United Nations A/AC.292/2022/INF/4

General Assembly

Distr.: General
7 September 2022
English
Original: English/Russian/Spanish

Open-ended working group on security of and in the use of information and communications technologies 2021–2025
Third substantive session
New York, 25–29 July 2022

Compendium of statements in explanation of position on the adoption of the progress report of the open-ended working group as contained in A/77/275, annex

Note by the Secretariat

1. At its third substantive session, on 29 July 2022, 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), entitled "Adoption of annual progress reports". The working group adopted its draft report as contained in document A/AC.292/2022/L.1. It also decided to include in its report the outcome of the substantive discussions of the working group on agenda item 5. The report of the working group, including the annexed progress report on discussions on agenda item 5, was issued on 8 August 2022 as document A/77/275.

2. Pursuant to paragraph 17 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.

22-21515 (E) 120922 120922

Contents

Australia

Note: a truncated version of this statement was delivered orally on 29 August 2022 before adoption of the Annual Progress Report; the full statement is provided for the record.

Chair, distinguished colleagues

Today, Australia is pleased to join consensus on this OEWG annual progress report. It is testament to the tenacity of our Chair, the importance all of our governments ascribe to this issue, and the joint commitment of each delegation, that we have maintained momentum in our discussions notwithstanding the unprecedented geopolitical reality in which we meet.

This week, the good faith and dedicated engagement from all delegations has shone through each intervention. Today, in our final day of meetings, we have before us a report balanced on a knife's point. Like many, there are parts of this report with which Australia is uncomfortable. And there are many things that we would have liked to have seen included which are not. However, Australia believes this is the most balanced report we could hope for in the circumstances. It is now incumbent on each of us to preserve that balance.

Australia urges all those with concerns about this report, to use explanations of positions as an opportunity to put those concerns on the record in a transparent way.

In this vein, Australia offers the following non-exhaustive explanation of position.

Australia welcomes the unequivocal reaffirmation of the framework of responsible state behaviour in cyberspace (international law, norms, confidence building measures and capacity building) as endorsed by all countries in General Assembly Resolution 70/237.

Australia welcomes the explanation of the threats we face in a way that provides the context against which the following chapters flow, and the context through which the work of this group becomes meaningful.

Australia would have liked to see further elaboration of the current and growing threats to international peace and security in cyberspace, particularly those raised by States in our first and second sessions including the threat of ransomware, and recognition that the use of ICTs in the context of armed conflict in no longer becoming more likely, but is a reality.

Australia welcomes reaffirmation that international law, and in particular, the UN Charter, applies to States' activities in cyberspace, and the report's recollection that international humanitarian law applies in cyberspace.

In this regard, Australia understands "international law" to be the entire corpus of international law. Australia underscores – as reflected in the quotation at paragraph 15(b) (i) the report – that there was no agreement among States on the need for additional legally binding obligations. Australia's position, as previously expressed in this forum, is that existing international law and the agreed norms provide a comprehensive and robust framework to address the threats posed by state-generated or state-sponsored malicious cyber activity. However, this framework will only be effective when it is implemented, adhered to and enforced. Therefore, rather than negotiating additional legally binding obligations, Australia's priority is on increasing implementation, adherence and enforcement of the existing framework. We look forward to discussions on specific topics of international law, including international humanitarian law, in future sessions of the OEWG.

Australia welcomes the strong, practical recommendations for implementation of measures that build trust and confidence in cyberspace, and in particular the establishment of a global point of contacts directory. We look forward to future elaboration of these measures in our sessions next year.

Australia welcomes the strong emphasis on the importance of capacity building, as well as reference to our agreed set of principles to guide these efforts, and reference to CERT-CERT cooperation.

Australia welcomes the call for countries to survey implementation and share national views and best practices with respect to norms (pp30), international law (pp38), confidence building measures (pp48) and capacity building (pp64), as well as recommendations to use on a voluntary basis the model "National Survey of National Implementation".

Australia also welcomes, with appreciation, the important contribution of the multistakeholder community and recognition in the report of the importance of substantial engagement will all voices.

Australia warmly welcomes the report's recognition of the high level of participation by women delegates and the prominence of gender perspectives in the discussions. In this regard, Australia recognises in particular the contributions of the Women in Cyber Fellows, whose participation has enriched the process, and improved our joint outcome.

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 report is not the end of our work.

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

Chile

Muchas gracias señor presidente,

Al ser la primera vez que hacemos uso de la palabra, mi delegación quisiera extender su agradecimiento y valorar el trabajo realizado por usted, Embajador Gafoor, su equipo, y la secretaría de la Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA), en la elaboración de la versión revisada del proyecto de informe anual de progreso de este Grupo de Trabajo de Composición Abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (OEWG).

En términos generales, Sr. Presidente, este documento nos parece un buen punto de partida para nuestras discusiones. Compartimos la esperanza de que este texto pueda ser aprobado por consenso. En pos del tiempo y de su llamado, seremos breves.

Como gobierno feminista, todas las acciones del Estado están enfocadas en la paridad de género y la igualdad. Así, nuestra Política Exterior feminista está enfocada en reforzar la promoción de los derechos humanos de las mujeres, niñas y disidencias en foros multilaterales y organismos internacionales.

En ese sentido, recibimos con beneplácito la inclusión de nuestros comentarios en la introducción del documento, respecto a la mención explícita de la participación de mujeres delegadas en estas sesiones, como una medida que apunta a la inclusión de una perspectiva de género en estas negociaciones. Por ello, apoyamos la solicitud de revisión de lenguaje realizada ayer por la distinguida delegación de Australia, que

creemos aporta a clarificar los puntos expuestos. Apoyamos también lo recientemente expresado por la distinguida delegación de Canadá.

Asimismo, agradecemos y reconocemos el establecimiento de la "Women in cyber fellowship", de la cual soy parte, y los esfuerzos de sus sponsors, especialmente de Canadá, en la inclusión de mujeres en este proceso. Cabe recordar que la mención a temas de género es indispensable y se sostiene en mandatos existentes en el marco de Naciones Unidas, especialmente en la esfera de la seguridad internacional. No se trata sólo de tener más mujeres sentadas en esta sala, no somos un número, se trata de hacer de este un proceso inclusivo, equitativo y efectivo en materia de género.

Señor presidente,

Agradecemos que en la introducción se reconozcan los esfuerzos regionales y subregionales en este informe. No se trata de que las instancias regionales sean más o menos importantes que la configuración global de Naciones Unidas, sino que son necesarias, especialmente para la implementación de las medidas establecidas y el reconocimiento del trabajo realizado. A pesar de ello, reconocemos que no todos los Estados son parte de estas instancias, por lo que valoramos la propuesta realizada por la distinguida delegación de México ayer, en el sentido de realizar una mención a organizaciones regionales y otros esfuerzos y mecanismos regionales, subregionales e interregionales, de manera tal de no dejar a nadie atrás y hacer de este un proceso realmente inclusivo.

Respecto a las secciones sobre "Amenazas reales y potenciales" y "Normas, reglas y principios", nuestro país no tiene mayores comentarios o sugerencias respecto a la redacción y el lenguaje utilizados.

Entendemos que este es un primer informe del grupo y un primer paso para las negociaciones futuras, por lo que consideramos relevante el intercambio de experiencias, que apunten a reducir brechas digitales, enfrentar amenazas reales y potenciales, y avanzar en la correcta utilización del ciberespacio, y en ese escenario, no estamos seguros de si es lo propicio realizar un listado exhaustivo de amenazas, por fines de estructura del informe y la posibilidad de que ello limite futuros debates en torno a nuevas amenazas. Sin embargo, somos flexibles si la mayoría de los países consideran relevante realizar estas menciones en este documento, por ejemplo, respecto a una mención explícita a ransomware.

Chile considera que las amenazas pueden afectar de distinto modo a los Estados en función de sus niveles de digitalización, capacidad, seguridad y resiliencia de las tecnologías de la información y las comunicaciones, su infraestructura y desarrollo. Las amenazas también pueden afectar de forma distinta a distintos grupos y entidades, teniendo especialmente presente a las mujeres y niñas.

Estados como el nuestro tienen otro tipo de amenazas y necesidades, por lo que se vuelve fundamental avanzar en mejorar nuestras capacidades, generando estructuras y planes de coordinación, no solamente a nivel de gobierno, sino también el desarrollar alianzas efectivas con la sociedad civil, el sector privado, y la academia.

Por otro lado, y tal como fuese solicitado ayer, nos referiremos a la sección sobre derecho internacional. Chile considera que el derecho internacional, y en particular la Carta de las Naciones Unidas, proporcionan el marco normativo aplicable que debe regular el comportamiento de los Estados en el ciberespacio, incluyendo el derecho internacional humanitario, los derechos humanos y aquellas leyes que regulan la responsabilidad internacional de los Estados, por ser esenciales para mantener la paz y la estabilidad necesaria para promover un entorno abierto, seguro, estable, accesible y pacífico en las tecnologías de la información y las comunicaciones.

Nos complace observar que este nuevo borrador contiene una referencia directa al derecho internacional humanitario como uno de los temas específicos sobre los que el Grupo de Trabajo de Composición abierta podría convocar a futuros debates.

Esto, sin duda, nos permitirá generar entendimientos comunes sobre cómo podemos proteger a la población civil, y tener claridad sobre qué acciones son prohibidas o inaceptables durante una situación de conflicto. En tal sentido, recordamos que nuestro país se ha sumado al comunicado conjunto recientemente leído por la distinguida delegación de Suiza, en el que reafirmamos que el derecho internacional humanitario aplica al ciberespacio y que la explicación de cómo éste aplica a las operaciones cibernéticas en el marco de los conflictos armados es una prioridad en los debates futuros.

Respecto a medidas de fomento de la confianza, nos complace observar la referencia de que este Grupo de Trabajo de Composición Abierta es, en sí mismo, una medida de fomento de la confianza. Creemos en esta instancia, por ser un espacio donde los Estados podemos intercambiar nuestras perspectivas, enfoques y necesidades, reforzando la seguridad, la resiliencia y el uso pacífico de las TICs en general.

En ese sentido, y respecto a la creación de un directorio global e intergubernamental de puntos de contacto nacionales, nuestra delegación considera que las organizaciones e instancias regionales pueden jugar un rol clave en la coordinación de esta instancia, especialmente porque ya existen acciones en este nivel y podría ser una oportunidad de realizar un trabajo integral, cooperativo y complementario a las labores de este Grupo, con miras a no duplicar esfuerzos. Un ejemplo de ello son las labores que realiza en mi región el Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA).

Nuestra delegación solamente tiene una sugerencia en el punto 6 de las medidas de fomento de confianza, respecto a los próximos pasos recomendados. En particular respecto a la convocatoria de una reunión inter-sesional, nos gustaría sugerir se considere la inclusión de los organismos e instancias regionales en la convocatoria de esta reunión, considerando su experiencia en el trabajo sobre medidas de fomento de la confianza, y también sobre el establecimiento de Puntos de Contactos. En tal sentido, destacamos, como lo hemos hecho anteriormente, el importante trabajo realizado por la OEA a través del Grupo de Trabajo sobre medidas de fomento de la confianza en el ciberespacio.

Señor presidente,

Chile aplaude la aprobación de las modalidades de participación de los stakeholders, sin embargo, nos sumamos a las voces que han señalado que la pluralidad efectiva es importante en este Grupo de Trabajo de Composición Abierta. Lamentamos que se hayan realizado vetos, especialmente porque reconocemos que este es un trabajo conjunto.

De esta manera, realizaremos nuevos aportes en la medida que avance la agenda de este encuentro, entendiendo las características de este estado de negociación y del texto presentado por esa Presidencia.

El ciberespacio, sus amenazas y desafíos no conocen límites y es necesario e imperante que podamos aunar esfuerzos hacia un camino común que nos permita avanzar de manera concreta. Debemos ir más allá de los acuerdos reflejados en papel, y así poder lograr resultados y avances concretos. En tal sentido, Chile manifiesta abiertamente su voluntad y disposición para que este proceso pueda avanzar y poder lograr, al final de esta semana, la aprobación por consenso del informe.

Muchas gracias.

STATEMENT 2REV. DRAFT
-28-07-2022-

Muchas gracias señor presidente,

Gracias. Muchas gracias por su trabajo y el de su equipo en la elaboración de este nuevo draft de texto. Apreciamos su esfuerzo por tratar de consolidar un documento que recoja las posiciones de todos los países aquí presentes.

Nuestra intención no es caer en repeticiones de lo antes mencionado, sin embargo, creemos importante aprovechar esta ocasión para hacer algunos comentarios generales a esta nueva versión de Informe.

En primer lugar, agradecemos que se haya considerado la solicitud de menciones a organizaciones e instancias regionales y subregionales de manera transversal. Tal como observamos en las recientes presentaciones de las y los representantes de diversas organizaciones regionales, su trabajo y labor es fundamental para el funcionamiento y avance de este grupo de trabajo. Sin embargo, aún debemos recordar que la Carta de Naciones Unidas reconoce la existencia de los acuerdos u organismos regionales en el desarrollo de sus funciones, especialmente en materia de mantenimiento de la paz y seguridad internacionales.

Chile es un país de América Latina, con desafíos y particularidades, como todos los Estados aquí presentes. Sin embargo, no todos compartimos las mismas herramientas y capacidades para desarrollarnos, y enfrentar los desafíos que trae consigo el ciberespacio. Digo esto, señor presidente, porque nos ha llamado profundamente la atención que se hayan eliminado diversas menciones, a través de todo el documento, a medidas e iniciativas relacionadas con la cooperación.

En ese sentido, apoyamos lo mencionado por Croacia, Colombia, Costa Rica y otros estados. Ello, especialmente respecto a la mención de los CSIRTs en este documento. Por ello, quisiéramos expresar abiertamente nuestro apoyo a la propuesta de lenguaje presentada por la delegación de Colombia en este tema.

Cabe destacar que en nuestra región se ha fortalecido el trabajo y cooperación de los CSIRTs a través de la iniciativa denominada “CSIRT Américas”, la cual promueve el intercambio de información sobre alertas de ciberseguridad. Consideramos que es esencial que este Grupo promueva el trabajo y rol de los CSIRTs, que son fundamentales para poder confrontar los ataques e incidentes en el ciberespacio, y componentes esenciales para construir y desarrollar resiliencia.

También, nos quisiéramos sumar a lo señalado por varias delegaciones respecto a la necesidad de mencionar específicamente a ransomware como parte de las amenazas que afectan actualmente nuestra realidad en el ciberespacio.

Si bien expresamos no estar de acuerdo con la realización de listados, también nos mostramos flexibles en la inclusión de este concepto. Creemos que es importante señalar este tipo de herramientas maliciosas, porque en esencia, todos podemos ser víctimas de ataques de este tipo, como lo ha sido también nuestro país. Y por ello, es fundamental que podamos generar mecanismos e instancias para intercambiar nuestras experiencias y lecciones aprendidas al respecto. Nuevamente, la importancia de la cooperación.

Incluso, en materia de Amenazas reales y potenciales, ya no se contempla la posibilidad de que los Estados podamos utilizar el marco de este Grupo de Trabajo de Composición Abierta para intercambiar información técnica referente a estas amenazas en el uso de las TICs.

Respecto a la sección sobre medidas de fomento de la confianza, nos parece importante que se hubiese contemplado en el texto de manera más completa los

elementos de la propuesta sobre una Red de Puntos de Contactos realizada por Australia, Brasil, Canadá, Alemania, Israel, Corea, México, Países Bajos y Singapur.

Respecto al derecho internacional, nos hubiese gustado una mención más amplia respecto al derecho internacional humanitario, el cual consideramos un componente esencial del derecho internacional. Coincidimos también con lo expresado respecto a la importancia de haber mantenido la mención hecha al Comité Internacional de la Cruz Roja, el cual ha realizado un destacado, histórico y valioso trabajo en la materia.

Señor Presidente,

Como hemos señalado anteriormente, esta nueva versión del draft contiene muchos elementos valiosos y positivos. Por ello, quisiéramos también agradecer el tratamiento especial que se dio a la preocupación de que actividades maliciosas de las TICs puedan afectar la infraestructura crítica, así como la mención abierta a la forma en que la pandemia del Covid- 19 nos mostró, entre otras cosas, los riesgos y consecuencias del mal uso de las TICs.

Asimismo, nuestro país recibe con beneplácito el reconocimiento al alto nivel de participación de mujeres delegadas en estas sesiones y la relevancia de la perspectiva de género en estas discusiones, y especialmente en el uso de las TICs en el contexto de la seguridad internacional y la creación de capacidades. Como señalamos en nuestro statement anterior, es del todo relevante recordar que estas materias responden a mandatos de Naciones Unidas, y especialmente a la conocida agenda "Mujer, Paz y seguridad", en la cual seguimos trabajando de manera comprometida.

Señor presidente, y delegaciones presentes. Sabemos que este informe debe ser aprobado por consenso, por lo que también creemos que este Grupo de Trabajo puede funcionar como una herramienta efectiva en el ofrecimiento de avances concretos en el ámbito de las tecnologías de la información y comunicaciones, acorde con su reconocimiento como medida de fomento de confianza.

Se nos preguntó esta mañana si creemos que este documento es viable para el consenso, y nuestra respuesta es sí.

Nuestra voluntad y compromiso es poder contribuir a que este informe sea equilibrado, pero que también pueda ofrecer un camino concreto de trabajo hacia el futuro, y que pueda ofrecer a la comunidad internacional avances y entendimientos comunes que permitan enfrentar con éxito las amenazas al ciberespacio.

Tenemos la disposición y convicción de que el trabajo de usted, señor presidente, y el esfuerzo de todas las delegaciones puede llegar a un resultado concreto que dé inicio a nuestras tareas en los próximos años.

Nuestro país aboga por el consenso, la flexibilidad y el reconocimiento de los pilares de este Grupo.

Muchas gracias.

STATEMENT FINAL REPORT
-29-07-2022-

Muchas gracias, señor Presidente.

En primer lugar, mi delegación quisiera agradecer su trabajo, el de su equipo, la Secretaría, y también reconocer el trabajo del resto de las delegaciones. Entendemos, señor presidente, que todos estaremos haciendo concesiones al aprobar este documento, y esa es precisamente la esencia de un consenso. Mostramos nuestra apertura con este documento, ya que nos permite sentar precedentes en el debate sobre las TICs, y me permito reiterar el compromiso de Chile con este proceso.

Chile está en condiciones de apoyar el consenso. Sin embargo, reconocemos que no estamos satisfechos del todo con el resultado de estas discusiones. Aún no logramos comprender la complejidad de incorporar mayor lenguaje relacionado con cooperación y creación de capacidades, algo que es fundamental para nuestra y otras regiones, como tampoco la identificación de algunas amenazas, como el caso ransomware, que ha afectado a muchos de nuestros países.

Sin perjuicio de ello, estamos satisfechos con el hecho de que podamos dar un primer paso en este Grupo de Trabajo, y que de esta forma podamos fijar el primer escalón hacia el futuro. Este no ha sido un proceso sencillo, y sabíamos que enfrentaríamos muchos desafíos, por lo que podemos reconocer que estamos ante un documento balanceado que inicia las discusiones, no las finaliza, como mencionaron también otras delegaciones.

Queremos también destacar la importante contribución realizada por la participación de mujeres en este proceso, y esperamos que esa participación siga aumentando de manera efectiva. Asimismo, destacamos también la participación de las y los representantes de organizaciones regionales, y de los stakeholders que estuvieron presentes.

Apoyamos este documento y hacemos un llamado a mirar hacia el futuro y evaluar la forma de seguir avanzando desde un espíritu de cooperación, con un enfoque constructivo, que nos permita generar avances concretos. Enfrentamos un escenario complejo en cuanto a amenazas en el ciberespacio, y como Grupo tenemos un deber y responsabilidad de poder ofrecer respuestas y soluciones satisfactorias a la comunidad global.

Señor presidente, como usted mencionó ayer, un camello es un caballo hecho por un comité. Este camello será el encargado de acompañarnos en el camino que iniciamos y esperamos que ese camino sea fructífero, y que pueda llegar a un buen final.

Muchas gracias.

Colombia

Señor Presidente:

Colombia desea reiterarle a Usted, a su equipo, y a la Secretaría su agradecimiento por su labor, su dedicación y trabajo. De manera especial destacamos su liderazgo en la conducción de las deliberaciones y sus esfuerzos por lograr consenso.

Agradecemos su propuesta presentada como Documento CRP.1 y estamos listos para adoptarla por consenso. Sabemos que no es fácil lograr un texto balanceado, que si bien no es el documento final, como Informe de Avance es una hoja de ruta para continuar y profundizar nuestras deliberaciones en las siguientes sesiones del Grupo, basados en el acervo de comportamiento responsable acordado y en desarrollo del derecho internacional que debe guíar todas las discusiones multilaterales. Esperamos que al final de este proceso podamos adoptar recomendaciones significativas, orientadas a la acción, que aporten respuestas concretas y permitan fortalecer nuestra acción colectiva frente a los desafíos que enfrentamos.

Señor Presidente:

Mi Delegación valora el ejercicio de discusión que hemos llevado a cabo de manera amplia, participativa, inclusiva y transparente en estas tres sesiones de este Grupo de Trabajo.

Si bien existen divergencias en la discusión de este tema, mi delegación reitera que son muchas las coincidencias y, lo más importante, que compartimos un objetivo

común: la promoción y mantenimiento de un ciberespacio abierto, seguro, estable, accesible y pacífico.

Hemos escuchado con beneplácito las intervenciones de hoy de las distintas delegaciones y su disposición de unirse al consenso. Deseamos agradecer a todas las delegaciones sus esfuerzos y flexibilidad.

Colombia ha participado constructivamente en este proceso y seguirá apoyando el multilateralismo, con voluntad política para lograr avances significativos en temas que, como éste, son fundamentales para el bienestar, la paz y la seguridad internacional.

Reiterándole el apoyo de mi delegación, señor Presidente, agradezco su atención.

Cuba

Señor Presidente:

Agradecemos sus intensos esfuerzos para lograr un primer informe anual progresivo del Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones. Apreciamos también la labor de su equipo y de la Secretaría.

Nuestra delegación participó de manera activa durante el proceso de negociación con vistas a construir consenso sobre el proyecto de informe, en virtud de nuestro compromiso con el Grupo de Trabajo. En ese empeño, presentamos propuestas en capacidad nacional y junto a países de ideas afines.

Notamos que varias de esas propuestas fueron tenidas en cuenta en el informe anual progresivo aprobado y nos hemos sumado al consenso.

Sin embargo, quisiéramos dejar registradas nuestras graves preocupaciones en relación con las referencias al informe del GGE de 2021 y su reafirmación excesiva en el texto, incluyendo la importación de lenguajes como los relativos al Derecho Internacional Humanitario, que no favorecemos. Recordamos que los GGE son de composición limitada, a diferencia del formato inclusivo que proporciona el GTCA.

Reiteramos que, en opinión de la delegación de Cuba, no debería incluirse referencia alguna al Derecho Internacional Humanitario en el informe, en tanto no consideramos pertinente su aplicabilidad en el ámbito de las Tecnologías de la Información y las Comunicaciones en el contexto de la seguridad internacional.

Nos oponemos resuelta y firmemente a la militarización del ciberespacio y a la posibilidad de su uso como escenario de conflicto armado. El ciberespacio debe preservarse para fines exclusivamente pacíficos.

El marco normativo para el comportamiento responsable de los Estados, al que se alude reiteradamente en este informe anual, resulta insuficiente y no se erige como tal. Esperamos que, en próximas sesiones, el GTCA discuta y pueda avanzar, en virtud del mandato establecido en la resolución 75/240, en la elaboración de nuevas normas, reglas y principios, incluidas posibles obligaciones jurídicamente vinculantes, en adición al conjunto de normas voluntarias existentes.

Enfatizamos en la importancia de desarrollar una terminología común en el ámbito de la seguridad y el uso de las TIC.

Debe respetarse y preservarse el papel del GTCA para entablar el diálogo institucional periódico en el ámbito de la seguridad y el uso de las TIC, en correspondencia con la resolución 75/240 de la Asamblea General. No favorecemos mecanismos paralelos, duplicativos o sustitutivos del GTCA, sino resultantes de este.

Muchas gracias.

El Salvador

Señor Presidente

La Misión Permanente de El Salvador ante las Naciones Unidas desea expresar su apoyo al reporte anual de progreso del Grupo de Trabajo de Composición Abierta, que menciona los avances respecto a los objetivos establecidos de seguir elaborando con carácter prioritario las reglas, normas y principios de comportamiento responsable de los Estados, así como las modalidades de aplicación correspondientes y, de ser necesario, introducir cambios o elaborar reglas de comportamiento adicionales; examinar las iniciativas de los Estados encaminadas a garantizar la seguridad en la utilización de las tecnologías de la información y las comunicaciones; entablar, bajo los auspicios de las Naciones Unidas, un diálogo institucional periódico con amplia participación de los Estados; seguir estudiando, con miras a promover el entendimiento común, las amenazas actuales y potenciales en la esfera de la seguridad de la información, incluida la seguridad de los datos, y las posibles medidas de cooperación para prevenir y contrarrestar esas amenazas, y la forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones por los Estados, así como las medidas de fomento de la confianza y la creación de capacidad.

Para la delegación de El Salvador el reporte en referencia no pretende ser un resumen exhaustivo de las acciones realizadas en los primeros períodos de sesiones, sino más bien mencionar los avances concretos alcanzados a la fecha y los próximos pasos para avanzar en nuestros trabajos.

En cuanto al estudio de las amenazas, se identificaron las siguientes: el desarrollo de capacidades de TIC para fines militares, las actividades perjudiciales dirigidas contra infraestructuras críticas e infraestructuras críticas de información y la evolución de nuevas tecnologías emergentes que amplían los ámbitos de ataque. Al respecto, es relevante mencionar que, aunque el reporte de progreso no hace mención específica al secuestro de datos (ransomware) que fue mencionado por la delegación de El Salvador y otras delegaciones, se toma nota que el GTCA de conformidad con su mandato, se compromete a seguir estudiando las amenazas para establecer las posibles medidas de cooperación para hacerles frente.

En cuanto a las normas, reglas y principios de comportamiento responsable de los Estados, se hicieron propuestas concretas y orientadas a la acción, para fomentar la aplicación de estas y se compromete a seguir trabajando para desarrollar entendimientos comunes que faciliten su aplicabilidad, invitando a los Estados a que presenten sus propuestas para lograrlo.

Respecto al Derecho Internacional, el análisis se centró en la realización de debates sustantivos sobre este tema que permitan alcanzan consenso entre los Estados. También se indicó la posibilidad de fortalecer los esfuerzos de creación de capacidades lo que podría incluir realizar talleres, cursos de formación, así como intercambios sobre las mejores prácticas en esta temática. Se aplaude la iniciativa de seguir alentando a los Estados a seguir aportando sus propuestas e intercambiando opiniones a través de los mecanismos existentes para ello.

En cuanto a las medidas de fomento a la confianza, se reconoce como muy positivo que el Grupo resaltó la iniciativa de acordar la creación de un directorio de puntos de contacto mundial e intergubernamental sobre la seguridad en el uso de las TIC en las Naciones Unidas para mejorar la interacción y la cooperación entre los Estados, y a los que se podría recurrir en casos de emergencia. Esto fue mencionado por la delegación de El Salvador porque creemos en el potencial de dicha iniciativa, desde

una perspectiva de fomento de la confianza, reducción de tensiones en el ciberespacio y respuesta pronta en casos de crisis.

Respecto a la creación de capacidades se planteó promover una mejor comprensión de las necesidades de los Estados en vías de desarrollo con el objetivo de reducir la brecha digital a través de esfuerzos de creación de capacidad adaptados y con perspectiva de género, comprometiéndose a trabajar por la financiación, el intercambio de opiniones e ideas, aplicar las mejores prácticas y tomar en cuenta lecciones aprendidas.

Por último, en cuanto al diálogo institucional periódico se indica trabajar en la práctica de sensibilización y seguir elaborando el Programa de Acción con vistas a su posible establecimiento como mecanismo para promover estas prácticas voluntarias y responsables de los estados.

Esta delegación reitera su apoyo a la Presidencia, se congratula de la adopción del reporte por consenso y reitera su firma compromiso de seguir trabajando e intercambiando activamente para enriquecer las discusiones de este Grupo de Trabajo.

Muchas gracias.

Chair

The Permanent Mission of El Salvador to the United Nations wishes to express its support for the annual progress report of the Open-Ended Working Group, which mentions progress towards the established goals of further elaborate as a matter of priority the rules, norms and principles of responsible behaviour of States on cyberspace, as well as the modalities of implementation and, if necessary, to introduce changes or develop additional rules of behaviour; to review States efforts to ensure security in the use of information and communication technologies; to engage under the auspices of the United Nations, in a regular institutional dialogue with the broad participation of States; to continue to study, with a view to promoting a common understanding, current and potential threats in the field of information security, including data security, and possible cooperative measures to prevent and counter such threats, and how international law applies to the use of information and communication technologies by States, as well as confidence-building and capacity-building measures.

For the delegation of El Salvador, the progress report is not intended to be an exhaustive summary of the actions carried out in the first sessions of the OEWG, but rather to mention the concrete progress achieved to date and the next steps to advance in our work.

Regarding the study of threats, the following were identified: the development of ICT capabilities for military purposes, harmful activities directed against critical infrastructures, critical information infrastructures and the evolution of new emerging technologies that expand the areas of attack. In this regard, it is relevant to mention that although the progress report does not make specific mention to ransomware, that was mentioned by the delegation of El Salvador and other delegations, it is noted that the OEWG in accordance with its mandate, undertakes to continue studying the threats to establish possible cooperation measures to address them.

With regard to norms, rules and principles of responsible behaviour of States, concrete and action-oriented proposals were made to promote their application and it undertakes to continue the work to develop common understandings that facilitate their applicability, encouraging States to submit their proposals to achieve the later.

Regarding international law, the analysis focused on substantive debates on this topic that would allow consensus to be reached among States. The possibility of strengthening capacity-building efforts was also mentioned, which could include workshops, training courses, as well as exchanges on best practices in this area.

With regards to confidence-building measures, it is recognized as very positive that the Group highlighted the initiative on the establishment of a directory of global and intergovernmental Point of Contacts (POCs) on security and ICTs within the United Nations to enhance interaction and cooperation among States, and that could be used in cases of emergency. This was mentioned by the delegation of El Salvador because we believe in the potential of such an initiative, from a perspective of confidence-building, reducing tensions in cyberspace and prompt response in the event of a crisis.

On capacity-building, it was proposed to promote a better understanding of the needs of developing States with the aim of reducing the digital gap, through adapted capacity-building efforts with a gender perspective, committing to work for financing, the exchange of opinions and ideas, apply best practices and consider lessons learned.

Finally, about regular institutional dialogue, it is indicated to work on the practice of raising awareness and to further elaborate the Programme of Action with a view to its possible establishment as a mechanism to promote these voluntary and responsible practices of States.

This delegation reiterates its support for the Chair, welcomes the adoption of the report by consensus and reiterates its firm commitment to continue working and actively exchanging to enrich the discussions of this Working Group.

I thank you.

India

Mr. Chair,

During our interventions in the first, second and current substantive sessions, we have been highlighting the need for focused and effective capacity building measures. We strongly believe that OEWG is the right platform to discuss capacity building and various proposals and recommendations as suggested by multiple small and developing countries in the previous sessions.

2. We would like to reiterate that an integrated approach towards capacity building is necessary. The ICT environment is evolving continuously with a range of new challenges from new and emerging technologies and use of the same by state and non-state actors. While bridging digital divide focuses more on bringing millions of people closer to access to ICTs and making them part in realising the opportunities presented by ICTs. Capacity building efforts needed for them are completely different compared to capacity building efforts needed for the implementation of the normative framework.

3. Implementation of the normative framework demands a ‘common minimum cyber preparedness’ for all Member States, especially small and developing countries. Such ‘cyber preparedness’ helps Member States in furthering their capabilities towards a bigger goal of normative framework implementation.

4. A permanent mechanism anchored at the UN is in the interests of Member States in the long-run with more and more challenges emerging in cyberspace and increasing need towards guiding Member States in capacity building under the UN framework. We hope that these proposals and recommendations as expressed by multiple countries in the current session would be discussed further in the future sessions of the Working Group.

Iran (Islamic Republic of)

Mr. Chair,

Distinguished delegates,

At the outset, I would like to take the opportunity to express our delegation's sincere gratitude to you, 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 share the hope of many other member states that this OEWG will guide the international community toward a just, secure, and sustainable cyberspace.

Based on this understanding, we have participated in the OEWG deliberations in a very constructive manner. Iran has offered its written submissions, outlining the rationale for each suggestion. During this process, Iran also has specified its genuine concerns, and itemized its priorities, the crossing of which would not be admissible for us.

While we must now conclude the OEWG's first cycle before starting its second, the extent of our success or failure might be determined by a thorough analysis of the road that has come before us, particularly taking into account the first annual progress report. This is crucial because it will serve as our first roadblock for the remainder of the OEWG's existence.

As we stated in the informal consultations and at the beginning of the current substantive session, the zero draft was yet to be balanced by incorporating the principled position of the entire membership. Now almost at the end of the session, we believe the required balance is still missing. Even the revisions, despite slow progress, were unable to include the necessary elements, representing the concerns and interests of all and not just the vocal minority against a sizable silent majority.

In accordance with Resolution 75/240, which established the OEWG, the working method of the group is consensus, and this never entails disregarding views of even a single member state. To put it another way, this process should be sufficiently representative in form, content and negotiation methodology. Listening only to some outspoken member states is not justifiable at all.

Now, the first year of this OEWG and also the experience of the previous OEWG are enough to demonstrate that our way of discussion so far does not align with the necessary working method of the OEWG. As a result, we should revise the practice and revitalize the work of the OEWG.

In this sense, we believe that all the procedural proposals that we made, in the organizational meeting of this OEWG, including thematic discussions, establishing subgroups, text-based negotiation, on different aspects of developing the annual and final report of the OEWG are not only more pertinent, but also demand serious consideration throughout the remainder of the OEWG's existence.

Once again we reiterate the necessity of beginning negotiations based on a rolling text, consistently exploring different avenues of informal diplomacy between the interested delegations, and launching fruitful dialogue to cover the gaps and discuss the differences, all under the direction of the esteemed Chair.

We wish that the report of the OEWG should satisfy all member states to feel the ownership and garner an unquestionable consensus. This can result in a rise in acceptance of and faith in about the method and the content of the process. Not in a way that ultimately each delegation would be put on undesirable situation to take it or leave it.

Last but not least, in light of the latest version of the first annual report, we are obliged to state that our observations and reservations as declared about the final report of the previous OEWG in March 2021 remain valid and apply to this annual report too. We will continue to advocate and follow them in future sessions of the OEWG.

Our distinguished Chair is adamantly believing that the OEWG itself is a confidence-building measure, and we agree with that, but 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.

I thank you, Mr. Chair!

Ireland

Mr Chair,

Ireland aligns itself with the closing statement made by the EU at the Third Substantive Session of the Open-ended Working Group (OEWG) on 29 July 2022.

Ireland wishes to thank you and your team for your tireless efforts throughout the past year, guiding us along in this process and for working in such an inclusive and transparent manner. We particularly wish to thank you for your work during the most recent session of the OEWG, when Ireland was pleased to join fellow Member States in consensus and agree on the First Annual Progress report.

We welcome the many diverse contributions made at the session, particularly from stakeholders, which have provided the OEWG with different and valuable perspectives and have helped to better inform our discussions and output.

The adoption of the report by consensus represents a firm commitment by the international community to continue our collective efforts to enhance peace and security in cyberspace, specifically within the context of the current global upsurge in malicious cyber activity, which has targeted our citizens, public institutions and critical infrastructure.

As you have aptly said previously Mr Chair, the report is but a snapshot of our work over the past year and is not exhaustive nor a final report. Therefore, it will not completely meet the needs of every delegation. Instead, it is a balanced document of compromise between Member States, who have all shown an incredible amount of flexibility in the name of consensus.

A few observations on the contents of the annual report;

On International Law, Ireland welcomes the inclusion of language on international humanitarian law and notes the importance of continuing to develop a common understanding amongst all Member States in this regard. We consider this reference important as it is in line with the UN consensus that existing international law applies to States' actions in cyberspace.

Ireland also welcomes references made to the Programme of Action on Cyber (PoA), which many other delegations highlighted throughout the last session. It is our hope that an open and transparent PoA will act as a permanent and inclusive mechanism with strong State and multi-stakeholder participation, driven by consensus.

Mr Chair, Ireland thanks you, your team and the UN Secretariat once more for allowing us to come to an agreeable compromise. We look forward to continuing our work at the OEWG in future sessions, and using the first annual progress report as a roadmap in these discussions.

Israel

Mr. Chairperson,

The Israeli delegation wishes to express our 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 final annual progress report.

Reading the final version of the report, shows that some of the positions, as well as reservations expressed by Israel during the negotiating process, remain unanswered, and unfortunately not all our concerns were fully addressed. However, in the spirit of consensus, wishing to express our positive attitude, and in light of the constructive cooperation presented through the last few days by so many delegations, we understand the need for a certain degree of flexibility. Israel stands ready to join other delegations and support this report. We can assure you that the Israeli delegation remains committed to work with other states and to continue to present a constructive approach and advance the dialogue in the OEWG.

That being said, it is very important for us at this point to raise and clarify our positions regarding few key points in the report:

Regarding section B paragraph 12 – we acknowledge that this paragraph is based on agreed language taken from paragraph 17 of the OEWG 2021 consensual final report. 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”. Norms and CBMs are voluntary measures and we believe that the text should have reflected that difference in legal standing. We therefore suggest that in future references the word “obligations” would be omitted.

In addition, in this section dealing with existing and potential threats we were disappointed to see that there was no reference to the threat of ransomware. Ransomware is an example of cybercrime which increasingly crosses the threshold of impacting international peace and security and Israel believes that specific attention should be given to it. This issue was flagged by multiple delegations, including our own, as an issue which should have been clearly reflected in our report.

Regarding section C paragraph 14 (b) - We wish to clarify and reiterate that while some states held the view that further development of norms and the implementation of existing norms could take place in parallel, Israel’s view is that it would be more constructive to reach high level of implementation of existing norms before moving to developing new 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 developing new norms, it would be more appropriate to focus on those norms that currently exist, to assess whether and how they are being properly 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 is 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.

With regards to section D paragraph 15 (b) – On the matter of International Law, Israel welcomes the statements, made by governments across the world, presenting

their views on the application of international law to the field of ICTs. This contributes to our mutual understanding as a community, and creates a positive starting point for discussions. We think that the current approach, of encouraging States to submit their views on a voluntary basis, is the most appropriate course of action for the OEWG to take. Going forward, we would welcome intersessional discussions in which academics and experts could be heard – to provide different perspectives on some of the issues. This will assist states in formulating their positions going forward. Given that many states have already presented their views on topics such as non-intervention, proportionality, distinction, and human rights, and there is already much academic writing on these issues, we suggest that the use of the OEWG's time could be best used after to first identify specific topics that could benefit from additional input of outside experts, and afterwards engage in discussion of these issues. The set of experts who will be invited to address our intersessional meeting can be decided once we have determined on the issues, and the relevant expertise required.

Furthermore, per paragraph 15 (b) (i) - We would like to emphasize that the language used in this paragraph does not reflect an international agreement regarding the need for additional legally binding obligations in the sphere of ICTs. As we and many other states have stated, there is no consensus over the need to develop additional legally binding obligations at this time and this should be clearly stated in this report. To the extent that this paragraph is read as an international consensus to develop at this stage a legally binding instrument, Israel wishes to disassociate itself from this position.

Furthermore, per paragraph 15 (b) (i) - We would like to emphasize that the language used in this paragraph does not reflect an international agreement regarding the need for additional legally binding obligations in the sphere of ICTs. As we and many other states have stated, there is no consensus over the need to develop additional legally binding obligations at this time and this should be clearly stated in this report. To the extent that this paragraph is read as an international consensus to develop at this stage a legally binding instrument, Israel wishes to disassociate itself from this position. This passing year has demonstrated the heightened responsibility of governments to provide security and protect state interests. This requires strict application of agreed 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.

In conclusion, Israel joined the consensus and hopes that the adopted progress report can serve as a roadmap for the continuation of our discussions and we 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.

Kazakhstan

Kazakhstan fully supports the work of the Open-Ended Working Group aimed at finding consensus on the key international agenda in the field of ICT. We believe that the adoption at the end of the current session of the interim report will fully contribute to the achievement of the final goals of the OEWG aimed at ensuring the security of ICT in accordance with UN General Assembly Resolution 76/19.

A. Introduction

Kazakhstan has international treaties and carries out practical interaction within the framework of the Shanghai Cooperation Organization, the Collective Security Treaty

Organization and the Commonwealth of Independent States, and also actively participates in the discussion of issues related to ICT security within the OSCE, the Conference on Interaction and Confidence Building Measures in Asia (CICA).

In particular, within the framework of the informal working group in the field of OSCE cybersecurity, Kazakhstan, together with Canada, supervises 4 confidence-building measures, within which it is envisaged that the participating States will, on a voluntary basis, share information on the measures they have taken to ensure openness, interoperability, security and the reliability of the Internet.

Within the framework of the Conference on Interaction and Confidence-Building Buildings in Asia (CICA) in 2021, a new confidence-building measure «Security and use of ICT» was approved, which is currently chaired by Kazakhstan. In October 2022, at the next summit of the Conference on Interaction and Confidence Building Measures in Asia, it is planned to adopt a statement by the heads of state.

Along with this, in order to build the capacity and improve the skills of domestic specialists in the field of countering the use of ICT for criminal and other illegal purposes, Kazakhstan actively cooperates with the bodies of the UN system - the Office of Counter-Terrorism, the Office on Drugs and Crime and others.

In view of the foregoing, we note the importance and timeliness of point A in the context of international and regional cooperation.

B. Existing and Potential Threats

Kazakhstan is taking comprehensive measures to counter cybersecurity threats at the national and international levels. The state policy in this area is implemented within the framework of the “Kazakhstan Cyber Shield” Concept, which provides for the qualification of threats and specific measures to level them.

Realizing that the influence of ICT is increasing in all spheres of activity of the state, organizations, civil society, work to strengthen cybersecurity will continue.

b) (i) Cooperation and assistance to establish and strengthen Computer Emergency Response Teams (CERTs);

Incidents, as a rule, are of a cross-border nature and equally threaten the security of the infrastructure of each of the countries, we believe it is important to support the point on cooperation and strengthening of computer incident response teams, this, in our opinion, will allow establishing direct contacts between national Computer Incident Response Services.

For its part, the National Computer Incident Response Service of Kazakhstan (KZ-CERT) has already concluded 26 memorandums with international organizations.

b) (vi) Undertaking international exercises and technical training including law enforcement officials.

As an enhancement of practical experience, we annually conduct cyber exercises, as well as practical conferences.

This year, on September 14–16, Almaty, Kazakhstan, the international practical conference KazHackStan 2022 will be held, which will be devoted to topical issues of cybersecurity.

A cyber polygon will be organized to imitate a critically important object of informatization.

Moreover, within the framework of this conference, the International Telecommunication Union of the United Nations will organize Interregional cybersecurity exercises for the CIS region and the Arab States.

We believe that such events will increase practical experience in responding to computer incidents, as well as strengthen international cooperation, which generally corresponds to paragraph 6 (VI) of international exercises and technical training.

b) (x) Measures to safeguard the general availability and integrity of the Internet.

We also want to support point 10 (X), as Kazakhstan pays great attention to creating a safe Internet from malware, phishing, etc.

In particular, in order to protect the Kazakhstan segment of the Internet, together with a private company, all websites with .KZ domain names were given a free opportunity to be protected by the WebTotem system.

It should be noted that more than 8,000 foreign clients use this system.

In addition, together with a Kazakh company, the BugBounty vulnerability detection program was launched, where researchers receive appropriate rewards for discovering vulnerabilities in systems/websites.

More than 1,100 independent cybersecurity experts from around the world have already registered on the BugBounty platform from which more than 1,200 reports of vulnerabilities have been received, some of which are critical.

d) States could consider strengthening interactions with interested stakeholders, including businesses, non-governmental organizations and academia, through the exchange of knowledge and best practices on the protection of CI and CII.

One of the most important issues of global digitalization is information security.

To address these issues, the Cyber Shield of Kazakhstan Concept is being implemented, within the framework of which a set of measures was taken on cyber security issues, which positively reflected in the UN Global Cyber Security Rating, where Kazakhstan is ranked 31st.

In particular, in order to develop a culture of cybersecurity, measures are taken on an ongoing basis to raise public awareness of cybersecurity threats. According to the results of a sociological survey, the level of public awareness is 75%.

For 5 years, the number of educational grants in the specialty of information security has been increased by 43 times.

In addition, the Information Security Management System is being actively developed, headed by the National Coordinating Center for Information Security of the country.

33 private SOC have been created to protect government agencies and critical informatization facilities.

There is an industry operational information security center in the financial sector, which coordinates the cybersecurity centers of second-tier banks.

Thus, we face the common task of ensuring cybersecurity. Not a single state is able to independently counteract modern threats.

In this regard, Kazakhstan is ready to participate in the process of exchanging experience in building an international cybersecurity system.

C. Rules, Norms and Principles of Responsible State Behaviour

c) Information exchange on best practices and cooperation could be enhanced, potentially drawing from models of information sharing in other fields, and could include topics such as innovation, vulnerability disclosure, the protection of critical infrastructure and cooperation between CERTs.

Since 2009, the country has been operating the Computer Incident Response Service, which is a single center for users of national information systems and the Internet segment, which provides the collection and analysis of information on computer incidents, advisory and technical support to users in preventing computer security threats.

Advisory and technical support to users, including foreign ones, is provided through the 1400 call center, email, telegram channel, and also through social networks. There is also a 24-hour emergency service.

As part of the international exchange of information for the current year, more than 360 notifications were sent to 40 states, and 361 notifications were received from 31 states.

Today, ICT plays an important role in all spheres of life. In this regard, we consider the proposal to expand the exchange of information between CERTs as a very important initiative.

E. Confidence-Building Measures

Thank you for opportunity to speak. I would also like to thank you for your efforts in preparing the document we are currently working on. We would like briefly touch on chapter E “Confidence-Building Measures”.

Kazakhstan generally supports the initiative to create a global register of contact persons on ICT issues under the auspices of the UN at the level of foreign policy, authorized, technical departments for operational interaction, indicated in paragraph A of chapter E “Confidence building measures”.

Also, Kazakhstan considers it important to exchange information on the adopted strategies and documents in the field of cybersecurity, for its part, we are ready to provide the adopted legislative acts and concepts in the field of cybersecurity, indicated in paragraph B of chapter E “Confidence building measures”.

In turn, Kazakhstan intends to send information to the UN Secretary General about the efforts being made at the national level to strengthen information security and promote international cooperation in this area.

We also generally support the proposed initiatives in chapters D “International law” and F “Capacity Building”.

Mexico

Thank you very much dear Chair,

La delegación de México se suma al reconocimiento a su trabajo, al equipo de apoyo y al Secretariado tras la adopción de este Informe Anual de Progreso. Mucho se ha ganado para el propio proceso multilateral que representa el *Open Ended Working Group* con la adopción del Informe Anual de Progreso.

Además de cumplir con nuestro mandato estamos entregando a la comunidad internacional su voto de confianza de vuelta en decisiones conjuntas y la posibilidad de lograr confianza suficiente aun en contextos complejos y en un momento internacional en el que las amenazas ataques e incidentes cibernéticos afectan a todos los países en todos los niveles.

Señor Presidente:

México puede afirmar que el Informe Anual de Progreso, cumple con la expectativa de conservar y reiterar los acuerdos previos y avanza en el camino correcto del

llamado a la implementación efectiva del marco (framework) que hemos adoptado en la Asamblea General de las Naciones Unidas y de informar nuestros esfuerzos para compartir la experiencia con todos, de avances y de obstáculos también.

México desea dejar registrado, sin embargo, que varias propuestas sustantivas no quedaron registradas en el texto adoptado aun cuando se mencionaron y se discutieron en sesiones previas. En especial, deseo señalar en nombre de Mexico, que seguiremos promoviendo y fortaleciendo el dialogo con las delegaciones sobre aspectos en los que insistiremos a lo largo de este proceso y que me permito señalar:

- La necesidad de fortalecer el recurso al uso de todas las herramientas de prevención de conflictos y la resolución pacífica de controversias como corresponde a un tema de la Primera Comisión y de una ciberdiplomacia ya existente.
- La necesidad de reconocer el equilibrio entre los usos pacíficos y para el desarrollo de las tecnologías de la información, y la protección y ejercicio de los derechos humanos en línea.
- La instrumentación efectiva de medidas de fomento de la confianza, incluso las acordadas en informes previos.
- La oportunidad de beneficiarnos de una mayor colaboración con otros órganos de las Naciones Unidas, incluso como con la Comisión de Derecho Internacional, de otras agencias internacionales como el Comité Internacional de la Cruz Roja, y otros esfuerzos regionales y subregionales, así como también la mayor apertura posible al dialogo y recepción de insumos de la academia, las organizaciones de la sociedad civil y el sector privado.

Señor Presidente:

Mi delegación no parte en la adopción de este informe de la existencia de un equilibrio frágil. Aun el más pequeño paso multilateral puede ser tan sólido como nuestra propia organización. Mexico espera que la velocidad de los asuntos en el ciberespacio pueda acelerar también nuestros acuerdos y respuestas para sesiones futuras.

Finalmente, en nombre de la delegación de México, deseo subrayar lo valioso de la sesión de este miércoles pasado, en la que diversos actores de sociedad civil presentaron sus aportaciones a este grupo de trabajo. Su participación en este marco formal de trabajos es una muestra clara para la delegación de Mexico de la importancia y enriquecimiento que puede ofrecer el dialogo amplio con todos los actores, particularmente en estos temas.

Muchas gracias señor presidente.

Thank you very much dear Chair,

The Mexican delegation joins in the recognition of your work, your team's and the Secretariat's after the adoption of this Annual Progress Report. Much has been achieved for the multilateral process, which the Open-Ended Working Group itself represents with the adoption of the Annual Progress Report.

In addition to fulfilling our mandate, we are giving the international community a vote of confidence on joint decisions and the possibility of achieving sufficient trust even in complex contexts and in an international moment in which threats, attacks and cyber incidents affect all countries at all levels.

Mr. Chair,

Mexico believes that the Annual Progress Report fulfils the expectation of preserving and reiterating previous agreements. It moves forward on the right path of the call for the effective implementation of the framework that we have adopted in the UN General Assembly and to inform about our efforts to share the experience with everyone, of the progress and obstacles as well.

Mexico wishes to emphasize, however, that several substantive proposals were not included in the adopted text even though they were mentioned and discussed in previous sessions. In particular, I wish to point out on behalf of Mexico that we will continue to promote and strengthen the dialogue with delegations on aspects on which we will insist throughout this process and which I would like to point out:

- The need to strengthen recourse to the use of all tools for conflict prevention and the peaceful resolution of disputes as it corresponds to a First Committee topic and an already existing cyber-diplomacy.
- The need to recognize the balance between the peaceful and for development uses of information technologies and the protection and exercise of human rights online.
- The effective implementation of confidence-building measures, including those agreed in previous reports.
- The opportunity to benefit from greater collaboration with other United Nations entities, including the International Law Commission, other international agencies such as the International Committee of the Red Cross, and other regional and sub-regional efforts, as well as the greatest possible openness to hold dialogue and receive input from academia, civil society organizations and the private sector.

Mr. Chair,

By adopting this report, my delegation does not assume the existence of a fragile balance. Even the smallest multilateral step can be as solid as our own organization. Mexico hopes that the speed of issues in the cyberspace can also accelerate our agreements and responses for future sessions.

Finally, on behalf of the Mexican delegation, I wish to underscore the value of this past Wednesday's session, in which various civil society actors presented their contributions to this working group. Their participation in this formal segment of work is a clear demonstration for the Mexican delegation of the importance and enrichment that a broad dialogue with all actors can offer, in particular on these issues.

Thank you very much Mr. Chair.

Netherlands

Dear Chair,

I would like to firstly thank you for Rev 2 of the draft annual progress report. We can see the hard work and careful thought put into it by you, your team and the Secretariat.

The Netherlands thinks that this new version is a step towards a consensus progress report. We still have some outstanding concerns, but we are ready to engage constructively on these issues with you and other delegations with a view to achieving consensus by the end of the week.

It won't come as a surprise that we have lots to say about the report, but in the spirit of consensus I will limit myself to a few key points.

We welcome:

1. That the document is clear in reaffirming the consensus reached in previous groups as the basis for our future work.

2. While we regret that some of our proposals on IL that we presented yesterday were not incorporated in the report, we can see a delicate balance has been struck by using consensus language from previous reports. REV 2 captures the essence of our proposal, and we thank the many delegations who gave input and / or supported our proposal.

We also have a few points of concern:

1. We welcome the reaffirmations of the UN Framework for Responsible State behaviour at the beginning of the substantive paragraphs. However, we do – like Brazil, the United States and Austria - not support the use of the word "initial" at the beginning of each paragraph. This is for the same reasons as other delegations have indicated. We support the US proposal to solve this.

2. On the threat section, we support the points made by several delegations on the importance of recognizing the malicious use of ICTs by State and non-State actors in the context of armed conflict, which has sadly become a reality.

3. In paragraph 10, we appreciate the notion on the specific concern of malicious ICT activity affecting critical information infrastructure. However, we would like to add a reference to critical infrastructure in the second sentence as well.

4. Also in par 10, we believe that only a part of the critical information infrastructure is addressed, while an important part that was previously noted under threats in paragraph 18 of the 2021 OEWG report is now omitted, including a reference to threats against critical infrastructure that undermine political and electoral processes. The Netherlands therefore, would like to also see the consensus language on this issue from para 18 of the 2021 OEWG report.

5. In par 13, like Mauritius we do not support the reference to the phrase information security, which is not consistent with previous reports, where "security in the use of ICTs" is the consensus term. We therefore propose the following change:

> *States also recalled the OEWG's mandate* ***to continue to study, with a view to promoting common understandings****, existing and potential threats in the* ***ICT-environment*** ~~***in the sphere of information security***~~*, inter alia, data security, and possible cooperative measures to prevent and counter such threats.*[12]

6. Lastly, I have an editorial comment. In the international law section para 15a, we would like to insert a semi-colon between State-responsibility and due diligence. So the semi-colon is to replace the word "and".

We stand ready to constructively discuss these proposals, Chair and we hope that we can all together find a way forward for a consensual progress report.

Thank you very much, Chair.

Pakistan

On Revised Draft-1 (Rev-I) of the Report

Agenda Item 1 & 2: Existing and Potential Threats in the Sphere of International Information Security & The Development of Norms, Rules and Principles of Responsible States Behavior

Mr. Chair,

Thank you for giving me the floor and the opportunity to present Pakistan's views on the revised draft-1 or (rev-1) of the first annual progress report of the OEWG.

Taking this opportunity I would like to express my appreciation for your untiring efforts to steer the work of OEWG in a steady and balanced manner.

Mr. Chair,

Pakistan attaches great importance to this OEWG which is a platform represented by all Member States and has the potential to make cyberspace secure, stable, and accessible for every country in the world.

This OEWG provides us an opportunity to get agree on means and methods conducive to the promotion of responsible behavior of States in cyberspace and to jointly counter the varying nature of threats emanating from cyberspace and impacting international security.

Mr. Chair,

Like any other country, Pakistan is confronting a multitude of threats posed by ungoverned cyberspace. Rising cyber-attacks against the critical infrastructure, Distributed Denial of Service (DDoS), data theft, and targeted disinformation campaigns are some facets of cybersecurity challenges faced by my country. Therefore, Pakistan consistently calls for a legally-binding instrument to promote responsible States' behavior in cyberspace.

To effectively counter cyberattacks on both public and private infrastructure and for the establishment of a stable cybersecurity ecosystem, Pakistan promulgated its first National Cybersecurity Policy in 2021. The policy envisages securing the entire cyberspace of Pakistan including all national digital assets and activity carried out in public and private sectors, and the information and communication systems used by the citizens of Pakistan.

The policy also envisions creating a culture of cybersecurity awareness through mass communication and education programs. It also focuses on the capacity building and skill development of cybersecurity professionals.

On the militarization of cyberspace, Pakistan's position is consistent. We consider the internet as a "Common heritage of mankind" and believe that the use of cyberspace for military purposes is gradually converting into an arena of military confrontation. Therefore, Pakistan calls for an outright ban on the development of offensive cyber weapons.

Coming to the draft annual progress report, Pakistan considers it as balanced and provides a base for further discussions among Member States. However, Pakistan has certain proposals to for amendments to make the report more holistic and agreeable for all Member States.

We believe that cyber threat landscape has changed a lot and posing varying nature to challenges and threats to international security. Global cyberspace has become more fragile thus enabling States and Non-State actors to target other States via cyber

means. Therefore, Pakistan proposes to add technical and cooperative measures to counter disinformation and fake news and non-disclosure of hardware / software vulnerabilities at number 9 & 10 of para 7 (b) of annual progress report.

On the Development of rules, norms, and principles of responsible behavior of States, Pakistan considers this portion of the report as balanced. However, on the further development of rules, norms, and principles of responsible behavior, Pakistan's position is quite clear. Though we do consider the formulation of non-binding voluntary norms is important for secure and stable cyberspace, however, non-binding norms can't be an alternative to a legally binding instrument. The main difference between non-binding norms and a legally-binding instrument is that the latter imposes certain obligations and their violation triggers the law of State responsibility. Moreover, norms are effective during peacetimes only and will lose efficacy in an event of conflict.

Pakistan welcomed the GGE report of 2015 when members expressed their agreement on 11 norms of responsible State behavior. Pakistan believes that there is a need of equipping the Member States with the required skills and technologies and clearly define the modalities for the implementation of the agreed norms. We also propose to mention those 11 norms in footnotes of the draft report.

I would like to conclude by affirming that Pakistan stands ready for enhancing inter-State cooperation to effectively counter the threats posed by ungoverned global cyberspace.

I thank you, Chair.

Agenda Item 3 & 4: Application of International Law in Cyberspace & Confidence Building Measures (CBMs)

Mr. Chair,

Pakistan welcomes the part of the report on the Application of International Law in cyberspace and believes that the foremost task of the OEWG is to get agree on defining how the existing international law can be applied in cyberspace and the formulation of a legally-binding instrument. The non-exhaustive lists of topics in para 9 (a) is comprehensive and encapsulates all those areas of international law including IHL which demand further politically neutral discussions among States for the development of common understanding. We also propose to add the topic of cyber attribution as identified by Indonesia.

Pakistan believes that as a result of such discussions, States will be able to formulate a legally-binding instrument to regulate the global cyberspace. An instrument, which will promote responsible State behavior by holding actors responsible for their acts, and forbade the use of cyberspace for destructive purposes. Pakistan is of the view that along with discussing theoretical aspects States must be encourages to discuss technical means necessary to ensure the application of international law in cyberspace.

We also greatly appreciate that the draft report acknowledges the fact that considering the unique attributes of cyberspace and the transnational nature of cyber technologies, international law has certain gaps which must be addressed.

Mr. Chair,

To make the report more balanced, Pakistan proposes that the following two recommended steps may be added at number 5 which could be read as "States, on voluntary basis, are invited to engage in discussions on getting definitional clarity on the terms such "cyber-attack", "Critical Infrastructure (CI)" "Critical information infrastructure (CII)" and unlawful ICT activities" and at number 6 the recommended

step could be read as “States shall continue to exchange views and engage in discussions on the formulation of a legally-binding instrument for responsible States behavior in cyberspace.”

On Confidence Building Measures (CBMs), Pakistan considers cyber CBMs are extremely important for fostering trust, cooperation, transparency, and predictability among the Member States and to avert misunderstanding and escalation of the conflict. We welcome the operationalization of the global directory of PoCs to deal with any crisis situation.

Pakistan has always supported the idea of CBMs and further proposes the following recommended action which calls for increasing cooperation among the respective Computer Emergency Response Teams (CERTs) of the Member States to address investigation / trace-back requests of Internet Protocols and to resolve the technical impediments in the way of cyber attribution.

I thank you, Chair.

Agenda Item 5 & 6: Capacity-Building & Regular Institutional Dialogue

Mr. Chair,

Pakistan believes that capacity building has a crucial role to play in effectively responding to current and potential cyber threats. Moreover, the need for capacity building becomes more important because of the large gap in terms of capacities and skills between States to deal with the threats emanating from cyberspace. In this regard, we welcome the cyber fellowships offered by the Republic of Singapore which will surely help in the capacity building of the Member States.

Coming to the annual progress report capacity-building portion, Pakistan welcomes it and considers it as action oriented. Pakistan acknowledges that report is cognizant of digital divide among the technology haves and have nots and welcomes the capacity-building proposals such as compiling the calendar of capacity-building programmes, developing a list of regional and sub-regional centers of excellence and finding further avenues of funding for ICT capacity-building on security in the use of ICTs. Pakistan proposes to upload all the capacity-building related activities at the OEWG website for better access.

Mr. Chair,

Pakistan has a proposal for amendment in the annual progress report. We recommend that a proposal could be added as para 11 (h) which could be read as “The OEWG to play a role in ensuring non-discriminatory and equitable access to cybersecurity related technologies, products, and services”.

Taking this opportunity I would like to renew Pakistan’s support for this intergovernmental process of OEWG for safe, secure, and stable cyberspace for all. We believe that the success of the OEWG process depends upon equal and all-inclusive participation of all Member States.

My country will keep on supporting all institutional dialogues under the auspices of the UN aimed at the promotion of responsible behavior of States in cyberspace.

I thank you, Chair.

****

On Revised Draft-2 (Rev-2) of the Annual Progress Report

Mr. Chair,

Pakistan extends its deep appreciation to you and your team for sharing the latest draft annual report. We thank you for your able leadership in guiding the group in a transparent and inclusive manner.

As we are still evaluating the current draft, therefore I am making my preliminary.

My delegation believes that the current draft is a step towards consensus and is more balanced and streamlined, it captures the important progress we have achieved so far. The current draft could be a good basis for the adoption of a consensual annual report at the end of this session.

Coming to the revised draft, for my delegation capacity building is of utmost importance. Pakistan welcomes that the report stresses upon the importance of narrowing the digital divide through tailored capacity building efforts. As mentioned in my earlier intervention, Pakistan once again calls for the inclusion of the language relating to ensuring non-discriminatory and fair access to products, technologies and services relating to cyber security in para 17 (c). We also support that this group should focus on delivering concrete and action-oriented proposals on capacity building.

On existing and potential threats, Pakistan believes that the current text could be a good compromise for all delegations. As for listing of new potential threats, we believe that there is a need for further discussion within this group and inclusion or listing of additional threats should be only made through further discussion and taking into account the views and consideration of all member states.

On international law, Pakistan`s position is well known. We welcome the reference to the legally binding obligations. Pakistan shares the view that it is essential to develop a legally binding international instrument, specifically tailored to the unique attributes of ICTs, to provide a regulatory framework that creates stability and safety in cyberspace. We support Chinese proposal pertaining the inclusion of reference to attribution.

In the area of CBMs, Pakistan welcomes the retention of reference to the formulation of global directory of PoCs.

On the regular institutional dialogue, Pakistan considers the central importance of the UN, therefore supports proposal made by China that all discussion on the PoA should be conducted under OEWG.

Taking this opportunity, I would like to renew Pakistan’s commitment to the OEWG process for a safe, stable and secure cyberspace for all and assure my delegation full support and constructive engagement, leading to the adoption of a consensual annual report.

I thank you, Chair.

Final Statement on 29 July 2022

Mr. Chair,

Firstly, let me commend your efforts and patience to steer the work of OEWG in a steady and balanced manner.

Pakistan believes that this could be the most suitable and balanced outcome document in the given circumstances. Though the proposal made by Pakistan didn’t get

incorporated in the final text, yet in spirit of multilateralism Pakistan would like to join the consensus on the draft circulated last evening.

We believe that the adoption of the annual progress report with consensus will instill the positivity to better help us to better bridge the diverging views in future sessions of the OEWG. Therefore we call upon the other States to be flexible.

Taking this opportunity I would again like to renew Pakistan's support for this intergovernmental process for safe, secure, and stable cyberspace for all.

I thank you Chair.

Philippines

Mister Chair, excellencies, distinguished delegates, ladies and gentlemen, good afternoon.

The Philippines aligns itself with the statement on capacity-building delivered by Cambodia on behalf of ASEAN.

The Philippines highly appreciates the Chair's effort and his team in steering the work of this Group. We remain supportive of your work, Mr. Chair, and we very much appreciate your efforts in producing the revised draft Annual Progress Report. We know that it is not an easy job and we commend you for all your hard work. We view that the current draft annual progress report as sufficiently effective and balanced that can pave the way for a more focused and action-oriented steps towards an open, secure, stable, accessible, and peaceful ICT environment in the coming years.

Mr. Chair,

On "Existing and potential threats," we note that specific mention on the need for focused discussions on the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII) were omitted, which is one of the priorities of the Philippine National Cybersecurity Plan 2022. We prefer the same to be included in part B. Nevertheless, we remain flexible on the matter and we acknowledge that paragraph 8 still recalls the threats identified in the 2021 OEWG report, wherein CI and CII are included.

On "Confidence-building measures," we welcome the retention of the establishment of global points of contact directory on ICT and we highlight the importance of taking into account the best practices of regional and sub-regional experiences, in particular, the ASEAN's development of a Points of Contact and Technical Expert Personnel Directory on cybersecurity.

On "Capacity-building," while we prefer the version of the previous draft, we note that there some reservations on how these capacity-building efforts be best implemented. We note however, and we reiterate our view in the previous substantive session, that two significant concerns that this Group can address are insufficient coordination and complementarity in the identification and delivery of capacity-building efforts. We prefer, in particular, that the request to designate an ICT capacity-building focal point that would foster coordination offers and requests for capacity-building be retained as it would have been a positive step forward in addressing these concerns. These capacity-building efforts could have been limited to those efforts related to the use of ICTs in the context of international security. Nevertheless, we stand ready to support consensus on the matter.

On gender, we join others in supporting reference to the OEWG welcoming the high level of participation of women delegates in its sessions and the prominence of gender perspectives in its discussions; to the OEWG underscoring the importance of

narrowing the “gender digital divide” and of promoting the full, equal and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security; and to States continuing to raise awareness of the gender dimensions of security in the use of ICTs and promote gender-sensitive capacity building at the policy level as well as in the selection and operationalization of projects. We look forward to further discussion on the gender dimensions of security in the use of the ICT in the fourth and fifth sessions of the OEWG as cited under Item F.

Finally, Mr. Chair, we appeal to all Member States to exert their utmost flexibility and work together to reach consensus on the Annual Progress Report, so we can all have a good smoothie that we can enjoy tomorrow afternoon.

Thank you, Mr. Chair.

Republic of Korea

[Introduction]

Mr. Chair,

Let me begin by thanking you the Chair and the Secretariat for organizing this session, and for the effort in drafting the Open-ended Working Group’s first annual progress report that reflects our lengthy discussions during the last two sessions.

As my delegation highlighted at the first session of this OEWG, this five year process is at once a continuation of our past achievements as well as a new chapter for further progression. In this regard, we believe the revised draft dated 20th July serves as a good basis for our deliberations during this week.

We welcome the introductory paragraphs 1 to 6 of the Draft, in particular their mentioning of the *acquis* of cyberspace including the 11 norms of responsible state behavior, the OEWG’s commitment to meaningful stakeholder engagement, and recognition of the role of regional organizations as well as participation of women delegates in its discussions.

Lastly, my delegation would like to extend a warm welcome to the multi-stakeholders present at this third session. My delegation notes the efforts made by the OEWG to provide greater opportunities for their participation, and looks forward to further engaging them in a more meaningful and substantial manner, so that we can incorporate in our discussions the valuable and varied expertise and experience of these stakeholders.

[Existing and Potential Threats]

Mr. Chair,

The last two sessions were a valuable opportunity for all member states to understand how each of us perceives threats in the ICTs environment.

We believe that paragraph 7 reflects the concerns raised by States regarding the growing and evolving nature of threats in the cyberspace in an appropriate manner, as well as the importance of fostering stronger cooperation between cyber emergency response teams, also known as CERTs.

We also support various member states’ proposal to include examples of threat elements such as ransomware and critical infrastructure attacks, as there is value in raising awareness on technical aspects of the threats.

On this note, my delegation would like to reiterate the importance of understanding the human elements of cyber security threats. The fact that the most persistent threat

and vulnerability in cyberspace stems from human behavior is often overlooked, and merits greater attention from the international community.

In this regard, we would like to suggest adding to the list in paragraph 7.b, “Measures to enhance understanding the human elements of ICT threats.”

[Norms, Rules and Principles]

Mr. Chair,

As my delegation highlighted in previous sessions, it has been well established through discussions at various international fora that there is no vacuum of legalities in the cyberspace, as the international law including the UN charter in its entirety applies to cyberspace.

The fact that the norms agreed to at the 2015 GGE reports and other subsequent GGE and OEWG reports have a non-binding and voluntary nature does not imply that states enjoy optionality in conforming to these norms.

This does not rule out the possibility of additional norms developing over time, as paragraph 8.b. duly elaborates. Regarding this, my delegation would like to stress that it is important that these additional norms develop in a way that will complement, not challenge or substitute, existing laws and norms in cyberspace.

Moreover, we believe that discussions to develop additional norms must focus on providing concrete protection to states affected by cyber attacks, and ways to promote implementation of existing norms in that regard.

We support the voluntary national survey of implementation of norms, mentioned in paragraph 8.d, as a useful mechanism for stocktaking the current state of norms implementation in the international community. Republic of Korea has submitted the national survey in March 2020, which we will update and share with the Open-ended Working Group in due course.

[International Law]

Mr. Chair,

Let me first begin by welcoming that the draft report includes “due diligence” in the list of specific topic of international law to be discussed in future sessions in paragraph 9.a. Due diligence is becoming increasingly important in both preventing and responding to cyber incidents. Promoting deeper understanding of this principle will also go a long way in enhancing the implementation of the agreed norms, as many of them are pertinent to the principle of due diligence.

Equally welcomed in the same list is the explicit mentioning of International Humanitarian Law, the importance of which has been echoed by many during our discussions.

Regarding this, we would like to suggest reinstating the deleted clause in the paragraph 9.a. mentioning briefings from ICRC, as we believe it will greatly help enhance member states’ understanding of the IHL in the context of ICTs security.

We hope to see these elements retained in the final outcome.

On the other hand, we suggest deleting the phrase “development of common understanding remains the exclusive prerogative of States” in paragraph 9.a., since such understanding can also be further developed by other entities such as the academia through legal interpretation of the international law.

A useful way of developing such common understanding is through voluntary sharing of national views on how international law applies in the use of ICTs, as mentioned

in paragraph 9.b. We appreciate that many states have submitted their national views, and we plan to submit our own in the second half of this year.

Lastly, The ROK also strongly supports the importance of capacity building on international law, and therefore welcomes the expression in paragraph 9.c. We are committed to promoting better understanding of how international law applies to cyber space through such efforts as ROK-Netherlands Joint Webinar on the Application of International Law in Cyberspace. We also take interest in improving mechanisms for mutual legal assistance regarding malicious use of ICTs mentioned in the same paragraph, and look forward to further discussions in this area.

[Confidence Building Measures]

Mr. Chair,

The ROK is committed to developing and operationalizing CBMs in UN and regional fora. We believe a functioning and effective POC network at the UN level can be a useful starting point for global confidence building. To this end we are participating in the joint effort to establish a UN Cyber POC Network, and believe that it is important to foster greater coordination between such efforts at the UN and those at regional level such as ARF and OSCE. We welcome the paragraph 10.a. and recommended next steps 2 in this regard.

We also believe in the utility of UNIDIR Cyber Policy Portal as a means to promote confidence building, and therefore support its mentioning in paragraph 10.b.

Lastly, we would like to share that ROK is engaged in efforts to enhance CBMs in regional and cross-regional fora, including through co-chairing the ARF Inter-sessional Meeting on ICTs security, and participation in the Cross-regional CBMs group. We hope these regional and cross-regional efforts for CBMs yield concrete results that build and reinforce mutual confidence in cyberspace.

The cross-regional CBMs group is hosting an event on the sideline of this session, and we welcome participation of many member states.

[Capacity Building]

Mr. Chair,

The importance of narrowing the digital divide in making of a safer cyber space has been echoed by delegations across the board during our previous sessions, and the role of capacity building in this regard has gained unequivocal support.

However, a significant gap still exists between the international community’s will for capacity building and concrete mechanisms on which it can rely to that end.

A permanent mechanism dedicated to capacity building efforts to be potentially established within the UN, as mentioned in paragraph 10.d. and recommended next steps 2, is a welcome step in the right direction.

In these paragraphs, we would like to suggest adding PoA as a concrete example of such mechanisms, considering many member states, co-sponsors and others, have recognized its potential role in enhancing capacity building. We suggest adding to the end of paragraph 10.d the phrase “states noted that PoA, among other proposals, could be a possible example of such a mechanism.”

Lastly, the ROK is also actively engaged in capacity building efforts in regional fora such as the ARF and ASEAN, including through proposing Workshops on Fostering Cyber Security Professionals. We are committed to continuing these efforts in and outside of UN.

[Regular Institutional Dialogue]

Mr. Chair,

As a co-sponsor of the Program of Action for advancing responsible State behavior, the ROK shares the same position with other co-sponsors.

We believe that PoA, as a permanent and organized mechanism, can serve as a practical way for operationalizing the various proposals put forward at the OEWG.

We welcome mentioning of PoA in paragraph 12.c. of the draft, and look forward to further discussions and development of the proposal. /end/

Thank you, Mr. Chair.

Republic of Korea expresses its gratitude for Chair and his team's productive efforts, and we'd like to briefly elaborate our views and touch on some of the points raised by other delegations.

To begin with the conclusion, we do view Rev 2 as viable summary of our discussions.

Although not all of the points we raised in our previous intervention are reflected in Rev 2, for us the priority lies in flexibly working towards consensus outcome rather than insisting all our preferences be taken into account. This is especially so considering the nature of this document, which is an annual summary of non-exhaustive nature, as it is repeatedly expressed in the document.

On International Law, we welcome that specific mentioning of the International Humanitarian Law is retained in Rev 2. The principle that existing international law applies to cyberspace has already been agreed to, and during the 3 sessions of this OEWG numerous delegations emphasized the importance of IHL. Therefore we believe IHL merits inclusion in the progress report.

As Croatia, Chile, Switzerland and other delegations mentioned, we also hoped to include explicit mentioning of expert briefings including ICRC in the progress report, but, in the spirit of consensus we can also accept the current version. We'd also like to mention that we do not believe such an exclusion in the progress report precludes future activities of the sort in the following sessions.

On Capacity building, we had initially proposed explicitly mentioning 'PoA' as a concrete example of the permanent capacity building mechanism to be established within the OEWG. However, we can live with the current version in Rev 2, with PoA being mentioned instead in the Regular Institutional Dialogue chapter. We look forward to more focused discussions on this topic in the upcoming sessions.

Lastly, I'd like to briefly echo some proposals by other delegations.

On Threats, we can support mentioning ransom-ware in the report, as proposed by various states during this week's sessions. On CBMs, we can support various delegations' proposal to include mentioning of 'cooperation between CERTs'.

Lastly, on Regular Institutional Dialogue, we support the proposal made by the U.S., Colombia, Canada and others, regarding the expression 'OEWG's centrality'. Considering that past discussions on ICTs security have been conducted in the GGE setting, and that possible future discussions could be conducted in the PoA, we believe that the expression 'current central role' is a more objective and appropriate one.

Once again, we thank the Chair and the team for their dedication and effort, and hope that all delegations can flexibly work towards consensus outcome by tomorrow. /end/

Romania

Mr. Chair,

While Romania aligns itself with the statements delivered by the EU and with the statement of the CZ Republic on the subject of multistakeholders, allow me to make some further remarks in my national capacity.

Romania welcomes the proposal to adopt an annual progress report of the second Open-Ended Working Group (OEWG) on developments in the field of Information and Telecommunication (ICTs) in the context of international security. We commend you, Mr. Chair, and your team's effort for drafting the report and for endeavoring to reach consensus and set a roadmap for the next discussions in this process.

Since the beginning of the work of this group, the cyber threat landscape has changed dramatically and the report should note this evolution, as well as the difficulties that arose in the work of the group in the first year (including in agreeing the modalities).

In this sense, we align ourselves with the remarks from statements delivered by the EU, the US, the Netherlands, the Czech Republic, Poland, Germany and other countries, including today by New Zealand, Ireland, Croatia, Italy and Estonia, in noting the unjustified and unprovoked Russian aggression against Ukraine and support the proposals to reflect the new challenges, in the Threats section, and their impact on the security environment. Not only did we see a hardening of the OEWG process itself, but, we have witnessed the use of cyberattacks in the context of an armed conflict and, as a neighboring country to Ukraine, we note concerning risks regarding (1) collateral effects of cyber operations; (2) potential cross-border spill-over effects; (3) increased and indiscriminate attacks by politically motivated hacker groups on governmental and private ICT infrastructure.

Now, more than ever, we need to adhere to the framework of responsible state behavior in cyberspace and contribute to its security and stability.

We welcome the focus on practical proposals in the report and the efforts by the Chair and his team to balance the content. However, clear delimitation should be given when reflecting the advancements of the group on consensual issues and the identified commonalities, while proper wording should mark the proposals made only by some states.

With regards to the previous work, as a participating state to the 2021 UNGGE and in the final negotiations of the first OEWG, we underline the importance of preserving the acquis by properly referencing the previous UN work in this field, as a basis for the current OEWG. In this respect, we see appropriate to better underline the importance of the UN framework for responsible state behavior in cyberspace. We support, in this sense, previous proposals made yesterday by the Netherlands, Australia and other countries.

We would like to reiterate Romania's strong opinion that existing international law equally applies to cyberspace and that there is no need to develop international legal frameworks to distinctively address cyberspace. As such, we believe that the International Humanitarian Law (IHL) applies in the context of cyber operations carried out as part of an armed conflict, and we underline the need to specifically mention IHL in the report, noting that this mention should not be misunderstood as legitimizing the use of force between States in this domain. We welcome, Mr. Chair, the references to the principles of IHL included in the current draft of the Report.

In reference to the regular institutional dialogue, the wording used in the report regarding the Programme of Action, should not in any way imply that the Program of Action should be created or defined by the OEWG, and the recommendation from the

2019–2021 OEWG should be kept as such. In this respect, the need to avoid duplication of efforts (including with other organizations) should be noted and further discussions on the subject should be welcomed.

I thank you, Mr. Chair.

Russian Federation

Уважаемый господин председатель,
Уважаемые коллеги,

Российская Федерация стояла у истоков переговорного процесса по международной информационной безопасности под эгидой ООН. С самого начала деятельности РГОС, впервые запущенной по нашей инициативе в 2018 г., наше правительство прилагало все усилия, чтобы обеспечить эффективность и результативность Группы на благо укрепления мира и безопасности в сфере использования ИКТ.

С сожалением констатируем, что сторона, принимающая штаб-квартиру ООН, все чаще злоупотребляет своим положением. Соединенные Штаты попытались дешевым способом помешать работе нашей делегации в третьей сессии РГОС. Сорвали участие руководства и экспертов из столицы, чтобы затруднить внесение вклада России в продвижение переговоров. Мы не поддались на провокацию. Решили проявить максимально гибкий и конструктивный подход. Наша задача – усилить отдачу от единственно открытого и демократичного механизма РГОС для формирования международно-правовых основ в информационном пространстве вместо «закона джунглей».

Высоко ценим руководящую роль председателя, уважаемого господина Б.Гафура. Признаем его упорную и последовательную работу в целях достижения Группой практических результатов. Полностью разделяем его суждение о том, что РГОС является важной мерой укрепления доверия между государствами.

У нас сохраняются существенные озабоченности по проекту промежуточного доклада. Не согласны с чрезмерным акцентом на выполнении правил ответственного поведения государств в информпространстве. Считаем нецелесообразным вести речь об отчетности по ним в условиях отсутствия юридических обязательств. Мандат нашей Группы четко закрепляет приоритетную задачу дальнейшей выработки правил, норм и принципов ответственного поведения государств и путей их выполнения.

В целях приведения нашей работы в соответствие с мандатом РГОС, Россия предлагала включить упоминание дальнейшей выработки норм в пунктах, в которых говорится об их выполнении *(в частности, в п.3 Введения, п.14a), рекомендациях 1, 2, 3 раздела C; п.17c), 17d) раздела F).* С учетом консенсусной резолюции ГА ООН №76/19, которая предусматривает возможность выработки в будущем дополнительных обязательств, имеющих юридически обязывающую силу, мы внесли предложение отразить данное положение в докладе *(п.2 Введения, п.14b) раздела C; рекомендация 1 раздела D).*

Россия не согласна с упоминанием применимости отдельных отраслей международного права, в частности, международного гуманитарного права к сфере ИКТ *(п.15b) ii раздела D).*

Доклад Генерального секретаря по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, который является международно признанным инструментом, используемым государствами на

протяжении многих лет, не может быть приравнен инициативам групп государств или неправительственных институтов наподобие Обзора хода реализации на национальном уровне [норм ответственного поведения] и Портала ЮНИДИР о киберполитике *(рекомендация 3 раздела C, рекомендация 3 раздела D, рекомендация 3 раздела F)*. Не следует переоценивать роль ЮНИДИР в контексте усилий по безопасности в сфере использования ИКТ *(рекомендация 3 раздела D)*.

Язык доклада должен быть приведен в соответствие с резолюцией ГА ООН №75/240. Термин «стейкхолдеры», соответственно, – заменен на «другие заинтересованные стороны» *(п.4 Введения; п.16d), рекомендация 4 раздела E; п.17g) и рекомендация 4 раздела F)*.

Существует настоятельная необходимость обеспечения очного участия всех представителей национальных делегаций, а также других заинтересованных сторон, аккредитованных при Группе, в официальных сессиях и межсессионных встречах РГОС, проводимых в штаб-квартире ООН, путем своевременной выдачи виз. Мы предлагали включить соответствующий призыв в текст *(п.6 Введения)* вместо акцента на гендерных аспектах *(п.6 Введения; п.17f), рекомендация 2 раздела F)*, которые не входят в мандат РГОС.

Россия считает, что ООН должна играть собственную роль универсальной организации в контексте усилий по созданию реестра контактных пунктов. Соответствующие региональные инициативы могли бы учитываться в работе и дополнять деятельность в рамках реестра ООН *(п.16b) раздела E)*.

Упоминание ссылок на обмен концептуальными документами, национальными стратегиями, политическими документами и программами по безопасности в сфере ИКТ между государствами *(рекомендация 5 раздела E)* необходимо дополнить тезисами о национальном законодательстве и обмене соответствующими практиками по его выполнению, которые являются элементами мер укрепления доверия.

Мандат РГОС не затрагивает финансовые вопросы. Россия предлагала изменить формулировки о «финансировании» усилий по наращиванию потенциала на их «поддержку» или «осуществление» *(п.17e), рекомендация 2 раздела F)*.

Программа действий является лишь одной из ряда национальных инициатив, представленных в рамках РГОС. Ей не должно уделяться приоритетное внимание. Мы предлагали сделать ссылку на Правила поведения в области международной информационной безопасности и Глобальную инициативу по безопасности данных в *п.18b) раздела G*. Внесли предложение четко отразить в докладе, что мандат РГОС и ее усилия не должны дублироваться в других структурах.

Кроме того, Россия предлагала добавить в документ следующие пункты:

– Государства могли бы рассмотреть возможность закрепления на уровне ООН принципов защиты персональных данных в целях гармонизации подходов государств и содействия безопасному трансграничному обмену информацией *(п.14b) bis раздела C)*;

– Государства отметили важность принятия мер по обеспечению общедоступности, безопасного и стабильного функционирования сети Интернет с учетом суверенитета стран в своем национальном информационном пространстве, а также по обеспечению равноправного участия государств в управлении данной сетью *(п.14c) bis раздела C)*.

Тем не менее, в целях сохранения положительной динамики деятельности РГОС и перспектив прагматичных переговоров до истечения ее мандата в 2025 г. нами

принято решение присоединиться консенсус по документу. Рассматриваем его как обобщение состоявшихся дискуссий, которое должно быть доработано в рамках последующих совещаний Группы. Положения доклада будут учитываться Россией в зависимости от дальнейшего хода переговоров.

Поддерживаем предложение председателя включить в процедурный проект доклада Группы пункт, предусматривающий издание сборника заявлений с разъяснением позиций государств по промежуточному докладу РГОС. Важно, чтобы его оформление полностью соответствовало практике сборника выступлений государств по докладу первой РГОС, в частности, документу должен быть присвоен номер. В ближайшее время представим в Секретариат РГОС комментарии Российской Федерации для отражения в упомянутом сборнике.

Спасибо за внимание.

Distinguished Mr. Chairman,
Distinguished colleagues,

The Russian Federation was the architect of the negotiation process on international information security under the UN auspices. From the very beginning of the OEWG, first launched upon our initiative in 2018, our government has made every effort to ensure the efficiency and effectiveness of the Group for the sake of strengthening peace and security in the use of ICTs.

We regret to say that the party hosting the UN headquarters increasingly abuses its position. The United States tried, in a cheap way, to hinder the work of our delegation at the third session of the OEWG, to prevent the head and leading experts of our team from the capital from participating with a view to impede Russia's contribution to advancing negotiations. We did not succumb to provocation and decided to show the most flexible and constructive approach. Our task is to enhance the productivity of the only open and democratic mechanism, which is the OEWG, for establishing international legal foundations in information space instead of the "law of the jungle".

We highly appreciate the leading role of the Chair, distinguished

Mr. B. Gafoor, and acknowledge his hard and consistent work to achieve practical outcome of the Group. We fully share his judgment that the OEWG is an important confidence-building measure for States.

As for the progress report, we still have a number of significant concerns about the text. We do not agree with excessive emphasis laid on the implementation of rules of responsible behavior of States in information space. It is unreasonable to consider reporting on them in the absence of legal obligations. The mandate of the Group clearly stipulates as a priority to further develop rules, norms and principles of responsible behaviour of States and ways for their implementation.

To align our work with the OEWG's mandate Russia suggested adding the notion of further developing norms, wherever implementation is mentioned *(namely, in para 3 in Introduction; para 14 a), recommendations 1, 2, 3 in section C; 17c), 17d) in section F)*. With regard to the consensus UNGA resolution 76/19, which provides for the possibility of future elaboration of additional binding obligations, we proposed to reflect this provision in the report *(para 2 in Introduction; para 14 b) in section C; recommendation 1 in section D)*.

Russia does not support mentioning the applicability of certain branches of international law, in particular, international humanitarian law to the use of ICTs *(para 15b) ii in section D)*.

The report of the Secretary-General on developments in the field of information and telecommunications in the context of international security, which is a universally recognized instrument utilized by States for years, cannot be put on the same level as initiatives of groups of states or non-governmental institutions like the National Survey of Implementation and the UNIDIR Cyber Policy Portal *(recommendation 3 in section C, recommendation 3 in section D. recommendation 3 in section F)*. The role of UNIDIR in the context of efforts on security in the use of ICTs should not be overestimated *(recommendation 3 in section D)*.

The language of the report should be in line with the UNGA resolution 75/240. The term "stakeholders", respectively, – replaced by "other interested parties" *(para 4 in Introduction; para 16d), recommendation 4 in section E; para 17g) and recommendation 4 in section F)*.

There is a pressing need to ensure in-person participation of all representatives of national delegations, as well as other interested parties accredited to the Group, in formal sessions and intersessional meetings of the OEWG held at the UN Headquarters through timely issuance of visas. We suggested including this call in the text *(para 6 in Introduction)* instead of emphasizing gender aspects *(para 6 in Introduction; para 17f), recommendation 2 in section F)* which are not covered in the mandate of the OEWG.

Russia believes that the UN should play its own role of a universal organization in the efforts on establishing a directory of points of contact. Relevant regional initiatives could be taken into account and be complementary to the UN directory *(para 16b) in section E)*.

References to exchanges of concept papers, national strategies, policies and programmes on ICT-security among States *(recommendation 5 in section E)* should be supplemented with the notion of adherence to the national legislation and exchange of relevant implementation practices which are the part of confidence-building measures.

The mandate of the OEWG does not cover financial issues. Russia suggested changing references to "funding" capacity-building efforts for their "supporting" or "maintaining" *(para 17 e), recommendation 2 in section F)*.

The Programme of Action is just one of a number of national initiatives presented within the OEWG. It should not be prioritized. We suggested making a reference to the International Code of Conduct for Information Security and to the Global Initiative on Data Security in *para 18 b) in section G*. We proposed to clearly reflect in the report that the mandate of the OEWG and its efforts should not be duplicated in other structures.

In addition, Russia suggested the addition of the following paras to the document:

– States could consider the possibility of establishing at the UN level principles of personal data protection in order to harmonize the approaches of States and foster secure transborder data flow *(para 14b) bis in section C)*.

– States note the importance of adopting measures to safeguard the general availability, secure and stable functioning of the Internet taking into account States' sovereignty in their information space, as well as to ensure equal participation of States in the governance of this network *(para 14c) bis in section C)*.

Nevertheless, in order to maintain the positive dynamics of the OEWG and the prospects for pragmatic negotiations until the expiration of its mandate in 2025 we decided to join consensus on the document. We consider it as a summary of the discussions that took place, which should be further elaborated at subsequent meetings of the Group. The provisions of the report will be taken into account by Russia with respect to the progress in negotiations.

We support the proposal made by the Chair to include in the procedural draft report of the Group a paragraph providing for the issuance of a compendium of statements with explanations of positions of States on the OEWG progress report. It is crucial to design it in full compliance with the practice of the compendium of statements of States on the report of the first OEWG – in particular, the document should be assigned a number. We will submit to the Secretariat of the OEWG the comments of the Russian Federation to be reflected in the abovementioned compendium.

Thank you for attention.

South Africa

Thank you, Chairperson.

South Africa would like to recognise the hard work of yourself and your team in preparing Rev 2 of the draft 2022 Annual Report, and for your tireless efforts to find common ground necessary for us to reach consensus on our mandated annual progress report. We believe that this report should provide a roadmap for concrete steps going forward.

We believe that this text is balanced and brings together the various strands that we have discussed in the first, second and third sessions of the OEWG.

We believe that reaching consensus on these aspects, and also agreeing to discuss these matters in a more focus manner throughout the next sessions, will send a positive message that multilateralism works, and that an Open-Ended, inclusive process is invaluable in this regard.

Chairperson,

On some specific matters, we support reference to the role of regional and sub-regional organisations in implementation of the 11 Norms of Responsible State Behaviour.

We are also encouraged that the report recognises the role that Points of Contact can play in promoting dialogue between States. It is practical and actionable initiative such as the PoC that will prove that the OEWG can itself build confidence and be immediately beneficial to all UN Member States.

The draft also takes into account the importance of narrowing the gender digital divide, and the inclusion of the gender dimension in capacity-building programmes, and my delegation welcomes the retention of this crucial aspect of our work. We believe that the reference to the principles of capacity building is also key to enabling context-specific, needs based capacity building.

Finally, we are eager to retain reference to the discussion on a Programme of Action (PoA) within the context of this OEWG. We would like to see a decision on the possibility of a PoA as an outcome of the deliberations of this OEWG, rather than a parallel track. We note that our discussions here on the 6 pillars of ICT security will provide us with vital elements that could be used in developing the PoA.

My delegation would like to assure you of our continued support and positive approach to the work of the OEWG.

I thank you.

Statement by South Africa on the adoption of the Draft 2022 Annual Progress Report of the OEWG on security of and in the use of ICTs, 29 July 2022

Thank you, Chairperson.

South Africa supports the Conference Room Paper that you circulated last night. We thank both you and your team for your hard work.

The current report incorporated many elements that South Africa supports and strikes the right balance in light of our discussions yesterday.

It is of the utmost importance that we adopt a consensus report to give momentum to the five-year-long process and prove the value of the Open-Ended Working Group.

As the delegations of Brazil and India stated yesterday, we also hope that Member States can rally around the multilateral process at work here in the spirit of cooperation.

I thank you.

Spain

España subscribe la intervención realizada por la UE y en su calidad nacional desea hacer los siguientes comentarios.

En primer lugar, agradecemos el trabajo desarrollado por usted, Sr. Presidente, y por su equipo de trabajo en la organización de esta tercera sesión del OEWG, especialmente la elaboración de los dos borradores de trabajo del informe anual de progreso para la Asamblea General, objeto principal de esta sesión. Esperamos también que, bajo su liderazgo, el OEWG sea capaz de definir en este informe las líneas de trabajo a desarrollar en 2023.

Somos conscientes del difícil contexto de la situación internacional en el que el grupo de trabajo tiene que desarrollar su labor. La injustificable invasión de Ucrania por parte de la Federación Rusa ha puesto de manifiesto, entre otras cosas, la importancia del ciberespacio como un nuevo escenario de guerra. Precisamente en esta situación, la labor del OEWG, aunque difícil, se hace más necesaria que nunca.

Como aspectos generales del informe, nos gustaría subrayar que es importante que en el mismo se deje constancia de que el OEWG no parte desde cero, remarcando la importancia de las recomendaciones del anterior OEWG y del Grupo de Expertos Gubernamentales (UNGGE). Es también relevante aprovechar las plataformas e iniciativas ya existentes y evitar la redundancia de esfuerzos con otras iniciativas y organizaciones regionales y nacionales que vienen trabajando en el ámbito de la ciberseguridad. Ya existen amplias redes de colaboración a diferentes niveles, la mayoría formadas por equipos de respuesta a incidentes de seguridad (CERT,s) nacionales, gubernamentales y funcionales, de las que los CERT españoles forman parte. España se ofrece a aportar la experiencia y conocimientos de sus CERT.

En el apartado de ciberamenazas, España propone que el informe incorpore una descripción de las mismas que refleje la realidad de los problemas de seguridad existentes en el ciberespacio y los problemas que implican para la seguridad de los estados, el funcionamiento de la sociedad digital o la privacidad de los ciudadanos.

Es necesario contemplar la necesidad de garantizar, mediante disposiciones técnicas y regulaciones normativas consensuadas, una protección efectiva de la privacidad de

los datos y las comunicaciones personales, así como de la propiedad intelectual en los intercambios transfronterizos e internacionales. En la UE disponemos de un Reglamento General de Protección de Datos que establece altos niveles de seguridad y confidencialidad en la obtención, almacenamiento, difusión e intercambio de los datos personales que podría servir de referente internacional al efecto. Cuanto más asegurada esté tal garantía de protección mayor será la disponibilidad de Estados, empresas y ciudadanos a compartir datos e información.

Respecto a la creación de capacidades, cabe resaltar la necesidad de identificar herramientas concretas de financiación así como mecanismos de transferencia de tecnología. Solo seremos creíbles en nuestros empeñados esfuerzos de colaboración y cooperación internacional para la creación de capacidades técnicas y capacitación humana si somos capaces de comprometernos a compartir tecnología aplicada y movilizar recursos financieros suficientes de una forma sostenible.

España apoya decididamente el impulso del PoA como mecanismo de solidaridad para avanzar en la creación de capacidades. No ahorraremos esfuerzos, junto a nuestros socios europeos, para impulsar la puesta en marcha de dicha iniciativa durante la cuarta y quinta sesiones de trabajo de la OEWG con vistas a dotarla del contenido y alcance más ambiciosos. Invitamos, por ende, a otros países a que se sumen a la misma.

España es partidaria de una participación activa y eficaz de los "stakeholders" privados en los trabajos y tareas del OEWG. Su indispensable contribución a los debates y en la posterior aplicación de las medidas adoptadas en el OEWG podría articularse en torno a un mecanismo permanente de diálogo que integre a representantes de los Estados y del sector privado así como a través de un Directorio de Puntos de Contacto del sector privado y la comunidad tecnológica.

Siendo conscientes de las dificultades que se afrontaron para alcanzar el acuerdo en las modalidades de participación de partes interesadas (stakeholders), España considera que la aplicación práctica de este acuerdo en esta sesión debe llevar a la reflexión sobre el resultado obtenido. Un gran número de entidades, entre ellas una española, con altos niveles de conocimiento y experiencia, han visto rechazada su participación en esta sesión, lo que sin duda supone un empobrecimiento del debate del grupo. Consideramos necesario que cada veto a una entidad vaya acompañado de una justificación del mismo.

Por último, quisiera salir al paso de algún comentario previo sobre la necesidad de abordar los temas de igualdad de género en las tareas del OEWG. Como cualquier organismo de NNUU, este también se debe al conjunto de las resoluciones de la Asamblea General, incluidas las que tratan de cómo alcanzar la igualdad de género. Es un tema que va mucho más allá de la composición paritaria o no de las delegaciones de los estados miembros. La digitalización es una de las nuevas fronteras que debemos superar para que se produzca un aumento general de la productividad de nuestras economías, muy especialmente en el sector servicios, donde se jugará en los próximos años el papel de las mujeres en la división internacional del trabajo. Y una de las condiciones previas es que la ciberseguridad llegue a todos y permita una digitalización que ponga en valor el trabajo de las mujeres. De ahí la importancia de tener en nuestros debates y conclusiones una visión de género. España hará todo lo posible para que así sea.

Esperamos y deseamos que estas sesiones sean productivas y que se logre un acuerdo en torno al informe a presentar a la Asamblea General, incluida la definición de las líneas de trabajo del OEWG para 2023.

Muchas gracias.

Sri Lanka

Thank you chair for giving me the floor. Ambassador Burhan Gafoor May I thank you for your stewardship and efforts in leading this Open-Ended Working Group (OEWG) and congratulate you on effectively driving it forward to the third substantive session. We were happy to see with us the High Representative for disarmament Madam Nakamitsu. The draft of the annual progress report is comprehensive and leaves us much for discussion on seven important aspects.

Sri Lanka wishes to bring to focus the following aspects for the purposes of this discourse. Your proposal that we file an annual progress report is most appropriate and timely. There is much support for such an initiative.

The draft more than cements the phenomena that cyber security is global. That it needs to be dealt through global collaborative efforts. It seeks to identify gaps that needs further attention, it reminds us that there is a need to harness collaborative efforts m consider diverse views to achieve a balanced outcome and build consensus. Such collaborative action will no doubt address the context specific challenges and bridge national and global policies in establishing norms and best practices in regulating the environment in the use of information and communication technology.

Mr. Chair

The draft Looks at the prevalent context specific threats, need for norms and applicability of international law, critical analysis of law and encourages the implementation of a multidisciplinary approach.

Such multidimensional approach will not only facilitate in threat detection but can give productive pointers to security risk management and impact assessment when norms principles and laws are implemented.

Sri Lanka believes that the collaborations can bring in global efforts closer and hence must focus on taking stakeholders such as industry bodies on board to work in parallel with governments, and promote ICT security and continuous innovation in cyber security.

It is pertinent that I briefly refer to site-specific international legal regimes that deal with the prevention of harm across economic sectors by governing firstly AI based processing or personal data and secondly as a target and tool for crime.

AI systems like other information technologies can be a target of and tool for criminal activity, as observed before both of which are within the scope of the 2001 Budapest Convention on cybercrime, also dealt with within the Council of Europe framework with active participation of non-member states from the outset. While universal ratification may be possible for political reasons, one of the principal objectives of the treaty is to harmonize domestic substantive and procedural criminal law as a precondition for more effective international cooperation. Being the first and most widely ratified multilateral treaty on cybercrime this treaty can achieve its objectives we believe without formal global participation, as it simply serves as a model instrument.

The convention which also catches up computer related forgery, computer related fraud, offenses related to child pornography and offenses related to the infringement of copyright. It is interesting to note that like all other criminal offenses, offenses contained in the convention require criminal intent that may be difficult to prove. It is our respectful view that this position must be revisited with a view to examine the proposition whether the concept of fixed liability can be used, thereby calling for an explanation from the respondent with regard to a matter that is particularly within his knowledge.

At just over two decades, old, the international law of cybersecurity remains in a relative state of infancy. This is despite the fact that the period has seen extraordinary advances in cyber capabilities, the exponential growth of societal cyber dependence and a corresponding rise in vulnerabilities to hostile cyber operations.

Indeed, States continue to struggle with such basic issues as sovereignty in cyberspace. In great part, the challenge is that many States are conflicted over the application and interpretation of key aspects of international law in the cyber context as we observe today. But that tension is to be encouraged as it has the potential to produce good results. We need to exploit the tension. After all, although international law can serve as a normative firewall against hostile cyber operations, the principle of sovereign equality must be understood as protective norms and also can act as barriers to a State's own cyber operations, some of which may be deemed essential to the State, especially with respect to national security. These differences of normative perspective often play out domestically in disagreements between ministries with different roles vis-à-vis cyberspace and internationally between States wielding offensive cyber capability and those that see themselves primarily as victims thereof.

Paradoxically, the international community today plainly sees hostile cyber operations as a significant threat to their security and their citizens' welfare, but efforts to legally prohibit or restrict them have borne little fruit. We need to address this issue in all earnest.

Mr. Chair

As much as ICT threats are becoming a rising global challenge, innovative research will no doubt develop understanding on the persistent threats in the ICT environment in the current context and we need to step up our efforts. Sri Lanka wishes to highlight that the current discussions needs to specifically look at the challenges in the industrial sector that needs more targeted delivery.

In particular, during the last two decades there had been vulnerability shown in critical infrastructure such as financial networks, power grids. These sectors have been prone to cyber-attacks. Despite there has been initiatives undertaken through sectoral partnerships, still work remain. This area is regarded as an area that has significant implications for public administration, civilian cyber security as well as ramifications for regulation. Hence, Sri Lanka believes that there is a need for global infrastructure to be built, to foster collaboration.

Mr. Chair,

As the cyber threat landscape continue to grow and expand, developing countries in particular, will require capacity building in the area such as infrastructure and technology, to understand and face the challenges by gaining cyber security management capabilities, in order to strengthen the resilience and preparedness.

Sri Lanka identifies that capacity building in Technical Support training through cooperation programs can build more collaboration, innovative ideas, in overcoming threats, in particular, in internet governance, international law.

Sri Lanka, having recognized that equitable global digital transition requires to meet contemporary challenges inclusive digital governance. Appreciate that developing countries such as Sri Lanka have to face issues such as cybercrime, cyber security, threats, disinformation, and violence. And that, the digitization must be environmentally friendly. We have also recognized the fact that multilateral digital collaboration and connection are required if it is effectively contribute to the green transition. We are also appreciate the fact that the digital technology can be of assistance in dealing with climate change and disaster prevention and that we cannot

have a digital divide that would weaken the whole policy towards digital and the resilience to confront criminality in Cyber space and an abuse of technology.

United Kingdom

The UK extends its thanks to the Chair of the Open-Ended Working Group Ambassador Gafoor, his team, and the working group for all their efforts in this year's discussion and the adoption of our annual progress report by consensus.

This group has taken an historic step in including a clear reference to International Humanitarian Law in this report. The importance of this reference should not be underestimated and we welcome all States flexibility on achieving this outcome, which was important to the UK.

We are pleased to see the group take concrete steps to deliver for Member States in the form of establishing a global Points of Contact Directory. This is an important move forward in binding Member States together in their shared goal of upholding responsible state behaviour in cyberspace.

In addition, the clear roadmap this report puts in place for next year's discussions is crucial if we are to make any kind of progress together. We must go deeper into discussions in order to find elusive consensus on complex issues. That discussion must start now and not wait until we next meet in six months' time.

This is particularly true on capacity building on which we hope to take further steps next time round. We regret that the OEWG was not able to promote practical steps towards building national capacities such as needs assessments and national strategies.

We have joined consensus on this report but note that the OEWG must work to find a balance between providing Member States the support the need to implement the framework of responsible state behaviour and addressing threats to international peace and security in cyberspace, which are real and escalating.

The UK sincerely regrets that the OEWG was unable to fulfil its mandate to promote common understandings of existing threats by commenting on the use of ICTs for military purposes in the Russian war against Ukraine. Resolution 75/240, which created this OEWG, expressed concern *"that a number of States are developing ICT capabilities for military purposes and that the use of such technologies in future conflicts between States is becoming more likely"*. This report should have included clear reference to malicious activity that results in cascading critical infrastructure effects in other States with potentially devastating security, economic, social and humanitarian consequences, and noted that technology plays an increasing role in humanitarian work and malicious ICT activity in conflict situations may also disrupt humanitarian operations.

With regard to the issue of due diligence, the UK recognises the importance of States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States. But the fact that Framework refers to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace. Discussion of due diligence should remain as part of the Rules, Norms and Principles section of the OEWG.

We further regret that the important contribution of regional organisations to development and implementation of the framework, and the inclusion of stakeholders in the OEWG's programme of work, are diminished. We welcome the contributions

of all States, regional organisations and stakeholders to this process so far. The number of both Member States and stakeholders taking part in these discussions has risen substantially since the start of the First OEWG in September 2019 and we hope we continue to further develop inclusive dialogue in coming sessions.

Viet Nam

Mr. Chair,

On behalf of the Vietnamese delegation, I would like to thank you for giving us the floor and in this first intervention, would like to express our full support for leadership at this Working Group.

Viet Nam welcomes the efforts of the Chair in consolidating comments and inputs from Member States to prepare the zero draft of the Annual Progress Report of the Working group which will be submitted to the General Assembly for consideration. These efforts will contribute to the overall objective of the Working Group as contained in Resolution 75/240 of the General Assembly.

Viet Nam also welcomes the 1st revision of the draft Progress Report by the Chair which has considered comments from Member States in the Informal Meeting on 12 of July. This draft will serve as a sound basis for future discussion and deliberation on various aspects of the security of and in the use of ICTs. We also believe that such discussion will help identify confidence building and capacity building measures needed to counter ICTs threats.

Mr. Chair,

Like many delegations in the room, Viet Nam shares the vision of a peaceful ICT environment which is built upon several pillars: first, international law and the United Nations Charter which enable States to cooperate in preventing military threats or conflicts in cyberspace; second, consensus and equal participation of States in formulating legally binding frameworks to resolve issues relating to the use, misuse, and application of ICTs; third, the primary role of States in securing its national ICT environment as well as the constructive collaboration of private and international partners; fourth, rules, norms and principles of responsible State behaviours and confidence building measures in cyberspace to prevent miscommunication, misperception and miscalculation.

In reaching that vision, we recognize the role of OEWG processes as steppingstones and therefore attach great importance to the efforts of all Member States in reaching agreement on the Annual report, which takes note of the progress made and helps shaping the future discussions of the Working group.

Mr. Chair,

Viet Nam is of the view that the discussion in the Working group has made significant progress even though major differences in national positions remain. Therefore, at this stage, the draft Report should: first, focus on the core issues with vision to address common ICT concerns in the context of international security and avoid controversial and divisive language; and second, contain items that have reached consensus and reflect comprehensively all views that have been exchanged in previous OEWG and GGE processes, including ICTs threats, application of international law in cyberspace, rules, norms and principles of responsible State behaviours, confidence building and capacity building measures as well as regular institutional dialogue.

Viet Nam will participate actively at this Working Group to foster a common vision on the security of and in the use of ICTs. We have accordingly submitted to the Chair our detailed comments on the draft Report during this session.

I thank you for your kind attention.

Viet Nam's inputs on the draft Annual Progress Report of the OEWG Chair

Third Substantive Session of the Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025) (OEWG) *New York, 25-29 July 2022*

1. Existing and potential threats (Section B)

In paragraph 7(a), it is suggested to be revised as follows: "States, recalling the threats identified in the 2021 OEWG report *and the consensus reports of the GGEs*, reiterating increasing concern…"

2. International Law (Section D)

Paragraph 9 should contain the reaffirmation of States that international law, in particular the UN Charter and International Humanitarian Law, is applicable in the ICT environment, as reflected in the 2021 OEWG report.

With regard to the proposed non-exhaustive list of topics for further discussion by the Working group (paragraph 9a), the topic of the principle of no threat or use of force should be included.

It should also be reaffirmed that States should show responsible behaviour in the use of ICTs and promote the use of ICTs and the development of new technologies for peaceful purposes and public interest. Moreover, the draft Report should reflect the necessity to develop legally-binding framework for responsible state behaviour. The adoption of a Code of conduct in the field of ICTs security could be further elaborated in this regard.

4. Capacity-Building (Section F)

Paragraph 11a could be further improved through revision as follows: "The OEWG could encourage the mainstreaming of the principles of ICT capacity-building… as well as better integrate ICT-capacity-buildiong efforts into the *implementation of the Sustainable Development Goals under the 2030 UN Agenda*…"

5. Regular institutional dialogue (Section G)

The draft Annual Report should reiterate the conclusion of the OEWG as reflected in the 2021 Report. It should not focus on the elaboration of a PoA in the future work of the OEWG as Member States have yet thoroughly discussed about the future mechanism for institutional dialogue.

6. Other matters

There should be further discussion about other aspect of ICTs, including the terminology of ICT/cybersecurity, international cooperation on ICTs, the role of regional and sub-regional organizations in confidence and capacity building initiative.