has proposed the development of a global cybersecurity cooperation portal anchored in the United Nations as a global platform for capacity-building and international cooperation among Member States. We look forward to productive discussions and a decision on that issue in the coming year in the OEWG.

Given the relevance and importance of this topic, there is a heightened need for States to work together to address the complex challenges involved. India seeks the continued support of all Member States towards the adoption of its draft resolution on the role of science and technology in the context of international security and disarmament by consensus this year. We would also encourage Member States to co-sponsor the draft resolution and join us in this collective endeavour to make a meaningful contribution to global peace and security.

Ms. Rodríguez Acosta (El Salvador) (*spoke in Spanish*): The growing interconnectivity and our dependence on information and communications technology (ICT) in all spheres of life require that all States heighten their interest in and increase their knowledge about developments in the field of information security and the importance of preventing any malicious use of ICTs.

For those reasons, my country deems cybersecurity to be a fundamental part of international security. We note with concern that recent incidents involving ransomware operations and other types of cyberattacks aimed at incapacitating or slowing down the provision of public services have had serious implications for international security and have laid bare the urgency of strengthening cyberresilience to protect ourselves from such global threats. That is a goal that States cannot meet alone. The active cooperation of the entire international community is necessary to tackle those challenges.

We therefore welcome the consensus adoption of the first progress report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, in which we participated actively. As stated by our delegation in the compendium of explanations of positions published upon the adoption of the report, that report did not claim to be an exhaustive summary of the Group's work but, rather, sought to outline the progress made to date and establish guidelines for future discussions.

Along the same lines, we welcome the progress made towards establishing a global points of contact directory, as mentioned by our delegation during the final sessions of the Group's work. We believe that that confidence-building initiative could be a valuable source of information exchange on threats, vulnerabilities and cybersecurity incidents in real time. We have therefore suggested studying the possibility of establishing that directory at the technical and operational levels, among national cybersecurity teams and cyberdiplomacy liaisons.

We hope to be able to present our national contributions before the fourth session of the Working Group. Likewise, we take due note of the submission of draft resolution A/C.1/77/L.73, on the establishment of a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. That initiative has been supported by El Salvador from the outset. We believe that it will complement the efforts of the current Working Group and allow for the future establishment of an action-oriented standing discussion mechanism for Member States.

My country continues to work towards and contribute to multilateral discussions aimed at bolstering the framework for responsible State behaviour in cyberspace and to discuss existing real and potential threats in the areas of security and information. We therefore reaffirm the importance of moving forward towards a binding framework that will allow us to protect critical infrastructure and critical cyberthreat information infrastructures, and to identify vulnerabilities with a view to protecting strategic national assets.

El Salvador is committed to advancing its digital transformation agenda with a focus on protecting personal data and critical infrastructure, so as to bolster our people's trust in digital-service provision at the national level. We are therefore pleased to have finalized our public consultations on the cybersecurity law, led by our presidency's Innovation Secretariat. In the same vein, it is important to continue encouraging the development of confidence-building measures, which make it possible to ease tensions and de-escalate conflicts in cyberspace.

We have actively stressed the importance that we attach to broad participation by other stakeholders in those processes. Challenges in cyberspace require active cooperation on the part of civil society, non-governmental organizations, regional organizations and academia.

Finally, my delegation has reiterated that a cross-cutting gender approach could help us to understand the prevalence of patterns of armed violence and conflict, which impact men and women differently. We must be decisive in tackling those challenges. Gender issues are also relevant in the context of international cybersecurity.

The full version of this statement will be published on the eStatements platform.

Ms. Lee (Republic of Korea): Over the past couple of decades, the human race has witnessed advancements in digital technology like never before. While that development has brought us unprecedented economic and social benefits, with more people online since the global pandemic, we have become ever more vulnerable to malicious cyberactivities. State and non-State actors' behaviour in cyberspace further complicates the international security landscape.

Notwithstanding the complexity of the challenges we face, the international community must work together towards an open, secure, stable, accessible and peaceful cyberspace. In that regard, the Republic of Korea supports the central role of the United Nations in the ongoing discussions to address pressing concerns and advance responsible State behaviour in cyberspace. I would like to highlight the following points in particular.

First, the Republic of Korea welcomes the 2022 annual progress report of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies, and we also welcome the Chair's decision to endorse the report. The Republic of Korea will continue our constructive engagement in the OEWG by building on that progress report, adopted by consensus.

As a co-sponsor of draft resolution A/C.1/77/L.73, entitled "Programme of action to advance responsible state behaviour in the use of information and communications technologies in the context of international security", submitted by France, we would like to underscore the need to establish a permanent mechanism within the United Nations such as the programme of action to enhance the practical implementation of the norms and encourage the exchange of best practices and capacity-building.

Secondly, the Republic of Korea believes that the consensus outcomes of the OEWGs and the previous Groups of Governmental Experts (GGEs) reflects the progress made in the cumulative and evolving framework for responsible State behaviour in the use of information and communications technology (ICTs). Accordingly, as there should be no vacuum for legalities in cyberspace, international law, including the Charter of the United Nations, in its entirety must be equally applied to cyberspace. Furthermore, States should faithfully uphold and implement the voluntary, non-binding norms set out in the consensus reports of the GGEs and OEWGs. In particular, my delegation believes that the principle of due diligence plays a crucial role in ensuring cybersecurity and would like to cooperate closely with other Member States in further developing and implementing the relevant norms.

Thirdly, the Republic of Korea is a strong supporter of confidence-building measures (CBMs) and capacity-building. CBMs can limit the risk of conflict deriving from misunderstanding and miscalculation. The Republic of Korea will also endeavour to bridge the gap in cyberdefence capabilities. We are actively engaged in relevant efforts in regional forums such as the Association of Southeast Asian Nations (ASEAN) and the ASEAN Regional Forum.

My delegation believes that the engagement, empowerment and education of the younger generation can lead to valuable contributions to the global non-proliferation regime. Since 2019, Member States have adopted a biennial resolution entitled “Youth, disarmament and non-proliferation” by consensus. Also, the draft final document of the most recent Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons recognized the importance of diverse voices and commitment to empower and enable youth participation in the field of disarmament and non-proliferation. As a champion of Action 38 of the Secretary-General’s *Securing our Common Future: An Agenda for Disarmament*, the Republic of Korea will continue to lead the agenda and commit to furthering that endeavour.

Before concluding, my delegation would like to point out that the Republic of Korea respects the right of all Member States to have access to equipment, materials and scientific and technological information for peaceful purposes and in that vein strongly believes that the existing export-control regimes foster that purpose, as they distinguish what can be exported from what cannot be exported, instead of giving a free hand to exporting countries for arbitrary restrictions or undue licensing.

Mr. Aydil (Türkiye): Today the global situation regarding peace, security, human rights and economic development is increasingly being impacted by the use of information and communications technology (ICT).

Türkiye remains concerned about the malicious use of such technologies and the increasing number and severity of cyberattacks worldwide. Our citizens’ lives are being severely impacted by cyberattacks that target critical infrastructure such as electronic communication, energy, finance, transportation, water management and other critical public-service sectors.

Tackling such threats and risks in the cyberrealm is essential in order to achieve an open, free, stable and secure cyberspace at the global level.

A wealth of work has already been done regarding responsible State behaviour in cyberspace. We underline the central role of the United Nations in that process. In our view, cyberdiscussions under the auspices of the United Nations have reached a certain level of maturity. We therefore need to start discussing how to promote the implementation of the existing normative framework.

The final report of the previous Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies indicated that the use of ICTs in future conflicts between States is becoming more likely. The war in Ukraine has justified that concern, and the task at hand is therefore urgent.

In order to better implement the existing cumulative framework, a good step forward would be the establishment of a programme of action on cybersecurity issues. We support draft resolution A/C.1/77/L.73, submitted by France, to that effect and look forward to continuing our discussions in future through the programme of action as a permanent, inclusive and action-oriented mechanism. The programme of action would also be beneficial for the promotion of dialogue and cooperation on capacity-building issues, which are central to cyberresilience. That initiative does not aim to duplicate or compete with the current OEWG on ICT security. It will take into account its conclusions and contribute to efforts towards their implementation.

Türkiye participates actively in the current OEWG. We welcome the consensus adoption of the annual progress report this year. We agree with the assessment that the Working Group, with its universal membership, is a unique platform and constitutes a confidence-building measure in itself.

The nature of cyberthreats makes unified action necessary. We would have wished to see a consensual approach in the First Committee this year, as happened last year. We once again appeal for a cooperative spirit in that regard.

Mr. Ogasawara (Japan): Cyberspace has become an indispensable economic and social infrastructure for all activities and is therefore a public space for all citizens to participate in. That economic and social transformation has also made us vulnerable to cyberattacks, which pose a major security risk to all. From a national security standpoint, we are particularly concerned about malicious cyberactivities emanating from other States that damage critical infrastructure, whether supported by those States or not.

It is difficult for any one country to respond to such cybersecurity threats alone. Cooperation and collaboration among States is paramount to protect and enhance a free, open and secure cyberspace.

On the issue of how international law applies to cyberoperations, Japan's position is clear: existing international law is applicable to all such operations. We also strongly support the development of voluntary norms of responsible State behaviour. Establishing the rule of law in the international community is of great significance for stabilizing relations among countries and realizing the peaceful settlement of disputes.

Japan considers it important to promote the rule of law in cyberspace as well. In order to do so and realize a free, fair and secure cyberspace, Japan welcomes the annual progress report adopted by consensus in the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies for the period 2021 to 2025. As it is an action-oriented process, it is important for the OEWG to achieve concrete results based on the outcome of past discussions as reflected in Group of Governmental Experts and OEWG reports. In that regard, we strongly support the OEWG Chair's decision to endorse the annual progress report.

We also support draft resolution A/C.1/77/L.73, on a programme of action to advance responsible State behaviour in cyberspace, presented by France.

I would also like to address the issue of disarmament and non-proliferation education, which Japan has been promoting as a useful and effective means of advancing towards a world without nuclear weapons.

In that regard, it is essential for us to raise awareness among the public of the catastrophic humanitarian consequences of any use of nuclear weapons, the threat of the diverse risks posed by the proliferation of nuclear weapons, as well as the steps required to overcome those challenges.

Disarmament and non-proliferation education and awareness-raising should be undertaken in an inclusive and collaborative manner. Various actors, including educational and research institutions, think tanks, the scientific community, civil society, the private sector, media, local municipalities, international organizations and Governments, should learn from one another and create synergies to advance educational initiatives.

It is from that perspective that Japan is proposing to mention some concrete initiatives in that direction in operative paragraph 11 of draft resolution A/C.1/77/L.61, entitled "Steps to building a common roadmap towards a world without nuclear weapons", which Japan submitted to the Committee this year.

Japan has been actively engaging in various disarmament and non-proliferation education efforts. Notably, at the Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), in August, Prime Minister Kishida announced the Youth Leader Fund for a world without nuclear weapons. Japan also took the lead of the joint statement on disarmament and non-proliferation education at the Conference, which gathered support from 89 States parties to the NPT.

Japan firmly believes in the power of disarmament and non-proliferation education and the potential for future generations to achieve our common goal: the realization of a world without nuclear weapons.

The full text of this statement will be uploaded to *The Journal of the United Nations.*

Ms. Romero López (Cuba) (*spoke in Spanish*): We align ourselves with the statement made by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

We reiterate Cuba's commitment to generalized and complete disarmament, which will allow us to achieve a world free of weapons of mass destruction for the benefit of present and future generations. We call for the adoption of further measures for disarmament and international security, which will allow us to move towards the building of a world of peace.

We must minimize as soon as possible the considerable resources currently devoted to military budgets. The same resources and scientific and technological progress that are currently being used to finance the military-industrial complex and to develop, produce and perfect increasingly deadly and sophisticated weapons would yield abundant benefits for humankind if they were to be redirected towards achieving sustainable development.

Member States must continue to work to preserve multilateralism as a basic principle for negotiations on disarmament and arms control. We would recall that such negotiations must observe current international environmental norms.

We call for the negotiation of legally binding initiatives to prevent the militarization of outer space, cyberspace and lethal autonomous weapons. We must reach agreement to regulate partially autonomous weapons and military attack drones.

We reiterate our commitment to the work of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies for the period 2021 to 2025. We support the discussions in that format, with the participation of all States on an equal footing.

Information and communications technology must not be used as a means of war but, rather, for exclusively peaceful ends. We reject the hostile use of telecommunications with the declared or non-declared purpose of subverting the legal and political system of States, or of committing or encouraging acts of terrorism.

We oppose the consideration of the use of force as a legitimate response to a cyberattack. We reiterate our concern regarding the United States' cyberstrategy, which authorizes the use of offensive cyberweapons and the realization of cyberoffensive operations, including preventive cyberattacks aimed at deterring its opponents.

We reject the non-conventional methods of war that the Government of the United States continues to use against Cuba and the vast resources expended on that goal. We condemn the use of new information technologies and other digital platforms to attempt to destabilize our country, disseminate fake news and foster regime change in Cuba. We oppose the Cuba Internet Task Force, which violates internationally agreed norms in that area. We call on the United States to put an immediate end to the economic, trade and financial blockade imposed against Cuba, which considerably restricts the access, use and enjoyment of information and communications technologies for the well-being of the Cuban people.

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

Mr. Salmeen (Kuwait) (*spoke in Arabic*): My country's delegation aligns itself with the statements delivered on behalf of the Movement of Non-Aligned Countries and the Group of Arab States, respectively (see A/C.1/77/PV.18).

Cybersecurity is one of the new issues that the world is facing, and many countries are currently suffering from its negative effects, including the State of Kuwait, which has been subjected in recent years to many cyberattacks as well as acts of cyberpiracy, whether individual or sabotage attacks sponsored by terrorist and foreign criminal groups. That was owing to the dual-use nature of cyberspace and the use of microtechnology and resources to develop new weapon systems, which has exacerbated doubts and lack of confidence among States.

In that regard, my country stresses the need to ensure security standards and provide protection against cyberattacks and programmed violations. We call on all countries to cooperate and coordinate their actions at the regional and international levels.

The State of Kuwait highly prioritizes cybersecurity because it is a critical defensive force, especially as cybercrime not only targets individuals and institutions but also jeopardizes national security and States' facilities and economies. That is why the State of Kuwait launched a national cybersecurity strategy for 2017-2020 in order to bolster the culture of cybersecurity and promote the fair and safe use of Kuwaiti cyberspace, as well as to protect critical and national information infrastructure, including by strengthening mechanisms for information exchange among various stakeholders, both local and international. We underscore that our strategy is in line with strict security policies and global criteria that ensure protection for information against all kinds of hacking and guarantee a safe and sustainable Kuwaiti cyberspace.

In that context, given that the political leadership in the State of Kuwait is aware of the scope of the challenges imposed on us by cyberspace and owing to my country's commitment to digital transformation to promote our national development as part of the new Kuwait 2035, the State of Kuwait created a national cybersecurity centre that includes a cybersecurity operations centre as well as a response team for cyberemergencies, with a view to establishing a comprehensive national strategy for cybersecurity. That will ensure the protection of our information and telecommunication networks as well as enable the collecting and exchange of information through the use of any electronic devices, in partnership with all national stakeholders.

We are facing a technological revolution and an unprecedented and accelerated digital transformation while increasingly making use of the Internet and modern communication means. The world is now more interconnected than ever, which increases the risk of cyberattacks, including information theft and breaches of confidentiality. There is also a high percentage of gaps in modern weapons that depend on modern technology. In that context, the State of Kuwait is concerned about autonomous weapons and 3D printing telecommunications, which has become more widespread in manufacturing processes throughout the world. That constitutes a new threat to international peace and stability — if those technologies were to fall into the hands of terrorist groups or organized criminal groups or were to be used illegally, which would certainly have disastrous consequences for the relevant infrastructure and the flow of safely manufactured goods. In that regard, my country reiterates its steadfast position on disarmament and international security. We believe that the flow and proliferation of weapons run counter to our desired goal of achieving international peace and stability.

We therefore call on all States to deploy efforts to achieve an international binding and consensual instrument that would govern the use of cyberspace as well as to establish mechanisms for the exchange of information among States parties. In addition, such an instrument must respect the sovereignty of States when it comes to drones, which are widely used as a new means of warfare targeting civilians and State infrastructures. The State of Kuwait underscores its condemnation of all cyber and electronic attacks involving the use of drones, as they have serious security repercussions at the regional and international levels. In that context, we call on States to uphold the principles of the Charter, including good-neighbourly relations and respect for the sovereignty of States and non-intervention in their internal affairs.

The State of Kuwait welcomes the two programmes of action on cybersecurity launched by Secretary-General António Guterres as part of the 2018 disarmament agenda.

In conclusion, we value all international efforts related to the issue of cybersecurity and call for them not to be politicized and for promoting the principle of transparency in that regard. We emphasize our continued support for all international measures that build confidence and capabilities in order to limit the threats to international peace and security.

Mr. Jotterand (Switzerland) (*spoke in French*): Switzerland is concerned by the increasing resort to cyberoperations as part of the armed conflict in Ukraine, especially when they are directed against critical infrastructure. The potential for involuntary consequences or excesses is thus increased. Switzerland calls on all parties to armed conflict to respect international humanitarian law as well as international human rights law. That also applies to cyberspace.

In our rapidly changing world, civilian and military uses of cyberspace are growing, posing new challenges for international peace and security. Those challenges can be addressed only through compliance with the agreed framework for the responsible behaviour of States in cyberspace. As confirmed by the consensus reports of the Group of Governmental Experts and the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies, that framework includes the application of international law in cyberspace, the implementation of the 11 voluntary norms and confidence- and capacity-building measures.

We welcome the adoption by consensus in July of the annual progress report of the Open-ended Working Group, which contains, among other elements, important proposals aimed at the further clarification of the concrete application of international law, including international humanitarian law and the implementation of the voluntary norms on responsible State behaviour in cyberspace.

The ongoing critical work of the current Working Group provides an invaluable opportunity to further build on the consensus that international law applies in cyberspace. To contribute to our shared goal of creating a common understanding of how international law applies to cyberspace, Switzerland in 2021 issued its national position on that important matter.

We encourage all States Members of the United Nations to consider issuing their own national positions. We also are looking forward to continuing deliberations on all elements of the mandate of the current Working Group.

We welcome the proposal by the Chair of the OEWG to hold intersessional consultations in 2023 and 2024 to advance discussions, build on the annual progress report and support the continued work of the Group. In that regard, we thank the Chair of the OEWG for having introduced to the Committee a draft decision (A/C.1/77/L.54) that encompasses both the endorsement of that report as well as the intersessional consultations that I mentioned. Switzerland fully supports the draft decision and that purely procedural and practical approach.

We also have to underline that we have serious questions regarding the draft resolution (A/C.1/77/L.23/Rev.1) introduced by the Russian Federation on this issue, as it seems to be both unnecessary and to duplicate the OEWG Chair’s text. The draft submitted by Russia also raises questions concerning substance, notably because it does not build on consensus language and uses a selective approach. That risks undermining the major progress made so far in the current OEWG. As things stand, Switzerland cannot support that draft.

The establishment of a platform for regular institutional dialogue on cyberissues within the United Nations also deserves our full attention. Switzerland would like to highlight that decisions about the future of cyberdiscussions at the United Nations must be based on inclusive deliberations that would allow all Member States to present their views. In addition, in our view, any future United Nations processes need to focus on supporting Member States in their efforts to implement the existing framework for the responsible behaviour of States in cyberspace.

It is important to build on and safeguard what has been achieved over the past few years and to make effective use of the agreed recommendations. That is why we support draft resolution A/C.1/77/L.73, on a programme of action to advance responsible State behaviour in the use of information and communications technology in the context of international security, submitted by France, which will allow States Members of the United Nations to move that discussion forward.

Ms. Vladescu (Romania): Romania fully aligns itself with the statement delivered by the representative of the European Union (see A/C.1/77/PV.18) and would like to make the following remarks in our national capacity.

We are meeting in a fundamentally altered security environment marked by increased tensions and global challenges that continue to erode the arms-control, disarmament and non-proliferation architecture. The illegal, unjustified and unprovoked military aggression by the Russian Federation against its neighbour Ukraine has brought us to an unprecedented phase of escalation.

Since 24 February, we have been witnessing the dramatic consequences of that aggression, during which Russia has used all categories of conventional weapons as well as disinformation and cyberattacks. Romania resolutely condemns the Russian aggression and reaffirms its unwavering support for Ukraine’s independence, sovereignty and territorial integrity within its internationally recognized borders.

The security of cyberspace has become a matter of the highest priority given the fact that malicious information and communications technology (ICT) activity by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, and the safety and well-being of individuals.

Now more than ever, it is important to promote an open, secure, stable, accessible and peaceful cyberspace, to fully adhere to the United Nations framework for responsible State behaviour and to continue our work of contributing to security and stability in the use of ICTs by States.

Romania welcomes the consensus reach this year on the annual progress report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies for the period 2021 to 2025, established pursuant to resolution 75/240. We reiterate our full support for the decision of the Chair of the Open-ended Working Group on the matter and his call for a consensual adoption.

We encourage all Member States to support draft resolution A/C.1/77/L.73, on a programme of action to advance responsible State behaviour in the use of ICTs in the context of international security, co-sponsored by a transregional group of States and which has Romania's full support.

In these times of heightened tensions and conflict, the need for strength and transparency, in particular in the field of military expenditures, is even more relevant. In that regard, we would like to draw attention to this year's draft resolution entitled "Objective information on military matters, including transparency of military expenditures" (A/C.1/77/L.63), traditionally submitted by Romania and Germany. We urge States Members of the United Nations to support the draft resolution, which is underpinned by the major principle of building trust and confidence among States.

The United Nations system for the standardized reporting of military expenditures has achieved remarkable success over many years and should remain one of our most important tools for strengthening transparency. We take this opportunity to emphasize once again the continued importance of the United Nations Report on Military Expenditures, all the more so given current circumstances, and encourage all States to actively participate in reporting.

As no notable developments have been registered with regard to the standardized reporting system since the adoption in 2019 of the previous resolution on the matter, resolution 74/24, also owing to the coronavirus pandemic, we chose to preserve the text as previously adopted by the First Committee and the General Assembly and to propose a technical rollover with only a few minor technical updates. That resolution has been on the agenda of the First Committee for more than two decades and has always enjoyed overwhelming support from States Members of the United Nations. We hope that at this session the draft resolution will be met with the same response and that States Members will once again show their support by adopting the draft resolution without a vote, as has been the case numerous times at previous sessions of the First Committee.

Mr. Vidal (Chile) (*spoke in Spanish*): Chile aligns itself with the statement made by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/PV.18).

We welcome texts based on gender equality and equity and that promote the human rights of women, children and sexually variant groups in multilateral forums and international organizations, as well as texts that focus on a gender perspective in such negotiations.

In that regard, we welcome draft resolution A/C.1/77/L.18, entitled "Women, disarmament, non-proliferation and arms control", submitted by Trinidad and Tobago and co-sponsored by my country. It is imperative that reference be made to gender issues, as contained in existing United Nations mandates, particularly in the field of international security. Gender issues must be dealt with in the context of an inclusive, equitable and effective process.

Chile believes that the threats posed by information and communications technology (ICT) can affect States differently, according to their levels of ICT digitization, capacity, security and resilience, as well as their infrastructure and development. Those threats can also affect various groups and entities in different ways, particularly women and girls. States such as ours face different kinds of threats and needs, making it critical to enhance our capacities to create structures and plans for coordination, not only at the Government level but also by developing effective partnerships with civil society, the private sector and academia.

Chile believes that international law, in particular the Charter of the United Nations, provides the applicable normative framework that must regulate the behaviour of States in cyberspace, including international humanitarian law, human rights and those laws that govern international responsibility of States, since those are vital to maintaining the peace and stability necessary to promote an open, secure, stable, accessible and peaceful environment for information and communications technologies.

For all those reasons, we support the work being done in the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies for the period 2021 to

2025, led by the Permanent Representative of Singapore, and the programme of action to promote responsible State behaviour in the use of ICTs in an international context. Our country, like other members, will always support texts that build confidence. We support all bodies in which States can exchange views and express their priorities and needs, thus bolstering the security, resilience and peaceful use of ICTs in general.

Mr. Soares Damico (Brazil): In his *Securing our Common Future: An Agenda for Disarmament*, the Secretary-General reaffirmed the need to bring the relationship between disarmament and development back to the forefront of international consciousness.

In keeping with the long-held view among developing countries, Brazil shares the self-evident notion that there is a positive correlation between disarmament and development. Indeed, domestic and international security are elements essential to economic growth. Had the financial and technological resources invested in the expansion of conventional and strategic arsenals been diverted to crucial sectors of human life such as education, health care and environmental protection, we would have been much better off. The connection between disarmament and the Sustainable Development Goals should thus reside at the very centre of our efforts.

The peace dividend we have been harvesting is quite substantial. In 1960, the average military expenditure amounted to 6.3 per cent of gross domestic product (GDP). Sixty years later, it reached its lowest level — 2.4 per cent. That means that in 25 years, we would be in a position to count on one year of GDP to improve social welfare.

Nevertheless, current tensions have resulted in a dramatic reversal of that trend. To make matters worse, that coincided with a period of unprecedented Government deficits, which, in some developed countries, reached levels previously seen only during the Second World War as a result of counteracting the effects of the coronavirus disease pandemic. The only solace we can take from that situation is that at a not-too-distant point in time, taxpayers will be compelled to decide on the dilemma of choosing between butter and guns.

No longer can disarmament, non-proliferation and arms control remain confined to high politics. More than ever, they reflect social choices, given their tremendous impact on the daily lives of millions of people everywhere, every day.

Our current disarmament agenda encompasses a new variety of topics closer to our realities such as gender considerations, discussions on unimpeded access to technologies for peaceful uses and the security aspects of information and communication technologies. Such proximity, however, does not make those topics less complex. A great divide persists on how to deal with them.

Brazil believes that the debate on sensitive and emerging technologies occupies a prominent position in current international relations. Not only must security concerns be carefully addressed; we must also advocate for an open, accessible, peaceful and safe environment for the development, exchange and use of those technologies. The priority is to strike a delicate balance in the treatment of this subject in order to safeguard the unquestionable economic and social benefits that technologies bring to our peoples as well as curbing their malicious use either by States or by non-State actors. Such an approach protects the legitimate right of all States to have access to crucial technology for their development while preserving the legitimate goals of non-proliferation and international security.

The development of information and communications technology (ICT) has become a central topic of discussion at our First Committee sessions. Since 1998, six Groups of Governmental Experts have been convened, of which Brazil chaired two.

That continued commitment by the membership to keep the issue of ICTs on its active agenda illustrates its strategic nature and the urgency of proper regulation aimed at preserving cyberspace as an open, peaceful and accessible environment, as well as the need to prevent cyberspace from becoming an arena for conflict.

To achieve that, it is essential to reconcile the various visions of the role played by cyberspace in our societies and what we want from it. By its very nature, that intergovernmental exercise would benefit from contributions emanating from civil society, academia and industry. Nevertheless, the foundation of that discussion rests on the applicability of international law, especially the Charter of the United Nations, and the uncompromising protection of human rights.

We hope that the current Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies and the future institutional dialogue mechanism to be established afterwards will strengthen the notions of responsible behaviour, transparency and confidence-building measures, as well as capacity-building, capitalizing on the work done in previous Groups of Governmental Experts and reflected in OEWG reports adopted by consensus.

We cannot fail to highlight the work carried out by Ambassador Burhan Gafoor of Singapore as Chair of the OEWG on ICT security. We welcome the adoption of the annual report at its most recent session. It provides a good basis for the continuation of our work.

Mr. Sánchez Kiesslich (Mexico) (*spoke in Spanish*): The cross-cutting challenges linked to international security require measures that are integral and go above and beyond traditional understandings of security. That is why we underscore the importance of all measures that bolster existing regional and international frameworks on international security, arms control, disarmament and non-proliferation.

The legitimate and peaceful uses of cyberspace, digital resilience and the possibilities offered by information technologies as enablers of sustainable development can be maintained and guaranteed only through multilateral means. The increasing and continued attention of the First Committee to that topic clearly attests to our trust in the priority role of the United Nations and of multilateralism. Here expectations are high, but the threats and challenges will be of a higher level still if we do not manage to guarantee an architecture for the digital environment of the future.

My delegation commends the progress made towards the inclusion of a gender perspective in various resolutions of the United Nations and in multilateral treaties linked to the First Committee. Like other delegations, we believe that the full, equal and significant participation of women in disarmament and non-proliferation efforts are key to achieving sustainable peace. We will continue to promote and support those initiatives that are aimed at increasing the participation of women in decision-making processes in that area. For that reason, this year, as in the past, we are pleased to co-sponsor draft resolution A/C.1/77/L.18, entitled “Women, disarmament, non-proliferation and arms control”.

Likewise, Mexico remains firmly committed to disarmament education as a means of prevention. We believe that that strategy promotes awareness about the impact of the use of any kind of weapon on society and our environment. It also educates younger, interested generations as new agents of change in the areas of disarmament and international security.

We are pleased this year once again to submit biannual draft resolutions on the United Nations Disarmament Information Programme (A/C.1/77/L.20) and the United Nations study on disarmament and non-proliferation education (A/C.1/77/L.15). We hope that those drafts will receive the support of all delegations.

Finally, we are pleased to see three Mexicans participating in the “#Leaders4Tomorrow” initiative, and we hope that those inspiring projects will reach many more young people so that they can disseminate information on the importance of disarmament in their own communities.

Mr. Tun (Myanmar): Myanmar associates itself with the statements delivered on behalf of the Movement of Non-Aligned Countries and the Association of Southeast Asian Nations (see A/C.1/77/PV.18).

There is no doubt that various aspects of our lives would grind to a halt in the absence of information and communications technology (ICT). The exponential growth of ICTs has enabled us to embrace unprecedented opportunities and socioeconomic developments, benefiting everyone all over the world, including even those who have no access to or have very limited understanding of ICTs.

At the same time, cyberspace is becoming more and more susceptible to malicious actors and non-State actors, whose complex capabilities are growing at the same pace as ICTs themselves. Pervasive cyberthreats, which are transboundary, elusive and evolving, have serious consequences for international peace and security and our day-to-day lives. Cyberspace has already become a forum for warfare, as we have witnessed over the past two decades.

Thus it is imperative for all of us to use international norms and standards as guides to minimize cyberthreats and maximize the positive benefits of ICTs. In that regard, Myanmar wishes to underscore the principal role of the United Nations and the multilateral efforts of Member States in addressing cybersecurity challenges and in constructing a secure and stable security environment. Accordingly, Myanmar reiterates its support for the work of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies for the period 2021 to 2025 and welcomes the adoption of the first annual progress report by consensus in July 2022.

We call for all parties to work together in good faith and with maximum flexibility for the continued progress of the OEWG. We also deeply appreciate the important work of the Group of Governmental Experts (GGE), which has provided valuable inputs in that area.

We condemn the use of ICTs as a weapon to suppress fundamental rights and freedom of expression. In Myanmar, my home country, a free, secure and open Internet is no longer feasible, as the military junta is exercising a digital dictatorship. Wiretapping and cyberattacks against its own people, including Myanmar nationals living abroad, is the new norm. The junta has actively monitored the social media activities of civil servants. The junta is also attempting to enact a draconian cybersecurity law that is specifically designed only to eliminate any dissent or expression against the military junta. We urge the international community and the technology industry to help in putting an end to the junta's misuse of ICTs as part of its clinging to power.

I take this opportunity to draw your kind attention, Mr. Chair, to the recent heinous crimes committed by the fascist military regime against ethnic Kachin minorities. In the evening of 23 October, terrorist military fighter jets bombed and attacked a music concert being held in A Nang Pa, Brigade 9 of Kachin Independent Army in Kachin state, Myanmar, to celebrate the anniversary of the sixty-second Kachin Independent Organization Day, which falls on 25 October. That reportedly resulted in the deaths of approximately 100 people, including artists, women and children, and many more injured. It clearly constitutes a crime against humanity and a war crime. It is not an isolated incident. Over the past 20 months, the terrorist military has carried out more than 250 air strikes against the civilian population across the country, including in ethnic areas, and committed several massacres. As long as the military retains its access to weapons and technologies, it will continue to commit its brutal and inhumane atrocities against the people, including children. I wish to ask those Member States that export deadly weapons and technology to the military to stop it immediately. We believe that will save the lives of the people of Myanmar.

In conclusion, we reaffirm our commitment to building a secure and peaceful cyberspace that prevents nefarious activities that undermine international peace and security and that promotes the application of international law, fundamental freedoms and human rights.

Mr. Balouji (Islamic Republic of Iran): My delegation associates itself with the statement delivered by the representative of Indonesia on behalf of the Movement of Non-Aligned Countries (see A/C.1/77/ PV.18).

The Islamic Republic of Iran once again reiterates its consistent position that cyberspace and the information and communications technology (ICT) environment, as a common heritage of humankind, must be used exclusively for peaceful purposes and that States must act cooperatively and in full compliance with applicable international law. Based on that viewpoint, Iran has been actively participating in the relevant intergovernmental negotiations processes, under the auspices of the United Nations, in the interest of the rights of all, while also establishing adequate responsibilities for all. Following the adoption of the first annual report of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies and a compendium of Member States' statements in explanation of position, including a statement by Iran, we believe that further progress and an increase in the Group's efficiency will hinge on the following.

First, it is essential, in future discussions, to consider and decide on the list of non-exhaustive and diverse proposals made on the elaboration of rules, norms and principles of responsible State behaviour, as reflected in the Chair's summary contained in the 2021 OEWG report.

Secondly, according to the OEWG's mandate, regular institutional dialogue should be established under the auspices of the United Nations, with the broad participation of States. In that regard, all national initiatives should be treated equally, while taking into account the concerns and interests of all States.

Thirdly, we call on States to continue to constructively engage in the negotiations during further activities of the Group, including in the intersessional period.

Fourthly, we call on the OEWG to establish, in line with its mandate, thematic subgroups to fulfil its mandate and facilitate the exchange of views among States and develop subsequent reports through text-based negotiations. From another perspective, and given the realities on the ground, it is important to note that not only have countries such as the United States started weaponizing cyberspace, but their militaries have also begun carrying out multiple cyberattacks. The Israeli regime has also launched many cyberattacks against Iran.

My country has long been the primary target and main victim of cyberattacks on its vital infrastructure, which have disrupted the delivery of public services and Government functions. Attacks by Stuxnet on Iran's peaceful nuclear facilities, as well as recent attacks on industrial infrastructure, such as its steel and petrochemical industries, gas stations and municipal public service systems, are just a few examples of such cyberattacks. The Israeli regime has repeatedly admitted its involvement in those internationally wrongful acts, using the ICT environment, and has received the unwavering support of the United States. We condemn all those attacks and urge the international community to hold those attackers responsible.

Regrettably, Iran was recently subjected to false and unwarranted blame for the alleged cyberattack. We reject any fictitious claims based on fabrications and wrong assumptions levelled at us for political agendas. Given the nature and technical characteristics of cyberspace and the challenges of attribution in the ICT environment, Iran warns of the negative consequences of falsified and forged attribution to States. If the United Kingdom were truly worried about any potential effects on security, economic, societal and humanitarian conditions, it would refrain from making hasty claims that could spread false information.

In conclusion, for the Islamic Republic of Iran the best way to guarantee a safe and secure ICT environment is to develop further international legal norms and rules concerning the prevention of the use of ICT and cyberspace for malicious purposes, as well as the peaceful settlement of disputes, in a legally binding instrument.

The Chair: I now give the floor to the observer of the Holy See.

Archbishop Caccia (Holy See): Pope Francis, in his encyclical letter, *Fratelli Tutti*, wrote that the ever-increasing number of interconnections and communications in today's world makes us powerfully aware of the unity and common destiny of nations. However, that unity is threatened by the growing malicious use of information and communications technology (ICT) by State and non-State actors alike. Such malicious use of ICTs stems in part from the fact that our immense technological development has not been accompanied by a development in human responsibility, values and conscience. In that regard, the Holy See welcomes the convening of the Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies, which provides an apt opportunity to correct that imbalance. My delegation has followed those meetings with great interest and, going forward, will continue to actively engage in its deliberations. The network of interconnected systems that makes up cyberspace constitutes a shared environment, whose maintenance requires all of us to shift from the paradigm of competition to one of cooperation. Undertaking such a shift calls for a set of common principles. With that in mind, allow my delegation to share a few considerations.

First, States' behaviour in cyberspace must respect the inherent dignity found in each human person. To that end, States must promote and protect every individual's freedom of expression online. Such freedom, which is essential for one's own quest for truth, also has its limits, being bound by the moral order and the common interest. Upholding human dignity in cyberspace obliges States to also respect the right to privacy by shielding citizens from intrusive surveillance and allowing them to safeguard their personal information from unauthorized access.

Secondly, States must ensure that those finding themselves in the most vulnerable situation are protected from harm. That means not only protecting one's own critical infrastructure, such as hospitals, water supply systems, power plants and facilities that contain dangerous forces, but also refraining from any activity that intentionally damages another State's critical infrastructure.

Thirdly, States must be guided by justice in their actions in cyberspace, which requires that States in a position to do so effectively contribute to efforts to bridge the digital divide. Such a divide not only leads to uneven patterns of human development but also creates cybervulnerabilities that threaten all countries. To address those vulnerabilities, the Holy See encourages capacity-building efforts to benefit those States that do not have an equal share in the fruits of the digital revolution. Such capacity-building should remain politically neutral and without conditions.

Humankind has entered a new era in which our technical prowess has brought us to a crossroads that offers us both great promise and risk. Ensuring that new advances in the field of ICTs contribute to integral human development requires us to continually evaluate how new tools can be applied in a manner that upholds human dignity. It is the hope of my delegation that such efforts, as well as the Open-Ended Working Group's further elaboration of responsible State behaviour, can enable us to rejoice in those advances and to be excited by the immense possibilities that they continue to open up before us.

The Chair: The Committee has heard the last speaker on the cluster “Other disarmament measures and international security”.

I shall now call on those who have requested to exercise the right of reply. In that connection, I would like to remind delegations of the time limitations and request that they be conscious of them.

Mr. Shin (Russian Federation) (*spoke in Russian*): I would like to exercise the right of reply in response to the hostile rhetoric contained in some of the statements we heard today.

I must admit that I was rather disturbed by the statements delivered by the representatives of the United States, the European Union, the United Kingdom, Australia and a number of other States, in which they affirmed their support for the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies for the period 2021 to 2025 and spoke about the positive aspects of that mechanism. I clearly remember that it was those very countries that voted against the establishment of the Open-Ended Working Group — and not just once, but twice. Does that mean that they are not telling the truth now? Why should we believe their words or actions? Now they assertively promote draft resolution A/C.1/77/L.73, on a programme of action on cyber-related matters, saying they do so in the interests of the OEWG. I would like to ask them to clarify exactly what they are talking about. The more we hear about the programme of action, the more questions we have.

We do not understand why United Nations States Members are being asked to first create that format and then afterwards decide what it is going to actually do, including the decision-making mechanism and the financing of that process. We are essentially being asked to put the cart before the horse. Why not first discuss that initiative in the framework of the OEWG, in full compliance with its mandate and previous consensus agreements? We believe that a period of three years, until 2025, is more than enough time to jointly develop an understanding of the feasibility of creating such a format and its potential scope and modalities.

Frankly, the actions of France and its partners seem like an attempt to create a mechanism that would be suitable only for a few, predominantly the Western States. In that context, they would be making decisions and then imposing them on the large majority. Frankly, in that regard, such an initiative resembles a manifesto of cybercolonialism. The decision for non-State entities to participate in the OEWG is, as we all know, the sovereign right of States.

The applications of many Russian organizations were also rejected without explanation. In our opinion, before talking about allowing non-governmental organizations to take part in inter-State negotiation processes, we should first ensure the unhindered access of States and their national delegations to the United Nations platform. In that connection, we would like to strongly protest against the actions of the Government of the United States, which through its use of visas as a weapon has systematically violated its obligations as the host State to United Nations Headquarters.

We continue to hear absolutely unfounded accusations against Russia with regard to cyberaggression, including in the context of the special military operation in Ukraine. Instead of using the established channels of communication of the relevant agencies, our Western colleagues have taken to coming down on certain States they dislike based on unfounded claims, distracting the global public from their own actions. The goal of their rhetoric is to cover up an unprecedented cyberaggression campaign against Russia and other States. There is a great deal of evidence showing that there have been systematic, aggressive activities in cyberspace carried out by the intelligence services of the United States and NATO countries. I recall the revelations by Edward Snowden and, as another example, the recent report published by our Chinese colleagues about the cyberattacks against Northwestern Polytechnic University, which were carried out with the direct participation of the United States National Security Agency. They do not hide their efforts to practice cyber warfare and conduct exercises, inviting representatives from outside of their bloc to attend them. Moreover, the Commander of United States Cyber Command, Paul Nakasone, has publicly acknowledged that his country is carrying out offensive cyberoperations against Russia, including, primarily, by using the information technology army of Ukraine, which was created by the Americans themselves.

Since the beginning of this year, the number of attacks on Russian network resources has increased more than fourfold as compared to the same period last year. Most of those attacks originate in the United States or in European Union countries. The scale of the cyberaggression shows that it is carried out in a coordinated manner by the Governments of Western countries, in cooperation with hacker communities and private companies. Unfortunately, I do not have enough time to fully go into detail on that topic, but it is important to understand that an escalation of tensions in cyberspace is not in the interests of the international community, which are better served by the prevention of conflict and the use of information and communications technologies for peaceful purposes and development.

Mr. Kim Song (Democratic People’s Republic of Korea): My delegation feels compelled to take the floor to exercise its right of reply in response to the reckless remark made by the representative of the United Kingdom.

We categorically reject the baseless allegation levelled by the United Kingdom at the Democratic People’s Republic of Korea. We are well aware of the United Kingdom’s bad habit of recklessly accusing others without any specific evidence. On the other hand, the United Kingdom is actively involved in different kinds of malicious acts in cyberspace through tools such as the Five Eyes to interfere in the internal affairs of sovereign States. The United Kingdom’s allegation is like a guilty party filing a lawsuit first.

We expect nothing different from the United Kingdom, which blindly follows in the footsteps of the hostile United States policy against the Democratic People’s Republic of Korea, which is aimed at demonizing our country in the international arena and enforcing so-called international cooperation to bring pressure to bear on the Democratic People’s Republic of Korea. The United Kingdom’s groundless allegation clearly reveals its extreme prejudice and hostility against the Democratic People’s Republic of Korea. We strongly urge the United Kingdom to come back to its senses and reflect on its reckless and outrageous behaviour.

Mr. Li Song (China) (*spoke in Chinese*): China takes note of the representative of the United Kingdom’s groundless accusations against China’s cyberactivities and firmly opposes those accusations.

China is firmly committed to preserving cybersecurity. It is also a major victim of cyberattacks. The Government of China firmly opposes and combats all forms of cyberattacks in accordance with the law, which fully demonstrates our responsible attitude in the field of cybersecurity.

China would like to stress that cybersecurity is a common challenge facing all countries. All countries should, on the basis of mutual respect, equality and mutual benefit, pursue dialogue and cooperation in order to jointly respond to threats to cybersecurity. We urge the relevant countries to cease their slander and groundless accusations against China on the issue of cyberattacks and to effectively adopt a responsible attitude, working together with all parties to safeguard peace and security in cyberspace.

Mr. Bourgel (Israel): I am compelled to take the floor with regard to the references concerning my country made by the representative of the Islamic Republic of Iran. Israel rejects those fraudulent allegations. Judging by Iran’s behaviour in the cyberdomain, and especially lately with the dangerous cyberattack on Albania’s infrastructure, its remarks are no less than absurd.

On this matter, allow me to also condemn the two recent cyberattacks on United Nations peacekeeping operations, both of which were carried out by the Iranian regime and its proxies. As with so many issues the Committee discusses, Iran is systematically working against the international community to bring about the collapse of arms control forums. Just as Iran sponsors and supports terrorist groups in order to raise fear among States throughout the region, it attempts to use malicious tools in the domain of information and communications technology, as well as in order to create fear and destruction among States worldwide.

Ms. McIntyre (France) (*spoke in French*): I wish to exercise my country's right of reply in response to the remarks made by the delegation of the Russian Federation with regard to draft resolution A/C.1/77/L.73, submitted by my country, on a programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.

As members are aware, France proposed — to all United Nations States Members, in a transparent and open manner — a draft resolution aimed at creating a programme of action for capacity-building on cyber-related matters. The draft resolution was discussed openly and at length during four rounds of open consultations held here in New York and previously in Geneva. The draft resolution has been improved considerably in order to take into account the many proposals that were made by delegations, for which we are most grateful.

The draft resolution is based on the consultations previously held to establish the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects. I would remind members of the process observed in that regard, which involved first a report by the Secretary-General and subsequently two years of consultations aimed at taking into account the suggestions of all Member States with regard to the content of the Programme of Action. Finally, the Programme of Action was adopted at an international conference held at the end of the process. That is precisely the sequence of events that we propose to follow in the consideration of draft resolution A/C.1/77/L.73, entrusting the Secretary-General with the task of presenting a report next year specifying the modalities and content of the future programme of action, all while fully respecting the prerogatives of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies for the period 2021 to 2025, which will of course also have to discuss the modalities of the programme of action before Member States to proceed with its adoption, if they so wish.

Therefore, I would recall that our process is open, transparent and inclusive and is aimed at respecting the entire process agreed upon by Member States, including within the OEWG. We will continue to adopt that transparent and inclusive approach until discussions are concluded.

Mr. Balouji (Islamic Republic of Iran): I am compelled to take the floor to reject the allegations made by the Israeli representative against my country.

We are not surprised by those lies proliferated by the representative of the regime, as it has no respect for international law. It has continuously initiated cyberattacks against many sectors in Iran, from peaceful nuclear facilities to public services such as emergency aid. We are well aware of the oppressive and apartheid nature of the Israeli regime, its dark record with regard to human rights and its disrespect for the international calls to join the Treaty on the Non-Proliferation of Nuclear Weapons, the Chemical Weapons Convention and the Biological Weapons Convention, among others.

Israel has violated 29 Security Council resolutions, which are legally binding on Member States under Article 25 of the Charter of the United Nations, including resolutions 54 (1948), 111 (1956), 233 (1967), 234 (1967), 236 (1967), 248 (1968), 250 (1968), 252 (1968), 256 (1968), 262 (1968), 267 (1969), 270 (1969), 280 (1970), 285 (1970), 298 (1971), 313 (1972), 316 (1972), 468 (1980), 476 (1980) and — last but not least — resolution 2231 (2015), which it has missed no opportunity and spared no effort to kill. Such a regime has no moral ground to talk about respect for the rules of and commitment to international law.

When it comes to cybersecurity, the situation is even worse. What we have said are not allegations, as all international observers have confirmed Israel's irresponsible actions, which we firmly condemn.

The Chair: We have heard the last speaker in the exercise of the right of reply.

We have a little bit of time on our hands, so let us try and maximize the use of those few minutes. Permit me the indulgence of taking up the cluster "Regional disarmament and security". We have a long list of speakers for the cluster, so I appeal for delegations' full cooperation.

Ms. Kristanti (Indonesia): I am honoured to speak on behalf of the Movement of Non-Aligned Countries (NAM).

NAM reiterates its strong concern at the growing resort to unilateralism, and in that context underlines that multilateralism and multilaterally agreed solutions, in accordance with the Charter of the United Nations, provide the only sustainable method of addressing disarmament and international security issues. NAM also underscores its principled position concerning the non-use or threat of use of force against the territorial integrity of any State.

NAM States parties to the Treaty on the Non-Proliferation of Nuclear Weapons are deeply concerned by the strategic defence doctrines of the nuclear-weapon States and certain non-nuclear-weapon States that subscribe to extended nuclear security guarantees provided by the nuclear-weapon States. Those not only set out rationales for the use or threat of use of nuclear weapons, but also maintain unjustifiable concepts of international security based on promoting and developing military alliances and nuclear deterrence policies. NAM therefore urges the States concerned to completely exclude the use or threat of use of nuclear weapons from their military and security doctrines.

NAM reiterates its full support for the establishment in the Middle East of a zone free of nuclear weapons and all other weapons of mass destruction. As a priority step to that end, NAM reaffirms the need for the speedy establishment of a nuclear-weapon-free zone in the Middle East in accordance with Security Council resolution 487 (1981) and paragraph 14 of Security Council resolution 687 (1991), as well as the relevant General Assembly resolutions. NAM calls upon all parties concerned to take urgent and practical steps towards the fulfilment of the proposal initiated by Iran in 1974 for the establishment of such a zone.

NAM States parties to the NPT reiterate their profound disappointment that the 2010 action plan on the establishment of a Middle East zone free of nuclear weapons and all other weapons of mass destruction has not been implemented. They strongly reject the alleged impediments to implementing the 2010 action plan on the Middle East and the 1995 resolution on the Middle East. NAM re-emphasizes the special responsibility of co-sponsor States of the 1995 resolution on the Middle East in implementing that resolution. NAM is concerned that the persistent lack of implementation of the 1995 resolution, contrary to the decisions made at the relevant NPT review conferences, undermines the effectiveness and credibility of the NPT and disrupts the delicate balance between its three pillars.

In that regard, NAM welcomes the convening of the first session of the Conference on the Establishment of a Middle East Zone Free of Nuclear Weapons and Other Weapons of Mass Destruction, in accordance with decision 73/546, presided over by the Hashemite Kingdom of Jordan, and the Conference's adoption of a political declaration. NAM also welcomes the convening of the second session of the Conference presided over by the State of Kuwait and its outcomes, including, inter alia, the adoption of the rules of procedure and establishing an informal working committee. Furthermore, NAM looks forward to the third session of the Conference and continues to call upon all States of the region, without exception, to actively participate in the Conference, negotiate in good faith and bring to a conclusion a legally binding treaty on the establishment of the zone.

NAM believes that nuclear-weapon-free zones established by the Treaties of Tlatelolco, Rarotonga, Bangkok and Pelindaba, the Central Asian Nuclear-Weapon-Free Zone Treaty and Mongolia's nuclear-weapon-free status are positive steps and important measures aimed at strengthening global nuclear disarmament and nuclear non-proliferation. In the context of nuclear-weapon-free zones, it is essential that nuclear-weapon States provide unconditional assurances against the use or threat of use of nuclear weapons to all States of the zones under all circumstances. NAM calls upon all nuclear-weapon States to ratify related protocols to all treaties establishing nuclear-weapon-free zones, withdraw any reservations or interpretative declarations incompatible with their object and purpose, and respect the denuclearization status of these zones. NAM urges States to conclude agreements freely arrived at among the States of a region concerned with a view to establishing new nuclear-weapon-free zones in regions where they do not exist.

In conclusion, NAM emphasizes the importance of United Nations activities at the regional level to increase the stability and security of its Member States, which could be promoted in a substantive manner by the maintenance and revitalization of the three regional centres for peace and disarmament.

Mr. Fuller (Belize): I have the honour to speak on behalf of the 14 States members of the Caribbean Community (CARICOM) on the regional disarmament and security cluster.

The member States of CARICOM have adopted a cooperative, coordinated and practical approach at the regional and subregional level to tackle the various security threats posed to the region. CARICOM is fully committed to playing its part in the global efforts to maintain our collective security by implementing our international obligations. Serious efforts aimed at regional disarmament complement our global efforts.

Security is an integral pillar of our regional integration. CARICOM has established a regional institutional framework to support regional cooperation inclusive of the CARICOM Implementation Agency for Crime and Security (CARICOM IMPACS) with oversight from the Council of Ministers of Security and Law Enforcement and complemented by other regional institutions, including the Regional Security System.

The illicit flows of firearms and ammunition through the region remains a major challenge and is identified as a tier one threat in the CARICOM Regional Security Strategy. Out of every 10 homicides in the region, 7 occur through the use of small arms and light weapons. It is estimated that more than half a million illegal firearms are in circulation in Haiti alone. Illegal firearms play a key role in all aspects of transnational organized crime and as a tool to support criminal and deviant behaviour. It therefore has a profound socioeconomic impact and human cost.

No CARICOM member State is either a manufacturer or major importer of firearms. It is a high priority for the region to disrupt and prevent illegal firearms and ammunition passing through our borders. Despite numerous initiatives and mechanisms aimed at addressing the problems of armed violence, high levels of gun crime persist in the region.

The CARICOM Crime and Security Strategy notes that while the region respects the rights of other States to establish liberal policies on access to guns, the negative impacts of these gun policies are not confined to their borders. They have very serious consequences for other countries, including CARICOM member States. Preventing the illicit trafficking in guns is therefore a responsibility to be shared not only among CARICOM States but also the countries that are the sources of these weapons. Our Heads of Government at its forty-third regular meeting, held in Suriname on 3 July 2022, further expressed particular concern about the inflow of guns from outside the region.

In 2020, CARICOM leaders adopted a road map for implementing the Caribbean priority actions on the illicit proliferation of firearms and ammunition across the Caribbean in a sustainable manner by 2030 (Caribbean Firearms Roadmap). CARICOM IMPACS is taking several concrete measures to implement the Roadmap, including providing technical and advisory assistance to national authorities, capacity-building and training, information- and intelligence-sharing, border and customs control, legislative support through development of model laws, provision of operational tools and the elaboration of international, regional and national regulatory frameworks, policies and standards.

We wish to highlight the work of IMPACS in the region with the support of partner Governments and organizations including development of a comprehensive, evidence-based study of the illicit arms trafficking to and within the Caribbean and the socioeconomic costs of this trafficking with the Small Arms Survey (SAS); establishment of a CARICOM Crime Gun Intelligence Unit to assist CARICOM member States in investigating and prosecuting firearms-related crimes, which will be supported by such agencies of the United States Government as the Bureau of Alcohol, Tobacco, Firearms and Explosives, Homeland Security Investigations and Customs and Border Protection; provision of assistance to CARICOM member States in firearms and ammunition management; establishment of critical partnerships with numerous international agencies to assist with the fight against gun crime, including INTERPOL, the World Customs Organization (WCO), the United Nations Office on Drugs and Crime, the United Nations Regional Centre for Peace, Disarmament and Development in Latin America and the Caribbean (UNLIREC), the SAS and the Mines Advisory Group; joint operations with Interpol to conduct Caribbean-wide joint firearms operations in partnership with INTERPOL from 24 to 30 September 2022, which led to the seizure of some 320 weapons, 3,300 rounds of ammunition and record drug hauls across the Caribbean; provision of training and capacity-building to law-enforcement and security institutions, including customs institutions, in partnership with WCO; support for member States in utilizing the Regional Integrated Ballistic Information Network; enhancement and expansion of the CARICOM Advance Passenger Information System, which is the world's only multilateral system that allows States to effectively verify persons of interest on board an aircraft or vessel at each port of entry in participating States, to ensure inclusion of all CARICOM member States and interested third States; establishment of a regional advanced cargo information system to support participating CARICOM member States in enhanced cargo targeting; and develop a Model Arms Trade Treaty Law.

The United Nations Regional Centre for Peace, Disarmament and Development in Latin America and the Caribbean continues to be an important partner for CARICOM. The Regional Centre is the co-custodian, along with IMPACS, for the implementation of the Caribbean Firearms Roadmap. UNLIREC conducted 54 activities in the region to contribute to the implementation of the Roadmap, in which 600 officials — of whom 220 were women — participated. The Centre also assisted with the drafting of national action plans to implement the Roadmap and to monitor and evaluate the progress of implementation. To date, 10 Caribbean States have drafted their national action plans.

The region also benefited from a number of webinars and training sessions on various matters, including international best practices for criminal investigators, forensic examination of privately made firearms, enhanced firearms investigative techniques and ballistics intelligence management.

CARICOM joins the call of the Secretary-General for Member States and other partners to provide financial and in-kind support to the Centre.

CARICOM considers the Arms Trade Treaty (ATT), the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, the International Tracing Instruments (ITI) and other applicable United Nations small arms and light weapons resolutions as critical instruments to prevent, control and eradicate the illicit trade of small arms and light weapons and associated ammunition in all its aspects. CARICOM encourages all States to fully implement the provisions of those instruments.

One of the major challenges faced by small island developing States in implementing the small arms and light weapons instruments is a lack of adequate resources and technical capacity. For the full and effective implementation of the ATT, the Programme of Action and the ITI, international cooperation and assistance should be treated as a partnership among developing States, developed States and donor States, anchored in national ownership. We therefore stress the importance of rendering unconditional and non-discriminatory assistance to developing countries, upon their request, to strengthen their capacity to effectively implement the provisions of the international disarmament instruments.

One of the major challenges faced by developing States, including in CARICOM, in implementing the ATT, the Programme of Action and the ITI is the lack of technology transfer and lesson-sharing regarding its implementation. The need to redouble efforts to address this imbalance is critical for enhancing small arms and light weapons controls and reducing the technological digital divide between developed and developing States.

Recognizing that cybersecurity is now integral to regional security and, if not addressed urgently, could severely hamper the social and economic development of our Caribbean States, the region has developed a CARICOM CyberSecurity and Cybercrime Action Plan. The Plan seeks to address the cybersecurity vulnerabilities in each participating Caribbean country and to establish a practical, harmonized standard of practices, systems and expertise for cybersecurity to which each Caribbean country could aspire in the short and medium terms. It also seeks to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of cybercrime and possible linkages to other forms of criminal activity.

Although our region has limited resources with which to confront the various complex security challenges resulting from porous borders, expansive maritime and land boundaries in a geographic location that is in a transit zone, we have developed a number of partnerships to give realization to regional disarmament through a number of practical measures.

The Chair: We have exhausted the time available for this meeting. The Committee will reconvene tomorrow morning, when we will first hear a briefing by the Chair of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies. Thereafter, we will continue the discussion under the cluster “Regional disarmament and security”.

I would like to remind members that, at the end of its morning meeting tomorrow, the Committee will hold its traditional certificate awards ceremony for graduating disarmament fellows.

The meeting rose at 6.05 p.m.