



General Assembly

Distr.: General
29 August 2023

Original: English/French/Russian/
Spanish

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

Fifth substantive session

New York, 24–28 July 2023

Compendium of statements in explanation of position on the adoption of the progress report of the open-ended working group as contained in [A/78/265](#), annex

Note by the Secretariat

1. On 28 July 2023, at its fifth substantive session, the open-ended working group on security of and in the use of information and communications technologies 2021–2025 considered item 7 of its agenda ([A/AC.292/2021/1](#)), “Adoption of annual progress reports”. The working group adopted its draft report as contained in document [A/AC.292/2023/L.1](#). It also decided to include in its report the outcome of its substantive discussions on agenda item 5. The report of the working group, including the annexed progress report on the discussions on agenda item 5, is contained in document [A/78/265](#).

2. Pursuant to paragraph 16 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>
Australia	3
Brazil	5
Canada	6
Colombia	6
Cuba	8
El Salvador.	10
Ghana	13
Iran (Islamic Republic of).	14
Israel	15
Russian Federation	16
Russian Federation (also on behalf of the Republic of Belarus, the Republic of Burundi, the People's Republic of China, the Republic of Cuba, the Democratic People's Republic of Korea, the Islamic Republic of Iran, the Republic of Nicaragua, the Russian Federation, the Republic of Sudan, the Syrian Arab Republic and the Bolivarian Republic of Venezuela). . . .	17
South Africa.	19
Switzerland	20
United Kingdom of Great Britain and Northern Ireland	24

Australia

Note: a truncated version of this statement (providing gender statistics) was delivered orally on 28 July 2023 after adoption of the Annual Progress Report; the full statement is provided for the record.

Chair,

During this session you asked us to see the forest from the trees in considering the report. Whilst, from our perspective, there may remain some birch trees to prune and some weeds to pluck, Australia has considered the Conference Room Paper for adoption this afternoon in light of your request.

Taking this view, **Australia is pleased to join consensus** on the 2023 OEWG annual progress report – a report that once again, is balanced on a knife’s edge. Australia expresses support for you and your work – and we have taken to heart your instructions that this Conference Room Paper is the best way forward to reflect the progress we have made over the past year.

We can see that the Chair and his team has woven together the various strands of our discussions into something productive, ambitious, and forward looking – you have indeed listened very carefully to our views. The report is testament to the tenacity of the Chair, the importance that all governments ascribe to this issue, and the joint commitment of each delegation to maintain momentum in our discussions.

Australia offers the following non-exhaustive explanation of position in regard to the report.

As has been the case previously, there were several issues that we hoped would be included, that are not. Australia would have liked to see the report: further reflect our in-depth discussions on international law, including international humanitarian law and international human rights law; provide a record of the significant focus our conversations have had on implementation of the norms; and reflect the threats discussed by the group more fulsomely, including the threat of ransomware.

Australia underscores – as reflected in paragraph 32 of the report – that this group remains undecided on the need for additional legally binding obligations. Australia’s position, as previously expressed in this forum and the processes that have come before it, is that international law, including the UN Charter in its entirety, as well as international humanitarian law and international human rights law, apply to States’ behaviour in cyberspace. We note this Group’s mandate, in addition to the language reflected at paragraph 23(a) of this report, is to also continue to study, with a view to promoting common understandings, how international law applies to the use of information and communications technologies by States.

Before we can embark on whether we need additional legally binding obligations, each State must be supported through capacity building and provided the time, to come to their own national position on how international law applies in cyberspace. It is only after allowing this time, and providing for such capacity building, that we can consider whether anything more is needed, and how best any gaps, if they exist, are to be addressed.

Therefore, Chair, Australia’s priority is to continue to reflect on our own national positions, and continue engaging in dialogue, including through this OEWG process, but also bilaterally and regionally, on how best to address the existing and potential threats that are emerging in cyberspace.

Secondly, Chair, Australia regrets that this report, in its description of the multistakeholder community, does not explicitly refer to civil society. We note that

the description of the multistakeholder community in this report is non-exhaustive, but we also observe that the phrase ‘civil society’ has been removed from the final version of the report. In this regard, Australia underscores the value it sees in the participation of civil society in this Group’s discussion on how we promote international peace and security in cyberspace. We greatly valued the statements made by civil society during the multistakeholder session and in previous sessions, and we will continue to reflect on those statements, in order to inform our thinking ahead of upcoming sessions.

There are also many very good things in this report – and I think it’s important not to just focus on concerns. Australia welcomes the establishment of the global Points of Contacts (POC) directory, noting it is no mean feat, and Australia is committed to breathing life into this initiative following adoption of the report.

Australia welcomes the recognition that threats may be experienced differently by States according to their levels of digitalisation, capacity, ICT security and resilience, infrastructure and development.

Australia welcomes the additional depth we are slowly and carefully making on international law – it is heartening to see.

Australia welcomes the references to the 2021 OEWG capacity building principles and the operationalisation of these principles throughout the report – because sustainable capacity building is absolutely essential to the further advancement and implementation of our framework.

Australia also welcomes, with appreciation, the important contribution of the multi-stakeholder community throughout this process, and recognition in the report of the importance of further strengthening this collaboration.

We join the expression of gratitude to you and your team for getting us through this week to adopt a consensus report. Australia will take you up on your offer and submit, in writing, a full explanation of position. In the interest of time, I will extract only one point from that statement.

Australia welcomes the references to gender, and to the gender digital divide in paragraph 8 of the report.

In particular, Australia welcomes the report’s recognition of the high level of participation by women delegates and the prominence of gender perspectives in the discussions.

I am delighted to announce that at our session this week 48% of interventions were made by women. We had even higher numbers of women participating in the interventions on norms and international law: 51%; and 54% of interventions made on confidence building measures and capacity building were made by women. This is a noticeable improvement compared to the OEWG’s hybrid intersessional in May – where only 27.5% of statements were made by women delegates. But hearteningly, these numbers are similar to the statistics from the fourth substantive session in March – where 47% of all interventions were made by women, and in July last year – which also reached 48%.

In this regard, Australia recognises in particular the contributions of the Women in Cyber Fellows: your participation enriches this process and improves our joint outcome. And I hope, despite the significant journey we have been on this week, you can all join us for a group photo with the Fellows at the close of our session.

In closing, Australia empathises with those who wanted more from this report. We hope that you will also empathise with us because Australia, too, wanted more. We

recognise, however, that this is an annual progress report – it is not the end of our work.

By supporting consensus today, we add another layer to the foundation, upon which our future work in this OEWG can build.

Thank you all again, and I wish everyone here, but most particularly the Chair, the Chair's team and the Secretariat a full night's sleep.

Brazil

Mr Chair,

We appreciate your able leadership during the last session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025 (OEWG). As a result of your efforts and compromises from several delegations, it was possible to have a consensus [final document](#), one that accommodates diverse views and priorities, as well as competing positions.

We believe that the content of the report broadly reflects the consensus that was possible for the group to achieve at the time. Thus, we welcome the reaffirmation of the *acquis* as laid out in [resolution 70/237](#), which the General Assembly adopted by consensus.

In this regard, we must acknowledge the cumulative and evolving framework for responsible State behavior in the use of ICTs and to reiterate that past reports from the GGE and OEWG remain the basis of our work.

With the aim of contributing to the future work of the OEWG, we would like to highlight the following:

- Brazil reaffirms that the United Nations Charter is applicable in its entirety and references to specific articles in the report does not imply otherwise.
- We stress that under international law, sovereignty entails an obligation in its own right, and is therefore applicable as a standalone rule in the use of ICTs by States. We recall in this regard the agreed language in several documents since the 2012–2013 GGE report, which refers to “State sovereignty and international norms and principles that flow from sovereignty” (para. 27), which is also present in the 2021 Report (para. 71, b), later endorsed by the UNGA.
- The question of how international law applies to cyberspace cannot be rushed, nor any can issues be considered closed at this stage, so we welcome the reference to a non-exhaustive, open list of topics proposed by States for further discussion under international law.
- The contributions of international legal experts are important reference material, but do not amount to a substitute for state practice and *opinio juris*, particularly in considering how international law applies in the use of ICTs by States.
- Expert briefings to be held during the intersessional period shall present States with a balanced offer of views, considering not only equitable geographical representation, but also different geographical legal systems in the world, with the objective of showcasing different perspectives and doctrinal divergences in each area of discussion.

This delegation wishes to once more congratulate and express our deepest appreciation for the hard work of the Chair and of his team.

Thank you.

Canada

Mr. Chair,

1. Canada thanks you for your tireless work and that of your team and the Secretariat in bringing us to consensus.
2. My delegation came to this room this morning in a genuine spirit of compromise, confidence building and consensus. Canada was not fully happy with the text, there was much that we would have wanted to see changed; however, we also respected the views of other Member States and understood the need for balance. We are pleased that we have reached consensus on what remains a substantive, action-oriented 2nd annual progress report. We are convinced that this report will allow us to advance our work in the coming year.
3. However, Canada is deeply concerned, Mr. Chair, that today, we were no longer in the space of consensus as it was intended within the multilateral system. The consensus of finding the best possible option to make everyone a little unhappy. The consensus where we may comprise and accept language in the best interest of the group as a whole.
4. What we saw today was an example of where we are tipping dangerously towards a form of consensus that has deadlocked other UN bodies for years. That is when we see consensus being used as a veto. Consensus being used as a bullying tactic. This is a very dangerous downward slope that benefits no one, as it risks blocking all progress in addressing ICTs in the context of international peace and security within the UN.
5. We hope this trend will not continue over the coming year.

Colombia

Julio 27, 2023

Señor Presidente:

Nos adherimos a las Declaración pronunciada por México, a nombre de un grupo de países de América Latina sobre creación de capacidades; a la Declaración pronunciada por Canadá a nombre de un grupo interregional de países constructores de confianza; y a la Declaración pronunciada por Estonia, a nombre de un grupo de países sobre derecho internacional.

En nuestra capacidad nacional, Señor Presidente, nos unimos al reconocimiento por su labor y al agradecimiento por sus esfuerzos, y los de su equipo, y por la presentación de la versión revisada del texto.

Como lo señaló de manera más elocuente el distinguido delegado de Vietnam, su liderazgo nos ha permitido tener una discusión fructífera y avanzar en el necesario diálogo sobre un tema tan importante para la paz y seguridad internacional.

Le reiteramos nuestro apoyo a su gestión y nuestra voluntad de aportar para el logro de consenso y adoptar nuestro segundo Informe Anual de Avance en la presente sesión.

Señalado lo anterior, quisiéramos hacer los siguientes comentarios breves:

En lo que se refiere al apartado de **amenazas existentes y potenciales**, hubiésemos querido que se conservara la referencia del borrador anterior a la inteligencia artificial y la computación cuántica, temas que durante el año fueron mencionados por

múltiples delegaciones y partes interesadas. Adicionalmente, esperamos que en futuras sesiones se considere la propuesta del repositorio de amenazas realizada por Kenia, incluida la posibilidad de contar con la participación de la sociedad civil en el mismo.

Con respecto al apartado de **reglas, normas y principios**, valoramos que se haya incluido en el párrafo 23b la referencia a la posibilidad de apoyar a países en desarrollo en la identificación de sus infraestructuras críticas.

En lo que corresponde al **derecho internacional**, como ya lo señalamos, adherimos a la intervención realizada por Estonia a nombre de un grupo de países y le agradecemos señor Presidente por haber tenido en cuenta las propuestas presentadas en el documento de trabajo de este grupo. Asimismo, quisiéramos destacar que varias delegaciones, incluida Colombia, manifestaron su apoyo a la propuesta de Alemania de incorporar la referencia a los derechos humanos en esta sección, por lo que agradecemos sea reconsiderada su inclusión.

Señor Presidente:

En lo que se refiere a la **construcción de capacidades**, reconocemos y valoramos la inclusión de acciones y recomendaciones tendientes a este propósito transversal de este Grupo de Trabajo (OEWG), así como las referencias sobre los esfuerzos de construcción de capacidades con enfoque de género.

En relación con el apartado sobre **Medidas de Fomento de la Confianza**, mi delegación estima que la aprobación del Directorio Global de Puntos de Contacto será una importante contribución para la promoción de la paz y la seguridad internacionales, incrementará la transparencia, la predictibilidad y proporcionará la base para la implementación de futuras medidas.

Con respecto a la Sección sobre el **Diálogo Institucional Periódico**, en el párrafo 56, al igual que Francia, preferimos el lenguaje contenido en el borrador de Informe previo.

Por último, señor Presidente, deseamos resaltar la importancia de mantener el diálogo que nos permita avanzar en la implementación del marco de comportamiento responsable de los Estados en el uso de las TICs acordado, y en la búsqueda de entendimientos comunes que nos permitan enfrentar cooperativamente los desafíos que enfrentamos en materia de ciberseguridad.

Muchas gracias.

28 Julio, 2023

Señor Presidente:

Le reiteramos nuestro agradecimiento por sus esfuerzos y su trabajo, por presentarnos un Reporte Anual de Avance que incorpore, en la medida de lo posible, las diferentes posiciones y propuestas, entendiendo la complejidad de esta tarea.

Valoramos el listado incluido en el Anexo D. que, como Usted lo señaló, refleja el concurso y compromiso que han demostrado todas las delegaciones.

Valoramos su dedicación y la de su equipo y la Secretaría. Esperamos que este fin de semana puedan recuperar las horas de sueño que han dedicado a esta labor.

Como lo mencionó la distinguida Embajadora de Costa Rica ayer, lo perfecto puede obstaculizar lo posible. El texto no es perfecto, porque nada lo es y porque este es un proceso en construcción, del que este es un paso más.

Por supuesto que mi delegación, como otras, hubiera preferido la inclusión de lenguaje adicional o algunos cambios. Sin embargo, entendemos que el texto representa un delicado balance y apoyamos firmemente su adopción.

Instamos a todas las delegaciones a hacer lo mismo, considerando la importancia de continuar nuestro diálogo orientado a la acción, necesario, sobre un tema tan importante para la paz y seguridad internacionales que, como elocuentemente lo señaló el distinguido delegado de Vietnam ayer, nos ha facilitado su liderazgo.

Para terminar, simplemente quisiera recordar que nos encontramos hoy aquí discutiendo este tema gracias a la iniciativa de Estados que lo pusieron sobre la mesa e instaron a su consideración, y que hemos logrado avanzar, en estos 20 años, en las deliberaciones sobre el particular, y acordar un marco de comportamiento responsable, gracias al concurso de todas las delegaciones y a su voluntad de continuar el diálogo, la comprensión de los diferentes puntos de vista y la búsqueda de entendimientos.

Adherimos a lo señalado por Usted, Sr. Presidente, este Grupo de Trabajo es una medida de fomento de la confianza, la adopción de este Informe Anual de Avance es un reconocimiento a su valor como tal.

Muchas gracias.

Cuba

Señor Presidente:

Nos sumamos a la declaración de la delegación de la Federación de Rusia en nombre de un grupo de países de ideas afines.

Agradecemos sus intensos esfuerzos y los de su equipo para lograr un segundo informe anual progresivo del Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y la comunicación.

Creemos firmemente en el valor del GTCA como el único foro que permite la participación de todos los Estados para discutir con transparencia y en igualdad de condiciones sobre la seguridad y el uso de las TIC.

De ahí que nuestra delegación haya privilegiado el consenso sobre el informe adoptado, a pesar de que tenía mayores expectativas, en especial para avanzar en el desarrollo de normas adicionales para el comportamiento responsable de los Estados en materia de seguridad en el uso de las TIC. Esperamos que en las próximas sesiones del GTCA podamos observar progresos en este empeño, en cumplimiento del mandato del Grupo.

Continuaremos trabajando en favor de la elaboración de un instrumento internacional jurídicamente vinculante amplio, sobre las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. A diferencia de normas de implementación voluntaria para los Estados, un instrumento vinculante establecería obligaciones para atender de manera efectiva los crecientes retos y amenazas en este ámbito. Ello permitiría, igualmente, responder a los vacíos legales existentes.

Insistimos en la necesidad de evitar que, en las próximas sesiones del GTCA, proliferen la inadecuada importación de lenguajes provenientes de los informes de los Grupos de Expertos Gubernamentales de composición limitada, en especial en relación con temas que no gozan de consenso internacional, como lo relativo a la noción de la aplicabilidad automática del Derecho Internacional en el ámbito de las TIC, incluido el Derecho Internacional Humanitario.

Para prevenir y enfrentar los peligros que entraña el uso malicioso de las TIC en el contexto de la seguridad internacional, es esencial la cooperación mancomunada de todos los Estados y la creación de capacidades. Apreciamos que el informe haya incluido varias iniciativas en este sentido. No obstante, esperamos que pueda fortalecerse el lenguaje al respecto en futuras sesiones del GTCA, en relación con todos los ámbitos del mandato del Grupo, para eliminar la brecha digital que tanto afecta a los países en desarrollo.

Abogamos por continuar discutiendo sobre el futuro mecanismo de diálogo institucional periódico bajo los auspicios de las Naciones Unidas, como recomienda el informe adoptado, sin prejuzgar el resultado de las discusiones, ni privilegiar la propuesta de Programa de Acción por encima de otras iniciativas nacionales. Dicho mecanismo deberá ser intergubernamental y basado en la toma de decisiones por consenso.

Reiteramos el compromiso de Cuba con el Grupo de Trabajo de Composición Abierta y su disposición a contribuir a la construcción de consensos sobre los temas bajo su mandato.

Muchas gracias.

Mr. Chair,

We align ourselves with the statement delivered by the delegation of the Russian Federation on behalf of a group of like-minded countries.

We appreciate your and your team's intensive efforts to achieve a second annual progress report of the Open-Ended Working Group (OEWG) on security of and in the use of Information and Communication Technologies.

We strongly believe in the value of the OEWG as the only forum that allows the participation of all States to discuss with transparency and on an equal footing the security and use of ICTs.

Hence, our delegation has favored consensus on the adopted report, despite the fact that we had higher expectations, especially to advance in the development of additional standards for the responsible behavior of States in the area of security in the use of ICTs. We hope that in the next sessions of the OEWG we can observe progress in this endeavor, in compliance with the mandate of the Group.

We will continue to work towards the elaboration of a comprehensive international legally binding instrument on information and communications technologies in the context of international security. Unlike voluntary implementation standards for States, a binding instrument would establish obligations to effectively address the growing challenges and threats in this area. It would also make it possible to address existing legal gaps.

We insist on the need to avoid the proliferation, in future OEWG sessions, of inappropriate importation of language from the reports of the limited-membership Groups of Governmental Experts, especially in relation to issues that do not enjoy international consensus, such as the notion of the automatic applicability of international law in the field of ICTs, including international humanitarian law.

To prevent and address the dangers posed by the malicious use of ICTs in the context of international security, concerted cooperation of all States and capacity building are essential. We appreciate that the report has included several initiatives in this regard. However, we hope that language in this regard can be strengthened in future OEWG

sessions, in relation to all areas of the Group's mandate, to bridge the digital divide that so affects developing countries.

We advocate continuing discussions on the future mechanism for regular institutional dialogue under the auspices of the United Nations, as recommended in the adopted report, without prejudging the outcome of the discussions or giving priority to the proposed Program of Action over other national initiatives. Such a mechanism for regular institutional dialogue must be intergovernmental and based on decision-making by consensus.

We reiterate Cuba's commitment to the Open-Ended Working Group and its willingness to contribute to consensus-building on the issues under its mandate.

I thank you.

El Salvador

El Salvador expresa su agradecimiento 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) y su equipo de trabajo por la hábil conducción con la que ha desarrollado la Presidencia del GTCA, mandado del 2021 al 2025). Del mismo modo, El Salvador reconoce la valiosa labor de acompañamiento de la Oficina de Asuntos de Desarme de las Naciones Unidas durante las sesiones formales y entre sesiones del Grupo desde sus inicios.

El Salvador ha participado constructivamente en las labores del GTCA, de conformidad al mandato de la Asamblea General conferido a través de su resolución [75/240](#). Durante la quinta sesión sustantiva, la delegación salvadoreña tuvo una participación activa en la negociación del Reporte Anual de Progresos (APR por sus siglas en inglés), en concordancia con su compromiso con las labores del grupo, presentando recomendaciones en capacidad nacional y con grupos de países de ideas afines en temas de derecho internacional y creación de capacidad.

El Salvador considera que el APR, adoptado por consenso en la quinta sesión del Grupo, es un documento balanceado que recoge los elementos centrales de las posiciones de los Estados Miembros y plantea una línea clara de acción para las sesiones venideras.

Varios de los posicionamientos presentados y defendidos por El Salvador se ven reflejado en el APR; sin embargo, algunos elementos que fueron apoyados por la delegación salvadoreña no fueron abordados en el reporte y sobre los cuales la delegación salvadoreña continuará s abogando, con la finalidad de que puedan seguirse discutiendo dentro del Grupo y, eventualmente, figuren dentro de las recomendaciones para cada área del mandato del GTCA.

- **Sobre amenazas reales y potenciales:** El Salvador ha ahondado sobre cómo las tecnologías emergentes pueden representar, en sí mismas, nuevos vectores de ataque y crear nuevas vulnerabilidades, se aprecian las menciones a la necesidad de proteger infraestructuras críticas (CI) e infraestructuras críticas de información (CII) de ataques maliciosos, particularmente aquellas que proveen servicios esenciales. La mención específica de explotación de vulnerabilidades en el ambiente de tecnologías de la información y las comunicaciones (TIC), la amenaza a la integridad de las cadenas de suministros y la utilización de software malicioso como el ransomware son notorias. Sin embargo, es necesario seguir ampliando los efectos disruptivos de estas amenazas en su relación con la paz y seguridad internacional. Particularmente en el caso de ransomware, ahondar en las ramificaciones de la utilización de este tipo de malware cuando

se paralizan las funciones gubernamentales y cuando se cruza el umbral internacional de paz y seguridad.

- **Inteligencia Artificial:** es necesario que se sigan discutiendo los retos asociados con los desarrollos tecnológicos derivados de los saltos cualitativos de usos de la inteligencia artificial (IA) y la computación cuántica. Discusiones sustantivas fueron sostenidas en las sesiones previas del grupo, las cuales no quedaron debidamente reflejadas en el APR. El Salvador ha ampliado sobre IA generativa y la necesidad tener discusiones profundas sobre la posible regulación y/o prohibición de algunos usos específicos de aplicaciones y capacidades de la IA. Adicionalmente, es necesario dar mayor atención a los retos que plantean las tecnologías de doble uso, incluidos los modelos de IA, para capitalizar las oportunidades sin amenazar la paz y seguridad internacional.
- **Sobre derecho internacional:** se reconoce como central la naturaleza evolutiva y progresiva de las discusiones del GTCA en el marco del comportamiento responsable de los Estados en el ciberespacio. El Salvador ha reafirmado cómo el derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz, seguridad, estabilidad y promover un ambiente de TIC seguro, accesible y pacífico. En esa línea y siguiendo las recomendaciones del Grupo de identificar áreas de convergencia, El Salvador, junto con Australia, Estonia, Colombia y Uruguay, trabajó lenguaje de convergencia sobre derecho internacional. Se estima que las menciones específicas al Artículo 33 de la Carta y Capítulo VI sobre arreglo pacífico de controversias deben seguirse ampliando en las próximas sesiones para aterrizar en concepciones comunes sobre cómo se aplican en el ciberespacio.
- **Sobre medidas de fomento de la confianza:** El Salvador apoya las referencias al establecimiento de un directorio global intergubernamental de puntos de contacto, que se construirá en base a experiencias regionales. Se estima que esta es una iniciativa orientada a la acción resultado de las labores del GTCA.
- **La creación de capacidades:** es un elemento transversal en las labores del GTCA y El Salvador – junto a un grupo de países de América Latina y el Caribe – apoya las referencias relacionadas en el documento. En capacidad nacional, El Salvador ha señalado que el fomento de capacidades debe tener en cuenta las cuestiones de género y una visión más amplia relacionada con la reducción de la brecha digital.
- **Sobre el diálogo regular institucional:** El Salvador reconoce como se ha enmarcado la propuesta del establecimiento del Programa de Acción (POA) para avanzar en el comportamiento responsable de los Estados en el uso de TICs en el contexto de la seguridad internacional y cómo se relaciona esta iniciativa con el Grupo de Trabajo. El Salvador es uno de los promotores de esta iniciativa y retoma las recomendaciones de seguir intercambiando visiones, con el objetivo de generar mecanismo único para continuar desarrollando la normativa de comportamiento responsable de los Estados en el ciberespacio en el marco de las Naciones Unidas.

El Salvador expresses its gratitude to the Chair of the Open-ended Working Group on the Security of Information and Communication Technologies and their use (OEWG) and his team for the skillful leadership with which he has carried out the Chairmanship of the OEWG, mandated from 2021 to 2025.) Likewise, El Salvador recognizes the valuable work of the United Nations Office for Disarmament Affairs in accompanying the Group during the formal and intersessional sessions of the Group since its beginning.

El Salvador has participated constructively in the work of the OEWG, in accordance with the mandate conferred by General Assembly resolution [75/240](#). During the fifth substantive session, the Salvadoran delegation participated actively in the negotiation of the Annual Progress Report (APR), in keeping with its commitment to the work of the group, presenting recommendations in national capacity and with groups of like-minded countries on issues of international law and capacity building.

El Salvador considers that the APR, adopted by consensus at the fifth session of the Group, is a balanced document that reflects the central elements of the positions of the Member States and sets out a clear line of action for future sessions.

Several of the positions presented and defended by El Salvador are reflected in the APR; however, some elements that were supported by the Salvadoran delegation were not addressed in the report and the Salvadoran delegation will continue to advocate for them, so that they can continue to be discussed within the Group and eventually be included in the recommendations for each area of the OEWG's mandate.

- **On actual and potential threats:** El Salvador has deepened into how emerging technologies can represent, in themselves, new vectors of attack and create new vulnerabilities. The need to protect critical infrastructures (CI) and critical information infrastructures (CII) from malicious attacks, particularly those that provide essential services, is mentioned. The specific mention of exploitation of vulnerabilities in the information and communications technology (ICT) environment, the threat to the integrity of supply chains and the use of malicious software such as ransomware are notorious. However, the disruptive effects of these threats as they relate to international peace and security need to be further amplified. Particularly in the case of ransomware, to deepen into the ramifications of using this type of malware when government functions are paralyzed and when the international threshold of peace and security is crossed.
- **Artificial Intelligence:** further discussion is needed on the challenges associated with technological developments arising from the qualitative leaps in the uses of artificial intelligence (AI) and quantum computing. Substantive discussions were held in the previous sessions of the group, which were not duly reflected in the APR. El Salvador has expanded on generative AI and the need to have in-depth discussions on the possible regulation and/or prohibition of some specific uses of AI applications and capabilities. Additionally, more attention needs to be given to the challenges posed by dual-use technologies, including AI models, to capitalize on opportunities without threatening international peace and security.
- **On international law:** the evolving and progressive nature of the OEWG discussions in the framework of the responsible behavior of States in cyberspace is recognized as central. El Salvador has reaffirmed how international law, in particular the United Nations Charter, is applicable and essential for maintaining peace, security, stability and promoting a secure, accessible, and peaceful ICT environment. Following the Group's recommendations to identify areas of convergence, El Salvador, together with Australia, Estonia, Colombia, and Uruguay, worked on convergence language on international law. The specific references to Article 33 of the Charter and Chapter VI on the peaceful settlement of disputes should continue to be expanded in future sessions in order to arrive at common conceptions of how they apply in cyberspace.
- **On confidence-building measures:** El Salvador supports references to the establishment of a global intergovernmental directory of points of contacts, to be built on regional experiences. This is considered an action-oriented initiative resulting from the work of the OEWG.

- **Capacity building:** is a cross-cutting element in the work of the OEWG and El Salvador – together with a group of Latin American and Caribbean countries – supports the related references in the document. In national capacity, El Salvador has pointed out that capacity building should take into account gender issues and a broader vision related to bridging the digital divide.
- **On the regular institutional dialogue:** El Salvador recognizes how the proposal for the establishment of the Program of Action (POA) to advance in the responsible behavior of the States in the use of ICTs in the context of international security has been framed and how this initiative is related to the Working Group. El Salvador is one of the promoters of this initiative and takes up the recommendations to continue exchanging visions, with the objective of generating a unique mechanism to continue developing the norms of responsible behavior of States in cyberspace within the framework of the United Nations.

Ghana

Mr. Chair, thank you for giving me the floor.

2. My delegation would like to thank you and your entire team for putting together a comprehensive APR for the consideration of member states. We acknowledge that this is no small feat and, as such, we commend your leadership in steering the affairs of the OEWG.

Mr. Chair,

3. Ghana joins its voice to those of other states who welcome the language of embracing the need to have a high level of participation of female delegation and ensure gendered perspectives in its discussions as outlined in paragraph 7 of the document and continue to welcome the inclusion of this text in the document and its eventual adoption. My delegation also supports calls for the inclusion of energy in paragraph 12 as part of the list of critical infrastructure proposed by member states. We believe that the designation and protection of key CIIs is an important component of cybersecurity development.

Mr Chair,

4. Ghana would like to propose that the previous text in paragraph 21 of the first APR calling for the participation of relevant experts to be invited by the OEWG chair, to have focused discussions on developments in new technology such as quantum computing and artificial intelligence in order to exchange views and build knowledge on its potential impact, must be considered and maintained in the revised APR. This is because an increasing reliance on cloud technology, while neutral, as outlined in the first APR, could increase vulnerabilities and expand attack vectors.

5. Ghana continues to recognize that the advent of the fourth industrial revolution and the increasing use of technologies specifically Artificial Intelligence (AI), Internet of Things (IoT), ubiquitous connectivity, Blockchain Technology, among others continue to pose risks to international security, despite the significant benefits they offer. Some of these threats include impersonation, ransomware attacks, online fraud, online blackmail, unauthorized access, disinformation, cyber bullying among many others. Thus, Artificial intelligence is currently magnifying the capabilities of cyber criminals to conduct attacks, and should not be overlooked.

6. On existing threats, Mr. Chair, Ghana is pleased that the APR has been expanded to reflect the salient existing and emerging threats and the various forms in which they take. However, we would have liked to see a text considering the possibility of a threat repository, namely because this will provide the benefits for member states including;

Enhanced Situational Awareness which will allow member states gain understanding of the evolving threat landscape by sharing data on the most recent attack vectors, malware strains, and techniques utilized by cybercriminals. Additionally, it will aid in Early Warning and Rapid Response and Cybersecurity Capacity Building through Information sharing among member states to help bridge the knowledge gap.

7. Ghana recognizes the need to establish a global POC directory and supports the nomination of national Points of Contact. However, we recommend that this nomination is done at technical, policy, and diplomatic levels, due the differences in capacities. Further discussions on the development of such a directory and related capacity-building initiatives at the OEWG sessions is, therefore important.

8. Regarding section D on international law, my delegation endorses the proposal to hold workshops, training courses, and exchanges on best practices at international, inter-regional, regional, and sub-regional levels. We also acknowledge the valuable contributions regional organisations can make by sharing their knowledge and experience in this field. We believe that is essential to draw upon these experiences, as applicable, to further strengthen efforts to build capacity.

9. To conclude Mr. Chair, Ghana recognizes that the OEWG is a progressive engagement, and we wish to assure you of our flexibility and support in reaching a consensus outcome.

I thank you.

Iran (Islamic Republic of)

In the Name of God

Mr. Chair,

Distinguished delegates,

At the outset, I would like to join other colleagues to express our delegation's sincere gratitude to you, your team, the secretariat, and all delegates for all the contribution extended to this multilateral, inclusive, unique, democratic, and historical process on security and in the use of ICTs.

We appreciate your acknowledgment of our proposals and hope that in future sessions of the OEWG a proper approach will be led by you Mr. Chair to accommodate all proposals including ours equally. In accordance with founding Resolution [75/240](#), the working method of the group is consensus, and this never entails disregarding views of even a single member state. This is the meaning of consensus and must be preserved and promoted. Our distinguished Chair is rightly believing that the OEWG itself is a confidence-building measure, and we agree with that, however, if concerns and interests of all member States would not be considered, such needed confidence and trust as one of the valuable features of the OEWG will gradually be diminished.

To avoid such a situation, we reiterate the necessity of beginning negotiations based on a rolling text, paragraph by paragraph negotiations, exploring different avenues of informal diplomacy, and launching fruitful dialogue to cover the gaps and discuss the differences, all under the direction of the esteemed Chair.

Last but not least, in light of the latest version of the annual report, we align ourselves with the statement delivered by Russia on behalf of the Like-Minded Group and furthermore we are obliged to disassociate ourselves from any of APR provisions that are not consistent with our national policy, laws and regulations as well as our national values and priorities.

I thank you, Mr. Chair!

Israel

Mr. Chair,

The Israeli delegation wishes to express its gratitude and commend you personally, together with your excellent team and the secretariat, for your hard work and relentless efforts leading us through the OEWG process and especially in crafting this year's final annual progress report.

Some of the reservations we have raised during this week remain unanswered, and not all our concerns were fully addressed in the final version of the report that was just adopted. However, in the spirit of consensus, wishing to express positive will, and in light of the constructive cooperation shown during the last few days by so many delegations, Israel joined the consensus and supported this report. We can assure you that the Israeli delegation remains committed, as you, to work with other states and to continue to present a constructive approach and advance the dialogue in the OEWG.

This being said, it is very important for us at this point to raise and clarify our positions regarding few key elements:

As for paragraph 19 – we recognize that this paragraph is based on agreed language taken from paragraph 17 of the OEWG 2021 and from last year's APR. However, in our view it needs to be noted that voluntary norms, international law and CBMs, from a legal standpoint, are not on an equal footing and cannot, strictly speaking, be all characterized as “obligations”. Two of them, norms and CBMs, are voluntary measures. We believe that the text should reflect this fundamental difference in legal standing. We therefore suggest that in future references the word “obligations” would not be used in connection to all three categories.

As per section C paragraph 23h – We wish to clarify and reiterate that while some states hold the view that further development of norms and the implementation of existing norms could take place in parallel, Israel's position is that it would be more conducive to reach higher levels of implementation of existing norms before moving to developing additional ones. As things currently stand, there is a lack of certainty as to the manner in which existing norms are being implemented and interpreted. The 2015 GGE norms are voluntary and nonbinding, and do not detract from or extend beyond international law. They are meant to signal expectations of the international community regarding appropriate state behavior, and from what we have seen thus far, their implementation has been at best uneven. Before embarking on a project of developing new norms, it would be more appropriate, in Israel's view, to focus on those norms that currently exist, to assess whether and how they are being understood and applied, ensuring that there exists a common language when referring to these norms. Once this is done, we as a community can begin to consider if there are any gaps or a need to clarify, enhance or even to reconsider the original norms. Only then we can assess whether there exists a need for additional norms.

As per section D paragraph 30 d – with regards to the reference made to the principle in the UN Charter of non-intervention, we suggested aligning the text with the language previously used during the OEWG and deleting the words “directly or indirectly” which in our view may create, in the context of cyberspace, more questions than clarity. In our view, the APR should refrain from introducing interpretative elements to the enumerated principles.

Furthermore, regarding paragraph 32 – we would like to emphasize that this paragraph reflects deep disagreement within the members of the OEWG and the notion of elaborating additional binding obligations is far from being agreed. As we and many others have stated, at this point in time, there is no consensus over the need to develop additional legally binding obligations and therefore such elaboration is

neither necessary nor appropriate. This passing year has demonstrated the heightened risks and threats associated with cyber, as well as the clear responsibility of governments to provide security to their citizens and safeguard national interests. This requires cautious application of time proven principles, confidence building measures, inter-State cooperation, and capacity building. As we have stated in the past, Israel stands ready to share its know-how, further develop bilateral and multilateral collaborations, and take other pragmatic steps to improve cybersecurity across the globe.

Finally, Mr. Chair regarding section E on the regular institutional dialogue, we wish to reiterate and clarify our position on the issue of consensus in this context. Throughout this process we have persistently made clear that it is imperative that all decisions in a regular Institutional dialogue, whether in the context of the PoA or any other mechanism be made be based on consensus, applied both to the negotiation processes, as well as to the decision-making process within it. Be it in relation to substantive matters or procedural ones.

Mr. Chair, in the spirit of flexibility we were willing to accept the wording “principle of consensus” in para 56 and wish to emphasize that we understand them as reflecting the application of consensus to both the procedural matters and the substantive matters alike, and to be put into practice in the next phases of our deliberations on the creation of any future Regular Institutional Dialogue, including a PoA.

In conclusion, Israel is pleased to see the adoption of the second progress report of the OEWG and hopes that the report serves as a roadmap for the continuation of our discussions in the group. We also wish that our perspectives and concerns will be taken in account and reflected in a better way in the future work of the OEWG.

Thank you Chair.

Russian Federation

Уважаемый господин председатель,

Уважаемые коллеги,

Российская Федерация присоединилась к консенсусу по ежегодному промежуточному докладу Рабочей группы открытого состава (РГОС) ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, поскольку нам удалось отразить в нем ряд ключевых инициатив, в том числе концепцию конвенции ООН об обеспечении международной информационной безопасности, а также договориться о запуске – по изначально российскому предложению – реестра контактных пунктов.

Тем не менее, мы обеспокоены избирательным подходом ряда стран к трактовке мандата РГОС, перекосом в сторону выполнения добровольных правил, норм и принципов ответственного поведения в ущерб разработке новых. Россия продолжит решительно отстаивать строгое соблюдение мандата Группы. Не позволит подчинить ее работу интересам отдельных государств.

Российская Федерация не считает себя связанной даже добровольными обязательствами по тем положениям доклада, которые противоречат нашему законодательству и национальным интересам.

Прошу председателя включить наше выступление в сборник заявлений с разъяснением позиций государств по промежуточному докладу РГОС.

Благодарю за внимание.

Distinguished Mr. Chair,

Dear colleagues,

The Russian Federation has joined consensus on the annual progress report of the UN Open-ended Working Group (OEWG) on Security of and in the Use of ICTs 2021–2025 because we managed to reflect in it a number of key initiatives, including the concept of a UN convention on ensuring international information security, as well as to reach agreement on the establishment of a directory of Points of Contact, initially proposed by Russia.

Nevertheless, we are troubled by the selective treatment of the mandate of the OEWG by some States, disbalance towards the implementation of voluntary rules, norms and principles of responsible behaviour to the prejudice of the development of new ones. Russia will continue to resolutely advocate for a strict observance of the Group's mandate. We will not allow making its work serve the interests of certain States.

The Russian Federation does not consider itself bound even by voluntary commitments stemming from those provisions of the report that contradict our legislation and national interests.

I request the Chair to include our intervention in the compendium of statements with explanations of positions of States on the OEWG's progress report.

Thank you for your attention.

Russian Federation (also on behalf of the Republic of Belarus, the Republic of Burundi, the People's Republic of China, the Republic of Cuba, the Democratic People's Republic of Korea, the Islamic Republic of Iran, the Republic of Nicaragua, the Russian Federation, the Republic of Sudan, the Syrian Arab Republic and the Bolivarian Republic of Venezuela)

Уважаемый господин председатель,

Мы хотели бы выразить признательность Вашему превосходительству и Вашей команде за усилия по подготовке ежегодного промежуточного доклада (ЕПД) и содействие его принятию консенсусом. В духе доброй воли и компромисса мы поддержали консенсус по документу, однако отмечаем наличие существенных недостатков, которые вызывают серьезную озабоченность у наших делегаций.

ЕПД в значительной степени посвящен имплементации правил, норм и принципов ответственного поведения государств в сфере использования ИКТ, при этом едва ли не пренебрегает приоритетной задачей дальнейшей выработки этих норм. Нас беспокоит, что упоминания последней были исключены из некоторых пунктов. Это очевидно противоречит мандату РГОС, который закреплен в резолюции Генеральной Ассамблеи ООН №75/240 и поддержан консенсусом всех государств в резолюции Генеральной Ассамблеи ООН №76/19.

Мы твердо выступаем в поддержку демократичного и способствующего формированию консенсуса процесса РГОС по безопасности в сфере ИКТ, в рамках которого интересы всех государств-членов ООН должны учитываться на равноправной основе.

Кроме того, мы разочарованы включением в доклад положений, касающихся прав человека, международного гуманитарного права, а также избыточным акцентом на гендерные вопросы, несмотря на четко выраженное несогласие

наших стран. Подобные противоречивые темы не следовало включать в проект доклада без достижения консенсуса на сей счет.

В связи с этим мы решительно оставляем за собой право интерпретировать или отвергать положения, которые противоречат нашим базовым принципам, политике, законодательству и ценностям.

Не следует переоценивать роль других заинтересованных сторон в обеспечении информационной безопасности. РГОС представляет собой межправительственный процесс, в котором ведение переговоров и принятие решений являются исключительной прерогативой государств-членов. Мы подчеркиваем, что только аккредитованные представители бизнеса, НПО и научно-академического сообщества, включая специалистов в области права, могут участвовать в деятельности РГОС.

Мы вновь подчеркиваем насущную необходимость урегулирования ситуации с выдачей – своевременной и в полном объеме – виз всем национальным делегациям и негосударственным субъектам, а также обеспечения соблюдения страной, принимающей центральные учреждения ООН, ее юридических обязательств.

По мере приближения РГОС к завершению своей деятельности принципиально важно в приоритетном порядке добиваться достижения подлинного консенсуса. Нас разочаровывает, что подходы и конкретные предложения не получают заслуженного внимания и приносятся в жертву политическим предпочтениям отдельных стран. Искоренение подобной практики не только исключительно важно для данного конкретного процесса, но имеет первостепенное значение для эффективности любого будущего процесса по международной информационной безопасности.

Мы любезно просим председателя включить настоящее заявление, а также выступления данной группы государств в сборник заявлений с разъяснением позиций государств по ЕПД и разместить на соответствующих порталах и веб-сайтах.

Благодарю за внимание.

Distinguished Mr. Chair,

We would like to express our appreciation for the effort put by Your Excellency and your team into developing the annual progress report (APR) and facilitating its consensual adoption. While supporting consensus on the document in the spirit of good will and compromise, we acknowledge the presence of significant flaws that are of deep concern to our delegations.

The APR is, to a large extent, devoted to the implementation of rules, norms and principles of responsible behaviour of states in the use of ICTs, while almost ignoring the priority task to further develop these norms. It is concerning that references to the latter have been removed from some paragraphs. This clearly contradicts the mandate of the OEWG as enshrined in the UNGA resolution [75/240](#) and supported by consensus of all States in the UNGA resolution [76/19](#).

We have been strong advocates of this democratic ever and consensus-building process of the OEWG on security of ICTs in which every Member State must be treated on an equal standing.

Moreover, we are disappointed by the inclusion of language on human rights, international humanitarian law, as well as the overemphasis on gender issues, despite

clear disagreement of like-minded delegations. Such contentious topics should not have been incorporated in the report without achieving a consensus.

Therefore, we do vehemently reserve the right to interpret or reject those provisions that contradict our national fundamental principles, policies, laws, regulations and values.

The role of other interested parties in ensuring information security should not be overestimated. The OEWG is an intergovernmental process in which negotiation and decision-making are exclusive prerogatives of the Member States. We stress that only accredited representatives of businesses, NGOs and academia, including legal experts, have the right to participate in the activities of the OEWG.

We once again underline the urgency of resolving the visa issue for all national delegations and accredited non-governmental entities in a full and timely manner, ensuring the adherence to its legally binding obligations by the host country.

As the OEWG approaches its conclusion, it is of utmost importance to prioritize achieving greater consensus. It is disheartening to witness our perspectives and concrete proposals not receiving the attention they deserve and being affected by undue political agendas of some States. Eradicating such a situation is not just essential for this specific process, but also paramount for the efficiency of any future processes on international information security.

We kindly ask the Chair to include this statement, as well as the interventions of this group of states in the compendium of statements on the APR and make them available at relevant portals and websites.

Thank you for your attention.

South Africa

Thank you, Chairperson.

We recognize the time and effort that you and your team have invested in this document.

The adoption of this draft 2023 Annual Progress Report, contained in the CRP, would be an important step forward for countries interested in developing their cybersecurity infrastructure and maintaining an open, secure, stable, peaceful, interoperable and accessible ICT environment.

The text provides us with the two overarching confidence-building measures: the continued work of the OEWG and the Points of Contact directory. Discussion on the different formats for exchange of views between States on potential and emerging threats have shown us that we, the international community, can engage during difficult geopolitical times. We have endorsed the capacity-building principles agreed to in the first OEWG report in 2021. Our agreement on the way forward with various stakeholders is a potential way forward in any future framework of regular institutional dialogue. And we thank the Chair for providing us with section H of the report and Annex D, reflecting the broad participation of States in the OEWG at all levels.

Chairperson,

This process has always been about peaceful cooperation between States. We understand that delegations have expressed differing views on the nature of the framework for regular institutional dialogue. We can only underscore not reaching consensus on the entire document would reverse the gains we have made in moving our discussion forward with concrete actions. It would also mean that trust and

confidence between States is undermined. South Africa is not eager for further ripple effects in other areas of multilateral cooperation.

South Africa has come to this meeting in good faith to ensure that the dialogue between States takes place under the auspices of the United Nations – a universal, multilateral forum that promotes peaceful settlement of disputes. We are grateful for the opportunity to promote balanced perspectives on the cumulative and evolving framework on ICT security.

Chairperson,

We reiterate our commitment to work with the international community under the auspices of the United Nations to develop a framework that is inclusive, open, transparent and effective.

While we did not get everything we want, and had to be flexible to accept proposals from other delegations so that we could move this process forward, South Africa stands ready to adopt the text as it is.

I thank you.

Switzerland

La Suisse se félicite de l'adoption du deuxième rapport d'activité annuel. Il constitue une base solide pour les travaux futurs de ce GTCNL. Nous nous réjouissons tout particulièrement de la possibilité de poursuivre la discussion sur l'application du droit international dans le cyberspace au sein de ce GTCNL sur la base de ce rapport.

Nous tenons à remercier le président et son équipe pour tous les efforts et le leadership qui nous ont guidés tout au long de la cinquième session et qui nous ont aidés à surmonter les divergences de vues. Nous remercions également toutes les délégations d'avoir fait preuve de souplesse pour parvenir à un rapport consensuel.

Le rapport n'est pas parfait, comme nous l'avons déclaré à l'occasion de son adoption, mais il atteint un équilibre délicat. Le rapport contient des éléments qui sont importants et précieux pour nous, d'autres sont problématiques de notre point de vue; plusieurs des points qui sont importants pour nous n'ont pas été inclus. Nous aurions par exemple souhaité une section plus ambitieuse sur le droit international, qui reflète de manière plus complète les discussions ciblées et les progrès que nous avons réalisés au sein de ce groupe.

Mais, et c'est là un point crucial, le rapport reflète également l'engagement important et actif d'un grand nombre d'États et d'autres parties prenantes lors des sessions formelles et des réunions informelles de ce groupe. L'annexe D en est la preuve et il appartient maintenant au GTCNL d'exploiter les progrès accomplis et de s'en inspirer lors des prochaines sessions.

La Suisse souhaite commenter brièvement quelques parties du rapport, de manière non exhaustive.

La Suisse salue le fait que le rapport mentionne pour la première fois au paragraphe 11 que les TIC ont déjà été utilisées dans des conflits dans différentes régions. Il s'agit d'une réalité, particulièrement vraie dans la guerre contre l'Ukraine, qui devait être reflétée dans le rapport. La Suisse estime que les menaces existantes et potentielles pour la paix et la sécurité internationales qui peuvent découler de cette utilisation, ainsi que leur compatibilité avec le droit international, en particulier le droit international humanitaire, devraient faire l'objet d'un examen approfondi au sein du GTCNL.

Nous saluons également la mention des ransomwares et de l'Internet des objets dans la section sur les menaces. La Suisse, comme beaucoup d'autres délégations, aurait également souhaité que l'intelligence artificielle et l'informatique quantique soient mentionnées. Nous pensons que les États et les parties prenantes devraient également échanger leurs points de vue sur ces technologies émergentes lors des prochaines sessions du GTCNL.

La Suisse se félicite de l'accent mis sur la protection des infrastructures critiques et des infrastructures d'information critiques contre les menaces liées aux TIC et de la recommandation de poursuivre les discussions sur ce sujet. Les récents cyber incidents et la situation géopolitique actuelle ont montré que la protection des infrastructures critiques devient de plus en plus importante. La Suisse estime qu'il serait utile de se concentrer sur les normes 13 c, f, g et h qui appellent à la protection de toutes les infrastructures critiques soutenant les services essentiels au public, en particulier les installations médicales et de soins de santé, ainsi qu'à la coopération entre les États à cette fin.

Dans ce contexte, la Suisse est d'avis qu'à l'heure actuelle, le GTCNL devrait se concentrer sur une meilleure compréhension, promotion et mise en œuvre des 11 normes volontaires existantes avant d'en élaborer de nouvelles. La Suisse souhaite rappeler le mandat du GTCNL, tel qu'énoncé au paragraphe 4, selon lequel des règles de comportement supplémentaires ne devraient être élaborées que si cela s'avère nécessaire.

La Suisse se félicite de la section sur le droit international et de la réaffirmation que le droit international, en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix, de la sécurité et de la stabilité et à la promotion d'un environnement TIC ouvert, sûr, stable, accessible et pacifique. La Charte des Nations Unies est un cadre juridique essentiel applicable au cyberspace. La Suisse est d'avis que la Charte est applicable dans son intégralité dans le cyberspace. Nous aurions préféré le mentionner également dans le rapport.

Avec le Canada, la Suisse s'est engagée à mener des discussions ciblées au sein du GTCNL sur des sujets spécifiques de droit international et a fait des propositions concrètes dans un document de réflexion. Nous nous félicitons que ces discussions ciblées aient eu lieu et que le rapport en rende compte, ainsi que des progrès que nous avons réalisés au sein de ce GTCNL. Un nombre record d'États se sont engagés dans des discussions ciblées et ont partagé leurs points de vue sur l'applicabilité du droit international dans le cyberspace. Ils ont ainsi montré leur engagement à faire progresser la compréhension commune de la manière dont le droit international s'applique dans le cyberspace. Bien que nous aurions souhaité que les discussions soient reflétées de manière plus détaillée, la Suisse soutient particulièrement la recommandation de poursuivre de telles discussions ciblées, y compris sur le droit international humanitaire, et voit beaucoup de mérite dans la recommandation d'organiser des briefings d'experts par le président.

La Suisse se félicite également de l'accent mis par le rapport sur les positions nationales et le renforcement des capacités dans le domaine du droit international.

En ce qui concerne le paragraphe 32, la Suisse souhaite rappeler sa position, à savoir qu'un nouvel instrument juridiquement contraignant n'est pas nécessaire à l'heure actuelle. Cela serait prématuré et inutile. À ce stade, le GTCNL devrait poursuivre ses travaux sur l'élaboration d'une compréhension commune de l'application du droit international existant dans le cyberspace. Nous devons faire la distinction entre la discussion ciblée sur des sujets de droit international et les conclusions que les États peuvent tirer de ces discussions, en particulier la question de savoir s'il existe des lacunes et, le cas échéant, lesquelles, et comment les États souhaitent les combler.

La Suisse souhaite également souligner qu'elle ne soutient pas l'argument d'une délégation selon lequel il n'y a pas de responsabilité dans le cyberspace sans une nouvelle convention. Il s'agit d'une déclaration inquiétante et potentiellement dangereuse qui sape tout ce que nous, en tant qu'États, avons développé au cours des dernières années et adopté par consensus au sein des GEG, des GTCNL et de l'Assemblée générale des Nations Unies. Au contraire, le droit international existant, en particulier la Charte des Nations unies et les normes juridiquement contraignantes sur la responsabilité des États, constituent la base de la responsabilité des États pour des actes illicites, y compris dans le cyberspace.

La Suisse se félicite de la décision d'établir un répertoire mondial et intergouvernemental de points de contact et de l'adoption du document intitulé "Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory", qui figure à l'annexe A du présent rapport. La Suisse participera de manière constructive à sa mise en place, mais souhaite rappeler sa position, à savoir que le répertoire des points de contact ne doit pas faire double emploi avec le travail des équipes d'intervention en cas d'urgence informatique (CERT) et des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT).

La réduction de la fracture numérique par des efforts adaptés de renforcement des capacités reste une priorité essentielle pour la communauté internationale afin de promouvoir un cyberspace ouvert, libre et sûr. Le rapport contient de nombreuses suggestions précieuses sur la manière dont le GTCNL peut contribuer à cette cause. La promotion des synergies et de la coordination entre les initiatives et programmes existants nous semble particulièrement importante. La Suisse estime que le maintien et l'amélioration d'un certain degré de coordination est nécessaire pour renforcer l'impact de ces initiatives et programmes. Cependant, comme d'autres délégations, la Suisse ne voit pas la nécessité de créer un mécanisme de renforcement des capacités cybernétiques à l'ONU à ce stade, mais de mieux utiliser ceux qui existent déjà, comme le GFCE.

La Suisse soutient les discussions en cours sur l'établissement d'un programme d'action des Nations Unies sur la cybersécurité au sein du GTCNL. Elle estime que ce programme d'action est le mieux à même de devenir le nouveau dialogue institutionnel régulier, sur la base des éléments communs énoncés au paragraphe 55, et se félicite de la recommandation visant à poursuivre des discussions ciblées dans le cadre du GTCNL.

Sur la base du rapport et des recommandations qu'il contient, la Suisse continuera à participer de manière constructive aux travaux du GTCNL.

Switzerland welcomes the adoption of the second Annual Progress Report. It is as a solid basis for the future work of this OEWG. We particularly welcome the opportunity to continue the discussion on the application of international law in cyberspace at this OEWG based on the report.

We would like to thank the Chair and his team for all the efforts and leadership that guided us through the 5th Session and helped bridge the differences in positions. And we would like to thank all delegations for showing flexibility in reaching a consensus report.

The report is not perfect, as we have stated on the occasion of the adoption, but it strikes a delicate balance. The report contains elements that are important and valuable for us, others are problematic from our point of view; several of the points that are important to us were not included. We would for example have liked to see a

more ambitious international law section that reflects the focused discussions and progress we have made in this group in a more comprehensive way.

But, and this is crucial, the report also reflects the great and active engagement of so many states and other stakeholders in the formal sessions and informal meetings of this group. Annex D is proof of this and it is now up to the OEWG to harness the progress made and build on it in the coming sessions.

Switzerland would like to briefly comment on a few parts of the report in a non-exhaustive manner.

Switzerland welcomes the fact that the report mentions for the first time in paragraph 11 that ICTs have already been used in conflicts in various regions. This is a reality, particularly true in the war against Ukraine, and needed to be reflected in the report. Switzerland believes that the existing and potential threats to international peace and security that may arise from such use, as well as their compatibility with international law, in particular international humanitarian law, should be discussed further in depth in the OEWG.

We also welcome the mention of ransomware and the Internet of Things in the threats section. Switzerland, like many other delegations, would also have liked to see artificial intelligence and quantum computing mentioned. We believe that States and stakeholders should also exchange views on these emerging technologies in the coming sessions of the OEWG.

Switzerland welcomes the strong emphasis on protecting Critical Infrastructure and Critical Information Infrastructure from ICT threats and the recommendation for further focused discussions on this. Recent cyber incidents and the actual geopolitical situation have shown that the protection of critical infrastructures becomes ever more important. Switzerland would see merit focusing on Norms 13 c, f, g and h) calling for the protection of all critical infrastructure supporting essential services to the public, in particular medical and healthcare facilities as well as cooperation between States for this purpose.

In this context, Switzerland is of the opinion that at the moment the OEWG should focus on better understanding, promotion and implementation of the existing 11 voluntary norms before developing new ones. Switzerland would like to recall the mandate of the OEWG as stated in paragraph 4 that additional rules of behaviour should only be developed if necessary.

Switzerland welcomes the section on International law and the reaffirmation that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. The UN Charter is a key legal framework applicable in cyberspace. It is Switzerland's position that the Charter is applicable in its entirety in cyberspace. We would have preferred to mention this in the report as well.

Together with Canada, Switzerland has committed itself to focused discussions in the OEWG on specific topics of international law and has made concrete proposals in a concept paper. We welcome the fact that such focused discussions have taken place and that the report reflects them and the progress we have made in this OEWG. A record number of States engaged in focused discussions and shared their views on the applicability of international law in cyberspace. Thereby showing their commitment to furthering the common understanding of how international law applies in cyberspace. While we would have liked the discussions to have been reflected in more detail, Switzerland particularly supports the recommendation to continue such focused discussions, including on international humanitarian law and sees a lot of merit in recommendation for the arrangement of expert briefings by the Chair.

Switzerland also welcomes the report's emphasis on national positions and capacity building in the area of international law.

With regard to paragraph 32 Switzerland would like to recall its position, that there is currently no need for a new legally binding instrument. This would be premature and unnecessary at this time. At this point the OEWG should continue its work on developing common understandings on the application of existing international law in cyberspace. We should distinguish between the focused discussion on international law topics and the conclusions that states may draw from such discussions, in particular whether and if so which gaps exist and how States want to deal with them.

Switzerland would also like to note that it does not support the argument of one delegation that there is no accountability in cyberspace without a new convention. This is a worrying and potentially dangerous statement that undermines everything we as states have developed over the past years and adopted by consensus in the GGEs, the OEWGs and the UN General Assembly. On the contrary, existing international law, in particular the UN Charter and the legally binding norms on state responsibility provide the basis for accountability of states for wrongful acts, including in cyberspace.

Switzerland welcomes the decision to establish a global, inter-governmental points of contact (POA) directory and the adoption of the paper entitled "Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory" as contained in Annex A of this report. Switzerland will constructively engage in its establishment but would like to recall its position, that the POC directory should not duplicate the work of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

Narrowing the digital divide through tailored capacity-building efforts remains a key priority for the international community in order to promote an open, free and secure cyberspace. The report contains many valuable suggestions on how this OEWG can contribute to this cause. Promoting synergies and coordination between existing initiatives and programmes seems particularly important to us. Switzerland believes that maintaining and improving a certain degree of coordination is necessary to hone the impact of such initiatives and programmes. However, as other delegations, Switzerland does not see a need to create a Cyber capacity-building mechanism at the UN at this point but to make better use of existing ones like the GFCE.

Switzerland supports the ongoing discussions on the establishment of a UN Program of Action on Cybersecurity (PoA) in the OEWG. Switzerland believes that the PoA is best suited to become the new regular institutional dialogue, based on the common elements contained in paragraph 55, and welcomes the recommendation to continue to engage in focused discussions in the framework of the OEWG.

Based on the report and the recommendations contained therein, Switzerland will continue to participate constructively in the work of the OEWG.

United Kingdom of Great Britain and Northern Ireland

The United Kingdom extends its thanks to the Chair of the Open-Ended Working Group, Ambassador Gafoor, his team, and the UN Office for Disarmament Affairs Secretariat for their efforts to facilitate meaningful discussions this year and to bring Member States to agree to establish the global Points of Contacts directory and deliver a consensus Annual Progress Report.

These are significant and meaningful achievements. The Points of Contact directory will allow States to build confidence and reduce tensions. The Annual Progress Report

reflects our discussions, which have benefited from increasingly wide participation and detailed expert briefings, and provides a roadmap for next year's meetings.

The United Kingdom was especially pleased that we were able to reach consensus on future intersessional meetings, including on the application of international law to cyberspace and the consideration of the Programme of Action as a means of future Regular Institutional Dialogue.

However, we are concerned by the risk that the consensus principle which governs this Working Group could be misused or undermined. We note the spirit of consensus that led many States, ourselves included, to sacrifice references to new proposals that did not enjoy sufficient support. The consensus modality is an important element of our Working Group and should not be abused. We urge States to refrain from using it as a veto.

In this context, we were also disappointed that this Working Group did not take further opportunities to reaffirm our existing consensus agreements in more detail. We have agreed that international law applies in cyberspace, a position reaffirmed by the General Assembly. This includes the UN Charter; Chapter 6 in its entirety and Article 33(2); the law of state responsibility; and International Humanitarian Law. We believe these should have been referenced in the Report and we look forward to focussed discussions in the coming year to help us deliver further articulations of the application of international law to cyberspace.

The United Kingdom will take every opportunity to reaffirm and support the implementation of the Framework of Responsible State Behaviour in the Use of ICTs. We urge all Member States to do the same.

We look forward to engaging constructively in this Open-Ended Working Group over the coming year.
