



General Assembly

Distr.: General
12 August 2025
English
Original: Arabic/English/French/
Russian/Spanish

Open-ended working group on security of and in the use of information and communications technologies 2021–2025

Eleventh substantive session

New York, 7–11 July 2025

Compendium of statements in explanation of position on the adoption of the final report of the open-ended working group as contained in [A/80/257](#), annex

Note by the Secretariat

1. On 11 July 2025, at its eleventh substantive session, the open-ended working group on security of and in the use of information and communications technologies 2021–2025 considered item 8 of its agenda ([A/AC.292/2021/1](#)), entitled “Adoption of the final report”. The working group adopted its draft report and decided to include in its report the outcome of the discussions of the working group on agenda item 5. The report of the working group, including the annexed report on discussions on agenda item 5, is contained in document [A/80/257](#).
2. Pursuant to paragraph 19 of the report of the working group, the Secretariat has compiled the following compendium of statements in explanation of position, as received from delegations.*

* Circulated in the languages of submission only and without formal editing.



Contents

	<i>Page</i>
I. Member States	3
Argentina	3
Australia	4
Brazil	5
Cuba	5
Egypt	6
El Salvador	7
Iran (Islamic Republic of)	11
Ireland	12
Israel	13
Malta	14
Nicaragua (joint statement of the Group of Like-Minded States: Belarus, China, Cuba, Eritrea, Iran (Islamic Republic of), Nicaragua, Niger, Russian Federation, Sudan, Venezuela (Bolivarian Republic of) and Zimbabwe)	14
Nicaragua	15
Niger	16
Republic of Korea	17
Russian Federation	17
Switzerland	22
Tunisia (on behalf of the Arab Group)	24
United States of America	25
II. European Union	26

I. Member States

Argentina

Sr. Presidente,

Hago uso de la palabra para realizar una explicación de posición con relación al Informe Final del Grupo de Composición Abierta sobre Seguridad de y en el Uso de las TICs, cuyo consenso acompañamos y felicitamos a todos por su adopción.

Respecto de la palabra género, la Argentina la entiende en el marco del derecho internacional, que se refiere a los dos sexos, masculino y femenino, conforme Estatuto de Roma, Art. 7.3).

El compromiso de la Argentina con los derechos de la mujer es sostenido en el tiempo y está plasmado en su legislación y en prácticas internas que van más allá de los estándares internacionales.

En cuanto a la Agenda 2030, la República Argentina recuerda que dicha Agenda está compuesta por aspiraciones jurídicamente no vinculantes que cada Estado, en el ejercicio de su soberanía, tiene derecho a interpretar y perseguir con libertad.

Sr. Presidente:

Deseo expresar nuestro reconocimiento por la conducción eficaz, transparente e inclusiva de los trabajos de este Grupo a lo largo de los cinco años de mandato. Valoramos especialmente el impulso brindado a una participación sustantiva de todas las delegaciones, así como el profesionalismo de la Secretaría de la UNODA y la labor de los intérpretes, cuyo apoyo técnico fue esencial a lo largo del proceso.

Destacamos que los aportes realizados por los Estados se reflejan de manera equilibrada en el documento final, como resultado de un ejercicio genuino de negociación. Ello confirma el compromiso colectivo con el mantenimiento de un ciberespacio abierto, interoperable, estable, seguro y pacífico. Nos complace especialmente la incorporación de un grupo temático dedicado sobre creación de capacidades, una propuesta que ha contado con el firme respaldo de mi delegación y de numerosos países de nuestra región a lo largo de todo el proceso.

Consideramos que el informe final representa un aporte significativo al fortalecimiento del marco multilateral en materia de ciberseguridad y ciber resiliencia. Su adopción consolida el acquis logrado durante más de dos décadas de trabajo multilateral, conformado por creación de capacidades, principios, normas, medidas y entendimientos que seguirán guiando los avances en el marco internacional para el uso y la seguridad del uso de las TICs.

Sr Presidente, el mecanismo que hoy se establece como resultado del esfuerzo colectivo y sostenido de la Presidencia, la Secretaría y la sala, tendrá la responsabilidad de consolidar los avances alcanzados hasta la fecha, preservando el espíritu de consenso, transparencia y representatividad que ha caracterizado a este proceso.

La presente explicación de posición ha sido remitida a la Secretaría para su publicación.

Muchas gracias.

Australia

Thank you Chair.

Australia aligns with the Pacific Islands Forum statement and wishes to make the following remarks in our national capacity.

Australia expresses its sincere appreciation to you and your dedicated team for your leadership throughout this process. The adoption of the Final Report and the establishment of the new permanent mechanism, by consensus, represents a significant milestone in our collective efforts to uphold the rules-based international order and the framework for responsible state behaviour in cyberspace.

This outcome underscores the enduring value of multilateralism and reaffirms the central role of the United Nations in facilitating dialogue, fostering understanding, and enabling Member States to navigate new and complex challenges together. It reflects the determination of our Chair, the importance that all governments place on this issue, and the collective commitment demonstrated by every delegation throughout these negotiations.

While certain elements of the Final Report do not fully align with Australia's national positions, we acknowledge the finely balanced package to achieve consensus. In the spirit of cooperation and flexibility, we accept the outcome that has been reached.

Australia believes the Final Report provides a strong foundation for the work ahead. It consolidates decades of work since the first GGE and sets a clear direction for the new permanent mechanism to advance the framework for responsible state behaviour in cyberspace.

As we take stock of our progress, Australia notes two major disappointments on the Final Report.

Firstly, on international law, Australia regrets that the section does not capture all the progress made, and the emerging convergences reached, over almost five years. Many states called for the inclusion of substantive additional language on the application of international human rights law, the law of state responsibility, and international humanitarian law, as reflected in the cross-regional paper on international law. While we appreciate the references to international law in paragraph 42, we regret that this paragraph makes no mention of international human rights law. We are also disappointed that reference to the ICT resolution of the 34th Conference of the International Red Cross and Red Crescent – an important consensus document – was deleted, as were the two OEWG cross-regional working papers, which remain important pieces of work.

Secondly, on stakeholders modalities, we regret that we were not able to make more progress on improving inclusiveness and transparency.

Australia welcomes the Final Report's recognition of the high level of participation by women delegates and the importance of integrating gender perspectives in our discussions.

We would particularly like to acknowledge the valuable contributions of the Women in International Security and Cyberspace Fellows, who delivered a quarter [24%] of the total statements, which has enriched our deliberations and strengthened the collective outcome.

Australia encourages all States to support the full, equal and meaningful participation of women, both within the new permanent mechanism and across the broader landscape of cybersecurity and international security.

In closing, Australia extends its sincere appreciation to all delegations, to our Chair, and to his exceptional team for their tireless efforts in achieving a consensus outcome. We look forward to continuing our work under the new permanent mechanism and advancing our shared goal to protect and promote a peaceful, stable and interoperable cyberspace for all.

Thank you Chair and congratulations to all.

Brazil

Mr Chair,

I would like to express the Brazilian delegation's deepest appreciation to you and your team for your outstanding work throughout the past five years, which culminated in the adoption of our final report this morning.

One of multilateralism's clichés is that a fair and balanced document is one that no delegation finds perfect, but with which everyone is equally unhappy. It is true that we would have liked a higher level of ambition in some sections, and especially regret that our final report does not adequately capture the richness of our discussions on international law – especially international humanitarian law. We also believe a dedicated thematic group on international law in the permanent mechanism would have been a good space to further advance those discussions. It would have also been our preference to have stronger modalities for stakeholder participation.

Nevertheless, we still have a fair and balanced document which is a meaningful addition to our acquis and an important contribution to the promotion of an open, safe, secure, stable, accessible, peaceful and interoperable ICT environment. Most importantly, it lays the groundwork for a seamless transition to a single-track permanent mechanism to address ICT security. We commend in particular its strong emphasis on capacity building, which includes the establishment of a dedicated thematic group on the issue in the permanent mechanism we have just created.

Achieving this by consensus in such challenging geopolitical circumstances is a testament to the crucial importance and effectiveness of multilateralism. We appreciate the flexibility shown by all delegations throughout this week, which allowed us to reach consensus and adopt our final report.

Brazil has been an active participant throughout this process, and you can count on us to continue our constructive engagement in the future mechanism.

On a final note, Brazil joins other delegations in thanking you for your extremely able leadership and unwavering commitment to a fair balance since the begging of this process. We must also acknowledge Clarice Lim, Matthew Wong and Gillian Goh from your team, and Katherine Prizeman and Virginia Browning from the Secretariat, for their exceptional work throughout the OEWG.

I thank you.

Cuba

Mr. Chairman:

We associate ourselves with the statement made by the delegation of Nicaragua on behalf of a group of like-minded countries.

We appreciate your intensive efforts to achieve the adoption of the final report of the Open-Ended Working Group on the security of information and

communications technologies and their use after five years of work. We also thank the professionalism of your team and the support of the Secretariat.

The agreement to establish a new intergovernmental mechanism, which will continue to operate by consensus and provide continuity to the regular institutional dialogue under the auspices of the United Nations, is a significant achievement.

The Cuban delegation worked actively to contribute to this, based on our firm commitment to the Working Group, a forum created at the proposal of Russia and a group of like-minded countries, including Cuba, to which we attach crucial importance, especially for developing countries.

We thank the delegations for their collaboration, which made this result possible, despite such diverse positions and intense days of debate.

Mr. Chairman:

With a view to the discussions within the framework of the new mechanism, we would like it to be noted that there is no common understanding on the supposed neutrality of ICTs, a notion mentioned in paragraph 26 of the final report.

At the same time, no attempt should be made to force the notion of the applicability of international humanitarian law to cyberspace. Given the concern that some States are developing offensive capabilities through the use of ICTs, we believe that, rather than tacitly consenting to the possibility of armed conflict in cyberspace, we should focus on the essential purpose of preserving ICTs for exclusively peaceful, development-oriented use.

We hope that, in this new stage that is now beginning, progress will be made in the development of legally binding obligations in the field of ICT security and use, which would facilitate common understandings of how international law applies to this domain, by addressing legal gaps and establishing clear obligations for all States. Cuba remains committed to actively contributing to this purpose.

Thank you very much.

Egypt

Mr. Chairperson,

1- We align with the statement delivered earlier by Tunisia on behalf of the Arab Group, as well as the statement delivered yesterday by Nigeria on behalf of the African group.

2- In the first intervention by the Egyptian delegation during this 11th meeting, we underscored that our main and key priority would be to ensure a seamless transition to a future permanent mechanism that can enable the continuation of a single-track, action-oriented and consensus-based UN-led process on security of and in the use of ICT, and not to open the space for a vacuum or competitive initiatives.

3- From this prism, Egypt joins consensus today around the draft report. We based our decision on number of considerations including the fact that this report complements the three annual progress reports previously adopted by consensus, and that the normative framework of responsible state behavior continues to be cumulative and evolving. We welcome also the steps taken at this report to reflect a more diverse and representative landscape of threats that captures the reality in different regions.

4- Nevertheless, and as explained on previous occasions, we continue to be deeply disappointed with some crucial points with this report and its annex.

5- The omission of a dedicated DTG on the application of international law in the context of cyber space is very alarming, and along with the significant reduction in the content of section D on international law, Egypt, like many others, is concerned with how the application of and compliance with respective international law obligations, including international humanitarian law, will be approached under the new global mechanism. It is important to indicate once again that our interest and commitment to discussions supporting respect to international law and the UN Charter, does not in any mean or way indicate conclusive preference or pre-empting a discussion of a legally binding instrument as an indispensable pathway.

6- As mentioned by the Arab Group, we will continue to advance this avenue at the upcoming review meeting, and request the Chairperson of the global mechanism to convene a focused round table on application of international law.

7- In addition, we maintain our view that the content and recommendations in relation to capacity building is significantly lower than our expectations. Without concrete and meaningful steps to establish a UN-led capacity building vehicle including through the voluntary fund and sponsorship program, and availing adequate, sufficient and predictable resources for this purpose, the discussion at DTG2 will not realize its desired potential. Making meaningful and prompt on this front will be crucial for the level of confidence and the credibility of the newly born mechanism.

Mr. Chairperson,

8- Having said that, we won't miss on paying tribute to your exemplary leadership. Chairperson, we have mentioned before and we are saying it again, you were the consistently serious and diligent participant in this process from its inception till its conclusion. Without your strong and impactful leadership, this process would have been in a very different place which is way less effective and ambitious. I want also to extend our gratitude to my two dear colleagues and friends from your team, Mathew Wong and Clarice Lim and the very dedicated team at the secretariat Ms Prizeman and Ms Browning.

9- Chairperson, thank you for taking us forward, at a time when consensus around progress at the UN is becoming the exception rather than the norm.

I thank you.

El Salvador

El Salvador expresa un profundo reconocimiento al Presidente del Grupo de Trabajo de Composición Abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (GTCA), a su equipo de trabajo, y a la Unidad de Ciencia y Tecnología de la Oficina de Asuntos de Desarme de las Naciones Unidas, por la excelente conducción de este proceso, que culminó con la adopción del Reporte Final por consenso.

Esta adopción no solo demuestra la voluntad de los Estados Miembros de las Naciones Unidas de seguir avanzado en la implementación del marco de comportamiento responsable de los Estados en el ciberespacio, sino que también allana el camino hacia el futuro establecimiento del Mecanismo Global sobre los avances en el ámbito de las TIC en el contexto de la seguridad internacional y el fomento de un comportamiento responsable en su uso, que nace como resultado directo del trabajo del GTCA.

El Salvador ha participado de manera activa y constructiva en las labores del GTCA desde su establecimiento, conforme al mandato conferido por la resolución

75/240 de la Asamblea General. Durante la décimo primera sesión sustantiva, que marcó el cierre del Grupo, la delegación salvadoreña participó activamente en la negociación del Reporte Final, presentando recomendaciones tanto a título nacional como en coordinación con grupos de países afines, particularmente en los pilares de derecho internacional y creación de capacidades.

El Salvador considera que el Reporte Final, adoptado por consenso, es un documento que preserva un delicado equilibrio de posiciones, que se construye sobre el trabajo realizado en sesiones anteriores y que además traza una hoja de ruta para el próximo Mecanismo Global.

Aunque varios de los elementos promovidos por El Salvador se reflejan en el Reporte Final, consideramos que algunos aspectos importantes que fueron respaldados por El Salvador no fueron incluidos, y sobre los cuales continuaremos abogando en el futuro.

Sobre amenazas reales y potenciales:

El Salvador lamenta que no se hayan retenido las referencias contenidas en los párrafos 15 y 16 del borrador inicial, que reflejaban de manera más precisa las interrelaciones entre el uso híbrido de las TIC y las armas convencionales, así como cómo la forma en que actividades delictivas e incidentes relacionados con las TIC pueden representar amenazas a la paz y la seguridad internacionales. Esperamos que el próximo Mecanismo Global pueda profundizar en estos temas.

En relación con el párrafo 17, expresamos nuestra preocupación por la eliminación de la mención específica a sectores previamente definidos como infraestructuras críticas. Los sectores sanitario, marítimo, aeronáutico, financiero, energético y del agua constituyen lenguaje acordado en el Tercer Reporte Anual, y su reconocimiento representa, desde nuestra perspectiva, un avance significativo en la identificación sectorial de riesgos y prioridades de protección.

Respecto del párrafo 24, lamentamos la eliminación de la referencia a un enfoque de ransomware centrado en las personas. Desde nuestra visión, dicho enfoque resalta la necesidad de comprender mejor los riesgos y mitigar los impactos del ransomware desde la perspectiva de las personas y comunidades afectadas.

Finalmente, El Salvador acoge con satisfacción la inclusión en el párrafo 26 de la referencia a avanzar en el desarrollo e implementación de soluciones criptográficas post-cuánticas, propuesta presentada por nuestra delegación en sesiones previas.

Sobre derecho internacional:

El Salvador reconoce la naturaleza evolutiva de las discusiones sobre la aplicación del derecho internacional en el ciberespacio. Junto con un grupo de más de 20 Estados, presentamos un documento conjunto sobre lenguaje de convergencia en esta materia.

Sin embargo, consideramos que la sección correspondiente del Reporte Final no refleja plenamente el alcance ni el tenor de las discusiones sostenidas en los últimos años. En particular:

- En el párrafo 40(c), se eliminó una referencia importante sobre cómo ciertas operaciones mediante TIC podrían constituir uso de la fuerza, cuando su escala y efectos sean comparables a los de medios tradicionales.
- En el párrafo 42(b), no se reflejan referencias a futuras áreas de discusión como las obligaciones relativas a la integridad territorial, la diligencia debida, y la protección de infraestructuras críticas y datos bajo el derecho internacional.

Nuestra delegación lamenta que la continuación de estas discusiones no se haya institucionalizado mediante un grupo de trabajo específico en el marco del futuro Mecanismo Global. Por ello, alentamos a que, de manera transversal, se continúe promoviendo la aplicación del derecho internacional en el ciberespacio y la armonización de criterios sobre su implementación. Los marcos normativos aplicables requieren una mayor convergencia y transparencia, a fin de crear condiciones seguras y estables en el ciberespacio, así como regular las conductas de los Estados, con todo lo que implica la responsabilidad en el cumplimiento de las obligaciones internacionales.

- Reiteramos nuestra preocupación por la ausencia de una referencia significativa a la aplicación del Derecho Internacional Humanitario (DIH) en el ciberespacio, especialmente respecto a las limitaciones a las ciberoperaciones en contextos de conflicto armado, la protección de infraestructuras críticas frente a ciberataques, y la reafirmación de que la aplicabilidad del DIH no legitima al ciberespacio como un dominio de conflicto.

Consideramos que esta omisión representa, aún más en el contexto geopolítico actual, una oportunidad perdida que esperamos pueda ser subsanada en el próximo mecanismo.

Sobre creación de capacidades:

El Salvador acoge con satisfacción el establecimiento de Grupo temático integrado, basado en los cinco pilares del marco, para acelerar el desarrollo de capacidades en materia de seguridad de las TIC, tal como se refleja en el Anexo I. Esta ha sido, de manera constante, una prioridad tanto para El Salvador como para varios países de América Latina y El Caribe.

No obstante, observamos con preocupación la eliminación de referencias claves y mecanismos esenciales para la operacionalización de esta área. Consideramos que un enfoque centrado en posibles reducciones debilita una sección clave para el trabajo futuro del mecanismo permanente.

Sobre los grupos temáticos:

En cuanto al establecimiento de los grupos temáticos reflejados en el Anexo I, reiteramos nuestra preocupación por la eliminación del grupo dedicado a continuar las discusiones sobre la aplicación del derecho internacional en el ciberespacio, una propuesta que nuestra delegación respaldó firmemente.

Asimismo, consideramos que la creación de un solo grupo temático que abarque todos los pilares del marco podría derivar en una generalización excesiva. La ausencia de una estructura temática claramente definida podría dificultar que las discusiones futuras sean sustantivas y efectivas.

Courtesy translation

El Salvador extends its deep appreciation to the Chair of the Open-Ended Working Group on the security of and in the use of information and communications technologies (OEWG), his team, and the Science and Technology Unit of the United Nations Office for Disarmament Affairs, for their excellent leadership of this process, which culminated in the consensus adoption of the Final Report.

This adoption not only demonstrates the will of United Nations Member States to continue advancing the implementation of the framework for responsible State behaviour in cyberspace, but also paves the way for the future establishment of the

Global Mechanism on developments in the field of ICTs in the context of international security and the promotion of responsible State behaviour in their use, which emerges as a direct outcome of the OEWG's work.

El Salvador has actively and constructively participated in the work of the OEWG since its establishment, in accordance with the mandate conferred by General Assembly resolution 75/240. During the eleventh substantive session, which marked the conclusion of the Group's work, the Salvadoran delegation actively engaged in the negotiation of the Final Report, submitting recommendations both nationally and in coordination with like-minded States, particularly in the pillars of international law and capacity-building.

El Salvador considers that the Final Report, adopted by consensus, preserves a delicate balance of positions, builds upon the work of previous sessions, and outlines a roadmap for the forthcoming Global Mechanism.

While several of the elements promoted by El Salvador are reflected in the Final Report, we consider that certain important aspects supported by our delegation were not included, and we will continue to advocate for them in the future.

On existing and potential threats:

El Salvador regrets that the references contained in paragraphs 15 and 16 of the zero draft were not retained, as they more accurately reflected the interlinkages between the hybrid use of ICTs and conventional weapons, as well as the ways in which criminal activities and ICT-related incidents can pose threats to international peace and security. We hope that the next Global Mechanism will explore these issues in greater depth.

Regarding paragraph 17, we express concern over the deletion of the specific reference to sectors previously defined as critical infrastructure. The health, maritime, aviation, finance, energy, and water sectors constitute agreed language from the Third Annual Progress Report, and in our view, their recognition represents a significant step forward in the sectoral identification of risks and protection priorities.

Regarding paragraph 24, we regret the removal of the reference to a people-centered approach to ransomware. From our perspective, such an approach underscores the need to better understand the risks and mitigate the impacts of ransomware from the perspective of affected individuals and communities.

Finally, El Salvador welcomes the inclusion in paragraph 26 of the reference to advancing the development and implementation of post-quantum cryptographic solutions, a proposal put forward by our delegation in previous sessions.

On international law:

El Salvador recognizes the evolving nature of discussions on the application of international law in cyberspace. Together with a group of more than 20 States, we presented a joint paper on convergence language in this field.

However, we consider that the relevant section of the Final Report does not fully reflect the scope or tone of the discussions held in recent years. In particular:

- In paragraph 40(c), an important reference was removed regarding how certain ICT operations could constitute a use of force when their scale and effects are comparable to those of traditional means.
- In paragraph 42(b), there is no reference to future areas of discussion such as obligations relating to territorial integrity, due diligence, and the protection of critical infrastructure and data under international law. Our delegation regrets

that the continuation of these discussions was not institutionalized through a dedicated working group under the future Global Mechanism. We therefore encourage that, in a cross-cutting manner, efforts continue to promote the application of international law in cyberspace and the harmonization of criteria for its implementation. Applicable legal frameworks require greater convergence and transparency to create safe and stable conditions in cyberspace and to regulate State conduct, with all that implies in terms of responsibility for compliance with international obligations.

- We reiterate our concern over the absence of a meaningful reference to the application of international humanitarian law (IHL) in cyberspace, particularly with respect to limitations on cyber operations in situations of armed conflict, the protection of critical infrastructure against cyberattacks, and the reaffirmation that the applicability of IHL does not legitimize cyberspace as a domain of conflict.

We consider that this omission, even more so in the current geopolitical context, represents a missed opportunity that we hope can be remedied under the next mechanism.

On capacity-building:

El Salvador welcomes the establishment of an integrated thematic group, based on the framework's five pillars, to accelerate the development of ICT security capacity, as reflected in Annex I. This has consistently been a priority for El Salvador and several Latin American and Caribbean countries.

Nevertheless, we note with concern the removal of key references and mechanisms essential to the operationalization of this area. We believe that an approach focused on potential reductions weakens a key section for the future work of the permanent mechanism.

On thematic groups:

Regarding the establishment of thematic groups reflected in Annex I, we reiterate our concern over the elimination of the group dedicated to continuing discussions on the application of international law in cyberspace, a proposal strongly supported by our delegation.

We also consider that creating a single thematic group covering all pillars of the framework could lead to excessive generalization. The absence of a clearly defined thematic structure could hinder the ability of future discussions to be substantive and effective.

Iran (Islamic Republic of)

Mr. Chair,

My delegation would like to express its sincere appreciation to you, your team, and the Secretariat for your dedicated, tireless, and professional efforts throughout the OEWG process. Your commitment to fostering an inclusive, transparent, and constructive dialogue has been instrumental in guiding our collective work and advancing progress on this complex and vital agenda. We commend your leadership in building consensus among Member States and in facilitating a smooth transition to the Global Mechanism.

My delegation aligns itself with the joint statement of the LMG Group, which will be delivered later today.

Mr. Chair,

While we welcome and appreciate the positive improvements introduced throughout various parts of the final report and acknowledge the progress made, my delegation remains disappointed that it does not fully reflect the entire range of the threat landscape, as it overlooks several threats highlighted by a number of States during the OEWG's deliberations, particularly those related to the responsibilities of the private sector and platforms with extraterritorial impact.

To address this significant gap and ensure a more balanced and comprehensive representation of the OEWG's mandate, my delegation put forward a compromise proposal to compile a list of threats identified by States throughout the OEWG process to serve as a valuable reference for the work of the Global Mechanism.

We continue to strongly believe that our proposal offers a constructive way to address this substantive shortcoming in the threat section.

In line with the final sentence of paragraph 14 of final report, which acknowledges the need to continue addressing the diverse landscape of ICT threats in a manner that reflects the realities of all countries and regions, my delegation will remain engaged in advancing the consideration of critical threats identified by a number of States, including my own, within the framework of the Global Mechanism.

Mr. Chair,

The consensus-based decision-making modality of the global mechanism is clearly articulated in Annex C of the Third APR, which states: "*The future permanent mechanism would take all decisions based on the principle of consensus. Based on consultations with States, decisions could be put forward by the Chair for adoption by States on a consensus basis.*" This language leaves no ambiguity regarding the intended approach: decisions within the future mechanism are to be made by consensus. Any interpretation that diverges from this agreed and fundamental principle would compromise the very foundation of the global mechanism and is therefore not acceptable.

I thank you, Mr. Chair.

Ireland

Chair

Ireland aligns with the EU statement but wanted to come in to thank you, your team, the secretariat and the translators for your extraordinary efforts both this week and over past years.

Your careful, thoughtful and effective chairmanship has led to this consensus outcome, threading the narrow pathway to success through the many conflicting opinions reflected here. This is a success for you, for us all, but also more broadly for the UN and for multilateralism.

Of course, there were points we would have liked to see in the text, in particular on International Law, IHL and IHRL, where we consider our many discussions in this process is not fully reflected in the text.

However, there is also much that is good in the text and which we strongly support.

What you have achieved here provides the base and tools from which we can build the new Global mechanism. We look forward to the challenging but vitally

important work to come in the new mechanism, drawing on the work done over the past 5 years.

We look forward to working with all here in that regard.

Thank you Chair.

Israel

Mr. Chair,

Israel wishes to express its sincere and profound appreciation to you, H.E. Ambassador Burhan Gafoor, and your very capable team, as well as to the devoted and highly professional UNODA Secretariat, for your steadfast leadership throughout this process, culminating today in the successful adoption of this consensus report.

This achievement underscores the fundamental importance of **consensus** as the cornerstone of our work. It is this spirit of inclusivity and shared ownership that has allowed us to advance a common understanding of responsible state behavior in cyberspace.

While some of our reservations remain unresolved, and not all of our concerns have been fully reflected in the final version of the CRP, we recognize the inherent value of compromise. In the spirit of consensus, and as a gesture of goodwill, particularly in light of the constructive cooperation demonstrated by many delegations over the past days, Israel is prepared to show flexibility. Accordingly, we join other delegations in supporting the adoption of this final report. We reaffirm that the Israeli delegation remains committed to working collaboratively with fellow Member States, and to maintaining a constructive and forward-looking approach in advancing an inclusive and transparent dialogue on cybersecurity within the UN framework.

As the mandate of the current OEWG concludes and we turn our attention to the establishment of a future permanent institutional dialogue, Israel underscores the need for **consensus to remain the guiding principle**, in all our decision-making processes on procedural and substantive matters alike. Upholding this principle leading to the creation of our new mechanism and while working in it is essential in ensuring that the interests and perspectives of all Member States are respected, and that our collective efforts are credible, balanced, and effective.

Israel further reiterates that building a **common understanding of the application of international law to the use of ICTs by States** must precede the formulation or adoption of any new rules, norms, or principles. In this context, we also reaffirm Israel's position that there is currently **no need for any new legally binding instruments**.

Finally, Israel strongly supports international capacity-building efforts, especially those aimed at enhancing the global cyber resilience. These efforts must be demand-driven, transparent, and politically neutral, and must respect the sovereignty and needs of recipient states.

And on a personal note, as head of the Israeli delegation, I have been deeply honored to participate in this process from its inception. Israel has long been an active and constructive voice in this field, including as a member of the 2015 GGE, which helped lay the foundation for the current framework of responsible state behavior in cyberspace. I can assure you, Mr. Chair, that Israel will continue to contribute meaningfully to global cyber resilience and to the stability and security of cyberspace.

Thank you.

Malta

Further to the comments submitted by the EU Delegation, Malta, in its national capacity, would like to highlight the following points.

Malta thanks the Chair, his team, and the Secretariat for their dedication and leadership throughout this process. We welcome the adoption of the final report and the decision to establish a Global Mechanism to advance responsible State behaviour.

We reaffirm our commitment to the UN Framework on Responsible State Behaviour in Cyberspace, recognising its key role in strengthening stability and security online. Malta emphasises the importance of continuing this work by building on prior UNGGE and OEWG outcomes, including the voluntary checklist and cross-regional efforts on international law, particularly international humanitarian law, aspects which were not adequately reflected in the final report.

The permanent mechanism's mandate to advance implementation of the normative framework of responsible state behaviour in cyberspace and to promote mutual accountability will be essential, as adherence to these norms will directly enhance stability and security in cyberspace, strengthen national cyber capabilities, and foster peace across divides. Malta recognises the value of cross-cutting working groups tasked with addressing specific security challenges and accelerating cybersecurity capacity-building. It is imperative to continue deepening our shared understanding of international law as applied in cyberspace, including the UN Charter, human rights law, and international humanitarian law.

The final report is truly historic, reflecting over 25 years of diplomatic efforts towards a consensus-based global mechanism that is action-oriented and inclusive. Malta recalls that the EU and its Member States first called for such a mechanism with the Programme of Action to Advance Responsible State Behaviour in Cyberspace as proposed by France. This mechanism helps ensure that all States are able to implement the normative framework, which serves as a cornerstone of our collective resilience and preparedness against cyber threats. Malta is pleased with the report's emphasis on capacity building and the way capacity-building efforts interact with the modalities of the permanent mechanism, creating the conditions for significant progress in this regard.

This transition to a single-track, inclusive, consensus-driven permanent mechanism marks a major milestone towards a safe, more secure, and more resilient digital space. Malta is honoured to have participated in this multilateral achievement.

Looking ahead, Malta stands ready to engage constructively with all stakeholders to strengthen accountability, promote responsible state behaviour, and enhance international peace and security in cyberspace.

**Nicaragua (joint statement of the Group of Like-Minded States:
Belarus, China, Cuba, Eritrea, Iran (Islamic Republic of),
Nicaragua, Niger, Russian Federation, Sudan, Venezuela
(Bolivarian Republic of) and Zimbabwe)**

Mr. Chair,

We appreciate the efforts made by You and Your team in preparing the final report of the OEWG and join consensus over this document. Due to Your long-standing commitment to the OEWG process the decision to establish a single-track, State-led, consensus-based Global mechanism on Developments on the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour

in the use of ICTs to deal comprehensively with a wide range of issues related to security of and in the use of ICTs has become possible.

We admit that a number of improvements has been made in the final report with the proposals of the LMG group taken into account. At the same time, we are disappointed with an overall misbalance between the implementation of the existing voluntary, non-binding rules of State behaviour and the development of new norms, including the elaboration of legally-binding obligations in the use of ICTs.

As for the modalities for NGOs' participation, we welcome that accredited stakeholders will participate on a non-objection basis and obtain a solely consultative status, as the future permanent mechanism is strictly an intergovernmental process. It is of utmost importance to ensure that all five pillars of the mandate of the FPM would be treated equally during the discussions with respect to States sovereignty and decision-making by consensus which may not be challenged or conditioned according to modalities adopted by consensus UN GA Resolution 79/237.

Our group remains committed to working constructively within the FPM to contribute to enhancing security of and in the use of ICTs.

Nicaragua

Señor Presidente, en nuestra capacidad nacional permítanos realizar unos breves comentarios adicionales.

1. Deseamos expresar nuestro sincero agradecimiento por el desarrollo del proceso del Grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y la comunicación y en su uso.
2. Valoramos la naturaleza abierta e inclusiva que permitió la participación plena y en pie de igualdad de todos los Estados Miembros, independientemente de su tamaño, nivel de desarrollo o capacidades tecnológicas, reflejando el verdadero espíritu multilateral y democrático que debe guiar nuestras discusiones sobre un tema tan crítico para la paz y la seguridad de todas las naciones.
3. Extendemos nuestro reconocimiento a la Presidencia y a su equipo, por su dedicación, imparcialidad y esfuerzos incansables para guiar nuestras complejas deliberaciones hacia un documento de consenso. Asimismo, agradecemos el apoyo técnico y sustancial fundamental brindado por la Secretaría, los intérpretes y funcionarios de apoyo, cuya labor ha sido indispensable para el funcionamiento eficaz de este proceso.

Señor Presidente,

4. La máxima prioridad de esta sesión fue lograr una transición fluida del actual GTCA al futuro mecanismo, bajo los auspicios de Naciones Unidas y que guiará su espíritu y decisiones por consenso.
5. En este sentido, destacamos que, en nuestras próximas discusiones, se deberá prestar atención especial a la materialización de mecanismos que promuevan eficazmente la cooperación internacional, con el objetivo que los países en desarrollo participemos en pie de igualdad en las reuniones futuras del mecanismo y fortalecer las capacidades de los países en desarrollo.
6. Reiteramos nuestra posición sobre el uso pacífico de las TIC, la prevención de una carrera armamentista en el ciberespacio y la condena al uso de estas tecnologías con fines hostiles o agresivos. Por tanto, rechazamos cualquier intento de imponer forzosamente la aplicabilidad del Derecho Internacional Humanitario al ciberespacio.

La comunidad internacional debe centrar sus esfuerzos en promover el uso de las TIC para el desarrollo de nuestros pueblos y prevenir conflictos creados por ciberataques.

7. Asimismo, esperamos que las discusiones para la elaboración de un instrumento jurídicamente vinculante en el ámbito de la seguridad de las TIC y de su uso continúen en el futuro mecanismo. Este instrumento nos podrá permitir abordar los vacíos legales en materia de ciberseguridad y establecer obligaciones para todos los Estados.

Señor Presidente,

9. Nicaragua reafirma su compromiso con este proceso multilateral. Continuaremos participando activa y constructivamente en las futuras etapas del Mecanismo, abogando siempre por un ciberespacio que sea un espacio de paz, cooperación, desarrollo y respeto a los derechos soberanos de todas las naciones. Es esencial que los resultados de este Grupo se traduzcan en acciones concretas que beneficien a toda la humanidad y prevengan el uso de las TIC como instrumentos de guerra o dominación.

Muchas gracias.

Niger

1. Tout d'abord j'adresse mes félicitations au Président du Groupe de travail, avec son équipe, pour leur professionnalisme et leur disponibilité qui ont d'emblée rendu possible la réussite du processus jusqu'à l'adoption du rapport final.

2. Sur l'application du droit international dans le cyberspace, il est clair que le rapport réaffirme à juste titre l'applicabilité du droit international, en particulier de la Charte des Nations Unies, au cyberspace notamment aux paragraphes 39-43.

3. Nous saluons entièrement cette position consensuelle qui vise à garantir à notre avis, le développement des discussions, des normes et des règles sûres et claires pour la stabilité et la prévisibilité des interactions entre États dans ce domaine. Cependant, nous proposons des clarifications supplémentaires sur quelques concepts clefs, notamment sur :

- La diligence raisonnable : Bien que mentionnée au paragraphe 40, une définition opérationnelle et assez développée de ce concept dans le contexte cybernétique renforcerait sa mise en œuvre pratique.
- Le droit international humanitaire (DIH) : Au paragraphe 40 (b) (ii), le rapport note son applicabilité en cas de conflit armé mais nous proposons une analyse plus approfondie des principes de distinction et de proportionnalité appliqués aux cyberopérations pour permettre aux États de connaître les implications pratiques.
- La Responsabilité des États : Le mécanisme d'attribution des cyberattaques et les voies de recours pour les États victimes mériteraient des lignes directrices plus concrètes, avec des cas pratiques clairs pour mettre en lumière le mécanisme d'attribution.

4. Sur le futur mécanisme permanent, nous proposons l'élaboration d'un guide pratique sur l'application du droit international, incluant des études de cas et des avis d'experts neutres, avec l'approbation des États membres.

5. Sur le renforcement des capacités, le rapport souligne la pertinence et l'importance du renforcement des capacités comme pilier transversal. Les propositions telles que le portail mondial (GSCCP) et le fonds volontaire sont des avancées considérables. Nous proposons plus encore, une approche inclusive dans le

programme de parrainage des délégués et la bourse pour les femmes, qui doivent être élargis pour couvrir davantage de pays en développement. Par ailleurs, on pourra instituer une évaluation des besoins dans le catalogue proposé, qui devrait intégrer un mécanisme de feedback des États bénéficiaires pour éviter les doublons.

6. Le futur mécanisme devrait adopter un plan quinquennal de renforcement des capacités, avec des indicateurs de succès mesurables et un budget dédié pour une question d'efficacité.

7. Sur l'annuaire des points de contact nationaux, nous saluons amplement cette initiative, qui doit au moins chaque année, être révisé et mis à jour. Son opérationnalisation nécessite à notre avis, des exercices et des simulations pratiques réguliers au moins chaque deux années.

8. Sur la participation du secteur privé dans le processus, il faut souligner le rôle des entreprises dans la sécurité des chaînes d'approvisionnement, qui devrait s'accompagner de cadres incitatifs et des facilitations afin d'accompagner leur action.

Republic of Korea

Chair, thank you for your excellent leadership and that of your team, as well as your dedication to this OEWG process and multilateralism.

As you rightly pointed out, it is rare to have 100 percent satisfaction with the outcome of multilateral negotiations. Nevertheless, we remain hopeful because you noted that the outcome of our work is not final, but rather part of a long journey in which we can accomplish more in the end.

I believe we still have a long way to go, but thanks to the solid foundation you have laid, we can continue to engage constructively with other distinguished colleagues and work toward a meaningful outcome in the future.

Russian Federation

The Russian Federation proceeds from the understanding agreed upon and fixed within the framework of the OEWG, in its reports, as well as relevant resolutions of the UN General Assembly, that the future Global Mechanism will focus, among other issues, on developing new legally binding norms in the field of digital security and continuing relevant substantive discussions. The automatic and unconditional application of the existing international law to the ICT-sphere is unacceptable. References to a certain sufficiency of the current international legal norms are untenable. This was vividly shown by the results of the negotiations on the elaboration of the first universal treaty in the field of information security – the UN Convention against Cybercrime, which was also discussed at the OEWG. We call on all States to sign it and ensure its early entry into force.

We proceed from the fact that the future Global Mechanism is to deal with the issues of the security of and in the use of ICTs. The Global Mechanism should aim at strengthening the trust between States and preventing interstate conflicts. This explains the necessity to make decisions on information security by consensus. An example that demonstrates the effectiveness of the consensus procedure is the unanimous agreement on the creation – on the Russian initiative – of the Global Intergovernmental Points of Contact Directory.

The participation of other interested parties in the activities of the OEWG has shown their limited ability to provide technical assistance to States in the field of dispute settlement and digital capacity-building. Moreover, some non-governmental

organizations and private developers/suppliers of ICT-products abused their status, undermining diplomatic efforts through dissemination of political propaganda and unsubstantiated accusations against distinct States. We insist that it is unacceptable to undermine the intergovernmental nature of negotiations on security in the field of ICT use within the framework of the Global Mechanism and welcome the preservation of the sovereign right of States to block the access of non-governmental organizations who politicize the process to the work of the Global Mechanism.

We note with disappointment the ongoing attempts to “split” the information security agenda into supposedly independent topics – artificial intelligence, quantum computing, the Internet of Things, ransomware, underwater cables, low-orbit satellite groupings, etc. We consider such actions counterproductive, aiming at increasing technological inequality between States to the detriment of those in need of technical assistance.

We welcome the consensus decision of the OEWG to establish a dedicated thematic group on capacity-building within the framework of the Global Mechanism. An important step has been taken towards reducing the “digital divide”. We look forward to the active engagement of all UN Member States in this matter. Russia will continue to cooperate with a view to strengthen the capabilities of developing countries in the field of information security, in particular, through the conclusion of legally binding agreements aimed at establishing and strengthening digital sovereignty.

We confirm our call to the international community to develop a universal convention on international information security, the concept of which was presented by Russia and a group of like-minded states as an official UN document in April 2023.

We strongly condemn the ongoing discriminatory policy of the host country of the UN headquarters towards members of the Russian delegation, including its leadership. Such an abusive practice significantly limits the State's ability to fully participate in the negotiation process, running counter to the principle of sovereign equality of States. We urge the UN Secretariat to resolve this issue and prevent a repeat of the non-admission of Russian experts to the work of the future Global Mechanism.

По утверждению итогового доклада РГОС

Господин Председатель,

Российская делегация благодарит Вас и Вашу команду за проделанную за 5 лет тяжелейшую работу в качестве Председателя данной РГОС. Под Вашим мудрым руководством Группа стала действительно эффективным механизмом, подтвердила свой статус в качестве центральной площадки ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ). За эти 5 лет, помимо принятия четырех консенсусных докладов, Группа смогла добиться конкретных, практических результатов, включая, прежде всего, создание по инициативе России Глобального межправительственного реестра контактных пунктов, который был запущен в мае 2024 г. и стал первой универсальной мерой доверия в области международной информбезопасности. Все это - во многом Ваша заслуга.

Господин Председатель,

Россия приветствует консенсусную договоренность о создании единого постоянного механизма по вопросам безопасности в сфере использования ИКТ. Этот механизм

еще больше повышает роль ООН в рассмотрении данной важнейшей темы и, будучи преемником РГОС, станет центральным универсальным форматом по вопросам безопасности в сфере использования ИКТ.

Господин Председатель,

Россия присоединилась к консенсусу по итоговому докладу РГОС. В нем нашли отражение важные для нас и большинства государств положения. Однако, к нашему глубокому сожалению, целый ряд российских идей и инициатив, которые поддерживались другими делегациями в течение 5 лет работы РГОС и являются объективным отражением дискуссий, не были учтены. Таким образом баланс по многим важным темам не был соблюден. Мы продолжим добиваться справедливого отражения мнений всех стран в рамках будущего постоянного механизма и на других площадках ООН в соответствии с принципом суверенного равенства государств. Не допустимо, чтобы одна группа стран препятствовала выражению мнений других государств, ставила свои интересы выше других. Это противоречит основополагающим принципам Устава ООН.

Господин Председатель,

Я хотел бы сделать следующее пояснительное заявление от имени Российской Федерации в отношении принятого консенсусом итогового доклада РГОС.

“Россия исходит из установки, согласованной в рамках РГОС, ее докладах и соответствующих резолюциях ГА ООН, на нацеленность Всемирного механизма (ВМ), среди прочего, на разработку новых норм международного права по цифровой безопасности и продолжение соответствующей предметной дискуссии. Автоматическое и безусловное применение действующего международного права (МП) к цифровой среде недопустимо. Ссылки на некую достаточность норм действующего МП несостоятельны. Это красноречиво показали обсуждавшиеся в РГОС итоги работы по согласованию первого универсального договора в области информационной безопасности (ИБ) – Конвенции ООН против киберпреступности. Призываем все государства подписать ее и обеспечить скорейшее вступление в силу.

Исходим из того, что будущий ВМ должен заниматься вопросами безопасности использования ИКТ и самих ИКТ. ВМ должен действовать в направлении укрепления доверия между государствами, предотвращения конфликтов между ними. Это обуславливает необходимость принятия решений по информационной безопасности консенсусом. Пример эффективности консенсусной процедуры – единогласное одобрение российской инициативы по созданию Глобального межправительственного реестра контактных пунктов.

Участие негосударственных субъектов в деятельности РГОС показало их ограниченную способность в оказании технического содействия государствам в урегулировании споров и наращивании цифрового потенциала. Более того, некоторые неправительственные организации и частные разработчики/поставщики ИКТ злоупотребляли предоставленным им статусом, подрывали дипломатические усилия через распространение политической пропаганды, голословных обвинений в адрес государств. Настаиваем на недопустимости подталкивания межправительственного характера переговоров по безопасности в сфере использования ИКТ в рамках ВМ и приветствуем сохранение суверенного права государства отстранять от работы ВМ те негосударственные субъекты, которые политизируют процесс.

С разочарованием отмечаем продолжающиеся попытки “раздробить” повестку ИБ на якобы самостоятельные темы – искусственный интеллект, квантовые вычисления, Интернет вещей, вирусы-вымогатели, подводные кабели, низкоорбитальные

спутниковые группировки и др. Рассматриваем такие действия как неконструктивные, преследующие своей целью усилить технологическое неравенство между государствами в ущерб тем из них, которые стремятся преодолеть “цифровой разрыв”.

Приветствуем консенсусное решение РГОС о создании рабочей группы по наращиванию потенциала в рамках Всемирного механизма. Сделан важный шаг в направлении сокращения “цифрового разрыва” между государствами. Рассчитываем на энергичное участие всех государств-членов ООН в реализации этой установки. Россия продолжит сотрудничество по укреплению возможностей развивающихся стран в области ИБ, в частности, через заключение с ними юридически обязывающих договоренностей, направленных на становление и укрепление цифрового суверенитета.

С учетом изложенного подтверждаем наш призыв к мировому сообществу к разработке универсальной Конвенции по МИБ, концепция которой была представлена Россией совместно с государствами-единомышленниками в ООН в апреле 2023 г.

Осуждаем продолжающуюся дискриминационную политику страны, размещающей на своей территории штаб-квартиру ООН, в отношении членов российской делегации, включая ее руководство. Такая порочная практика существенно ограничивает возможности государства полноценно участвовать в переговорном процессе, идет вразрез с принципом суверенного равенства государств. Настоятельно призываем Секретариат ООН урегулировать данный вопрос, не допустить повторения недопуска российских экспертов к работе Всемирного Механизма.”

Я прошу Вас включить данное выступление в сборник национальных заявлений, являющихся неотъемлемой частью итоговых решений РГОС.

Благодарю за внимание.

Unofficial translation

On the adoption of the final OEWG report

Distinguished Mr. Chair,

The Russian delegation thanks you and your team for the hard work you have done over the past 5 years as the Chair of this Open-Ended Working Group. Under your wise leadership, the Group has become an essentially effective mechanism and has confirmed its status as the UN central platform for security of and in the use of ICTs. Over the past 5 years, in addition to adopting four consensus reports, the Group has been able to achieve concrete, practical results, including, first of all, the establishment, on the initiative of Russia, of the Global Intergovernmental Points of Contact Directory, which was launched in May 2024 and became the first universal confidence-building measure in the field of international information security. All this is largely your merit.

Mr. Chair,

Russia welcomes the consensus agreement on the creation of a single-track future permanent mechanism on security in the field of ICTs. This mechanism will further enhance the role of the United Nations in addressing this critical topic and, as a successor to the OEWG, will become the central universal format for security issues in the sphere of ICTs.

Mr. Chair,

Russia joined the consensus on the final OEWG report. It reflects provisions important to the Russian Federation, as well as to the other States. However, to our deep regret, a number of our ideas and initiatives, which were supported by other delegations during the 5 years of the OEWG's functioning and are an objective reflection of the discussions, were not taken into account. Thus, the balance on many important topics has not been maintained in the text. We will continue to seek a fair reflection of the views of all States within the framework of the future permanent mechanism and at other UN venues in accordance with the principle of sovereign equality of States. It is unacceptable that one group of States creates obstacles for the expression of other States' positions, putting its interests above others. This is contrary to the fundamental principles of the UN Charter.

Mr. Chair,

I would like to make the following explanatory statement on behalf of the Russian Federation regarding the consensus final report of the OEWG.

“The Russian Federation proceeds from the understanding agreed upon and fixed within the framework of the OEWG, in its reports, as well as relevant resolutions of the UN General Assembly, that the future Global Mechanism will focus, among other issues, on developing new legally binding norms in the field of digital security and continuing relevant substantive discussions. The automatic and unconditional application of the existing international law to the ICT-sphere is unacceptable. References to a certain sufficiency of the current international legal norms are untenable. This was vividly shown by the results of the negotiations on the elaboration of the first universal treaty in the field of information security – the UN Convention against Cybercrime, which was also discussed at the OEWG. We call on all States to sign it and ensure its early entry into force.

We proceed from the fact that the future Global Mechanism is to deal with the issues of the security of and in the use of ICTs. The Global Mechanism should aim at strengthening the trust between States and preventing interstate conflicts. This explains the necessity to make decisions on information security by consensus. An example that demonstrates the effectiveness of the consensus procedure is the unanimous agreement on the creation – on the Russian initiative – of the Global Intergovernmental Points of Contact Directory.

The participation of other interested parties in the activities of the OEWG has shown their limited ability to provide technical assistance to States in the field of dispute settlement and digital capacity-building. Moreover, some non-governmental organizations and private developers/suppliers of ICT-products abused their status, undermining diplomatic efforts through dissemination of political propaganda and unsubstantiated accusations against distinct States. We insist that it is unacceptable to undermine the intergovernmental nature of negotiations on security in the field of ICT use within the framework of the Global Mechanism and welcome the preservation of the sovereign right of States to block the access of non-governmental organizations who politicize the process to the work of the Global Mechanism.

We note with disappointment the ongoing attempts to “split” the information security agenda into supposedly independent topics – artificial intelligence, quantum computing, the Internet of Things, ransomware, underwater cables, low-orbit satellite groupings, etc. We consider such actions counterproductive, aiming at increasing technological inequality between States to the detriment of those in need of technical assistance.

We welcome the consensus decision of the OEWG to establish a dedicated thematic group on capacity-building within the framework of the Global Mechanism. An important step has been taken towards reducing the “digital divide”. We look

forward to the active engagement of all UN Member States in this matter. Russia will continue to cooperate with a view to strengthen the capabilities of developing countries in the field of information security, in particular, through the conclusion of legally binding agreements aimed at establishing and strengthening digital sovereignty.

We confirm our call to the international community to develop a universal convention on international information security, the concept of which was presented by Russia and a group of like-minded states as an official UN document in April 2023.

We strongly condemn the ongoing discriminatory policy of the host country of the UN headquarters towards members of the Russian delegation, including its leadership. Such an abusive practice significantly limits the State's ability to fully participate in the negotiation process, running counter to the principle of sovereign equality of States. We urge the UN Secretariat to resolve this issue and prevent a repeat of the non-admission of Russian experts to the work of the future Global Mechanism.”

I would ask you to include this explanatory statement in the compendium of national statements being an integral part of the final decisions of the 11th OEWS session.

Thank you for your attention.

Switzerland

Monsieur le Président,

La délégation Suisse se félicite de l'adoption du rapport final. Comme vous l'avez dit, le rapport final est un ensemble très équilibré. Ce n'est pas un document parfait. Nous aurions souhaité un rapport plus ambitieux, en particulier en ce qui concerne le droit international, avec un accent particulier sur le droit international humanitaire. Nous saluons toutefois le fait que les paragraphes 15 et 42 du rapport contiennent des références supplémentaires au droit international humanitaire et aux opérations cyber dans les conflits armés, ainsi qu'à la responsabilité des États et à la diligence raisonnable, jetant ainsi les bases de discussions plus approfondies sur ces questions au sein du Mécanisme mondial.

Tout au long de ce groupe de travail, la Suisse a constamment plaidé en faveur de discussions approfondies, ciblées et fondées sur des scénarios concernant l'application du droit international existant, y inclus le droit international humanitaire, à l'utilisation des TIC. Elle a soumis des propositions pertinentes et, en collaboration avec d'autres délégations, rédigé et présenté des documents de travail. La Suisse poursuivra ce travail au sein du Mécanisme mondial.

Si le groupe de travail n'a pas obtenu de résultats décisifs sur les questions les plus controversées, il a néanmoins réussi à maintenir le dialogue multilatéral, à renforcer les capacités, à contribuer à instaurer la confiance et à obtenir des résultats concrets. Nous devons mesurer son succès à l'aune de la nature complexe de la cybersécurité et des divisions politiques qui existent entre les États sur ces questions. La large participation de tous les États membres et de toutes les parties prenantes intéressées a permis de prendre en compte un large éventail de points de vue et de préoccupations, rendant les discussions plus complètes et plus représentatives des intérêts divergents.

Ce groupe de travail et son rapport final constituent des étapes très importantes, mais progressives, dans notre ambition commune de créer un environnement des TIC ouvert, sûr, sécurisé, stable, accessible, pacifique et interopérable. Le Mécanisme

mondial offrira aux États et aux parties prenantes intéressées un nouveau cadre permanent pour œuvrer à la réalisation de cet objectif, d'une manière pragmatique et transversale, notamment en renforçant les capacités. À notre avis, il convient de se concentrer dans un premier temps sur la mise en œuvre du cadre élaboré à ce jour avant de décider, par exemple, de nouvelles mesures de confiance à l'échelle mondiale.

Monsieur le Président, ce matin, j'ai demandé à un modèle d'IA si le président du groupe de travail avait fait du bon travail. La réponse a été la suivante :

« Le président du Groupe de travail à composition non limitée (OEWG), l'ambassadeur Burhan Gafoor de Singapour, est largement reconnu pour avoir accompli un travail remarquable et efficace, compte tenu notamment de la nature très polarisée et sensible du sujet. »

Nous savons que les modèles d'IA ont parfois des hallucinations. Mais dans ce cas-ci, c'était juste. Sous votre direction, nous avons adopté un rapport final qui couronne un processus de cinq ans. Vous et votre équipe avez fait un excellent travail. Nous tenons à vous remercier, Monsieur le Président, ainsi que Katherine, Virginia, Clarice, Mathew et, bien sûr, Gillian. C'est elle qui détient la mémoire historique du GGE 2019-2021, du premier OEWG et de cet OEWG.

Enfin, nous tenons à remercier toutes les délégations pour leur flexibilité, ainsi que les parties prenantes intéressées pour leur participation et leurs précieuses contributions.

Merci, Monsieur le Président.

Unofficial translation

Mr. Chair,

The Swiss delegation welcomes the adoption of the final report. As you said, the final report is a very balanced overall package. It is not a perfect document. We would have liked to see a more ambitious report, particularly regarding international law, with a special focus on international humanitarian law (IHL). However, we welcome the fact that paragraphs 15 and 42 of the report contain additional references to IHL and cyber operations in armed conflicts, as well as to State responsibility and due diligence, thereby laying the foundation for further discussions on these issues within the Global Mechanism.

Throughout this OEWG, Switzerland has consistently advocated in-depth, scenario based and focused discussions on the application of existing international law, including IHL, to the use of ICTs, submitted relevant proposals and, together with other delegations, drafted and presented working papers. Switzerland will continue this work within the Global Mechanism.

While the OEWG hasn't achieved breakthrough results on the most contentious issues, it has succeeded in maintaining multilateral dialogue, building capacity, contributing to confidence and creating practical results. We must measure its success against the complex nature of cybersecurity and the political divisions that exist among states on these issues. The broad participation by all Member States and stakeholders ensured that a wide range of perspectives and concerns were considered, making the discussions more comprehensive and representative of divergent interests.

This OEWG and the final report are very important but incremental steps in our common ambition to building an open, safe, secure, stable, accessible, peaceful and interoperable ICT environment. The Global Mechanism will offer States and

stakeholders a new permanent format for working towards this goal, in an action-oriented and cross-cutting manner, including by strengthening capacity. In our view, the focus should initially be on implementing the framework developed so far before we decide, for example, on new global confidence-building measures.

Mr. Chair, this morning I asked an AI model whether the chair of the OEWG had done a good job. The answer was:

“The Chair of the Open-Ended Working Group (OEWG) — Ambassador Burhan Gafoor of Singapore — has widely been regarded as having done a commendable and effective job, especially given the highly polarized and sensitive nature of the subject.”

We know that AI models sometimes hallucinate. But in this case, it was right. Under your leadership, we have adopted a final report that crowns a five-year process. You and your team have done a great job. We would like to thank you Mr. Chair, as well as Katherine, Virginia, Clarice, Mathew and of course also Gillian. She is the one with the historical memory of the GGE 2019-2021, the first OEWG and this OEWG.

Finally, we would like to thank all delegations for their flexibility and the stakeholders for their participation and valuable contributions.

Thank you, Mr. Chair.

Tunisia (on behalf of the Arab Group)

السيد الرئيس سعادة السفير بُرهان غفور،

1 - تتشرف الجمهورية التونسية بإلقاء هذا البيان نيابة عن المجموعة العربية لتسجيل موقفها تجاه الورقة المطروحة لاعتماد مشروع تقرير الاجتماع الرابع والأخير لمجموعة العمل مفتوحة العضوية المشكلة بموجب قرار الجمعية العامة رقم ٢٤٠/٧٥.

2 - بداية ننقل لسيادتكم خالص الشكر والتقدير على قيادتكم الحكيمة والفعالة على مدار أربع سنوات من العمل الجاد، ولدولة سنغافورة، الدولة العضو بحركة عدم الانحياز التي تنتهي لها المجموعة العربية بالكامل، على ما قدمته من دعم كبير لأعمال مجموعة العمل ومُساندة تحقيقها لأهداف ترتقي لمستوى التطلعات.

3 - تؤكد المجموعة العربية استمرار التزامها بدعم الانتقال لآلية عالمية دائمة مُوحدة وجامعة وذات صبغة عملية وتقوم على التوافق داخل الأمم المتحدة، وهو الأمر الذي تراه المجموعة هدفاً رئيسياً لاجتماعنا الحالي وجسر لا غنى عنه نحو مُستقبل لضمان القيادة الأممية المُوحدة للمسار وإفساح مجال لكافة الدول الأعضاء لتشكيل ملامح الاستجابة العالمية للتحديات والمخاطر والتهديدات التي تواجهها الدول بشكل مُتزايد في الفضاء السيبراني واستخدام تكنولوجيا المعلومات والاتصالات.

4 - ومع التنويه بهذا الملمح الإيجابي الهام وجهودكم الدؤوبة لتحقيقه لا يفوتنا إبداء الشواغل إزاء النقاط الآتية:

أولاً: حذف المساحة المُخصصة لمناقشة انطباق القانون الدولي في الحيز السيبراني، في خطوة تؤثر سلباً على الثقة وتعمق من المخاوف إزاء الموقف الذي تتخذه بعض الدول إزاء استخدامات تكنولوجيا المعلومات والاتصالات في ظل استمرار وجود مساحة كبيرة من الغموض وعدم اليقين بشأن الفهم المشترك لكيفية انطباق قواعد ومبادئ القانون الدولي في الفضاء السيبراني بما في ذلك القانون الدولي الإنساني، والذي شاهدنا في الشرق الأوسط أمثلة مُباشرة لخرقه عبر قدرات تكنولوجيا المعلومات والاتصالات. وتؤمن المجموعة العربية بأن مجموعة العمل الأولى وما تتسم به من ولاية فضفاضة لن تُتيح إجراء نقاش مُتعمق بشأن هذا المبحث بالغ الأهمية. وتأسيساً على الفقرتين ٩ و ١٠ من الملحق ستدفع المجموعة بتعديل ذلك خلال اجتماع المُراجعة، كما ستطالب الرئيس المُعين للآلية بعقد مائدة مُستديرة مُخصصة للقانون الدولي.

ثانياً: الضعف الكبير في المحتوى الخاص ببناء القدرات، وفي الوقت الذي نُثمن فيه تخصيص مجموعة عمل مُتفرغة لهذا الغرض، فإن الجولة الختامية لمجموعة العمل أخفقت في تفعيل صندوق طوعي لدعم بناء القدرات وبرنامج زمالة مُتخصص فضلاً عن عدم وجود أي التزام بتأسيس آلية أممية لدعم بناء القدرات مدعومة بموارد كافية ومُناسبة وقابلة للتنبؤ، وحتى يتحقق كل ذلك أو بعض منه يظل الحديث عن دعم بناء قدرات الدول النامية وجسر الفجوات حديثاً خاوياً وليس التزاماً سياسياً حقيقياً مُستنداً لخطوات وتدابير عملية.

ثالثاً: تُعرب المجموعة العربية عن قلقها إزاء ما أصاب قسم القانون الدولي من تعديلات كبيرة تسببت في حذف مساحات هامة شملت مبادئ بالغة الأهمية تتبناها المجموعة العربية وفي مُقدمها السيادة الوطنية، وعدم التدخل في الشؤون الداخلية للدول الأعضاء، وعدم استخدام القوة، واحترام القانون الدولي الإنساني. ومع إسقاط مجموعة القانون الدولي المُشار إليه سلفاً، تزايدت المخاوف إزاء وضعيية القانون الدولي والامتثال لأحكامه في إطار الآلية العالمية الدائمة.

رابعاً: تُرحب المجموعة العربية بالإبقاء على الطابع الحُكومي للآلية الجديدة وقيادة الدول لها بما في ذلك عبر إطار مُنضبط لمشاركة الأطراف صاحبة المصلحة يقوم على الوضعية الاستشارية لدى المجلس الاقتصادي والاجتماعي وقاعدة عدم الاعتراض، وتراها المجموعة كافية ومُناسبة لتنظيم هذا الأمر.

5 - ختاماً، فإن المجموعة العربية في ظل حرصها على استمرار هذا الحوار البناء داخل الأمم المتحدة وأملها في إسهامه في توفير قدر أكبر من الحماية من المخاطر والتهديدات ذات الصلة، ستنضم للتوافق على الورقة المقدمة من الرئيس بشأن مشروع التقرير، مع تحفظاتها على الشكل النهائي للتقرير والترتيبات التكميلية للآلية العالمية الدائمة وما تسبب فيه من الدُخول لمرحلة جديدة من العملية الأممية دون الاستجابة للاعتبارات والضمانات التي تكفل بشكل موثوق منه الاستفادة الحقيقية وتعزيز الأمن والسلامة.

شكراً السيد الرئيس.

United States of America

Thank you, Mr. Chair. I would like to start by recognizing the work you, your team and the Secretariat have undertaken this week to get to the final report today. We appreciate your efforts to produce a document that is a better reflection of the work this OEWG has undertaken over the course of its mandate.

In particular, the report sets the stage for a smooth transition to a single-track, global mechanism that will continue important discussions on cyber stability and responsible state behavior while making meaningful progress on implementation of the Framework through its Dedicated Thematic Groups.

We recognize the significance of capacity building to States' ability to implement the Framework, and we are pleased to have found a path to retaining the capacity building thematic group.

We also appreciate that the report more accurately conveys the progress made in discussions on the application of existing international law to cyberspace, in particular by referencing discussion on international humanitarian law.

Mr. Chair, the United States would like to express its disassociation with paragraphs 9, 12, 28, and 53(a) of the report. The United States remains deeply disappointed that the report retains references to gender and the Sustainable Development Goals. The United States strongly supports protecting women and girls, defending their rights, and promoting women's empowerment, and promotes the ability of women and girls to engage in all aspects of social, civic, political, and economic life. However, the United States does not support references in the final report to "gender."

Additionally, the Sustainable Development Goals advance a program of soft global governance that is inconsistent with U.S. sovereignty and adverse to the rights and

interests of Americans, and the United States does not support references in the final report to SDGs.

Thank you, Mr. Chair.

II. European Union

In line with our commitment to international security and stability in cyberspace, the EU and its Member States have shown commitment to the OEWG. In contribution to the efforts of the international community in this regard, we have shown flexibility and dedication during the discussions with the aim to advance responsible state behaviour in cyberspace, and conclude the OEWG with a smooth and seamless transition to a single-track future permanent mechanism.

The EU and its Member States have repeatedly called for such a single-track permanent mechanism since 2020, with the proposal by France on the establishment of a UN Programme of Action to Advance Responsible State Behaviour in Cyberspace. Further work over recent years have contributed to propose, promote and establish a single-track mechanism that will allow the implementation of commitments of the successive UNGGE and OEWG reports, adopted and endorsed by consensus.

The ambition for the principle to establish a permanent mechanism has been at the core that unites us.

The EU and its Member States applaud the collective achievement of the international community to agree on a Global Mechanism to advance responsible state behaviour that will allow us to walk the talk, and to take real action, using the tools that the UN framework and all its pillars offers us, against the real challenges that we are facing in cyberspace. Challenges that affect our security, affect our economies and democracies.

We stress that we need to continue this work, building on the UN framework, building and strengthening consensus on a higher level of detail as regards the expectations set for states' behaviour by the 11 norms, international law and confidence building measures, and increasing and improving our cyber capacity building efforts.

We have the work of prior UNGGE's and OEWG's to build on, including the draft Voluntary Checklist, as well as the work done by cross-regional groups on the application of international law, particularly International Humanitarian Law. We regret however that this work is not appropriately reflected in the final OEWG report.

We look forward to continue our work and take this next step, working together under the Global Mechanism to advance responsible state behaviour in cyberspace and to increase stability and security in cyberspace.

The EU and its Member States want to wholeheartedly convey our appreciation to the Chair, his team and the UNODA for the effort and the good cooperation. The leadership demonstrated has collectively moved us forward on advancing responsible behaviour in cyberspace, and serves to demonstrate the value of multilateralism.