Declaración conjunta de la sociedad civil sobre la paz cibernética y seguridad humana

Primera Comisión de Desarme y Seguridad Internacional de la Asamblea General de las Naciones Unidas el 12 de octubre 2022

Hace un año, la sociedad civil entregó conjuntamente una declaración a este Comité en que reconocimos que, a pesar de algunos desarrollos importantes por las Naciones Unidas para avanzar la paz cibernética y seguridad internacional, el panorama de amenazas seguía siendo sombrío. Desafortunadamente, algunas de las preocupaciones que nosotros destacamos persisten y la seguridad general del ambiente en línea continúa deteriorándose.

Las capacidades cibernéticas ofensivas son más generalizadas entre los Estados, así como el uso de ciber mercenarios. Las ciber operaciones son más frecuentes y sofisticadas, incluso en su focalización de infraestructura crítica y la interrupción de servicios críticos tales como atención médica, tanto como las cadenas de suministro, incluyendo las de la tecnología de información y comunicación (TIC).

En el contexto de la invasión continuada rusa en Ucrania, las ciber operaciones se emplean con frecuencia en apoyo o complementarias de operaciones militares cinéticas para interrumpir la entrega de servicios críticos civiles o para destruir infraestructura crítica. Estas operaciones han impactado a la población civil, causando también efectos secundarios desestabilizadores. El uso de estas operaciones en las hostilidades entre Rusia y Ucrania eleva puntos importantes para clarificar en cuanto a la aplicación de la ley internacional y ley internacional humanitaria en particular, al mismo tiempo subraya la necesidad para mecanismos de rendición de cuentas y la condenación clara de actos que violan las leyes internacionales y normas acordadas de comportamiento estatal en el ciberespacio.

El internet y los dispositivos conectados están siendo usados en maneras que tienen impactos en los derechos humanos, tales como vigilancia, hackeo, censura y la disrupción intencional de los servicios del internet y a cómo accederlos. Se ha mostrado que estas medidas impactan y dañan desproporcionadamente a los individuos y grupos de la sociedad, por ejemplo periodistas, defensores de derechos humanos, comunidad LGBTI, mujeres y otros quien ya puede estar en posiciones de vulnerabilidad o marginalización.

El costo de las operaciones cibernéticas sin restricciones en la seguridad humana aumenta cada día, y como consecuencia, las discusiones y decisiones que surgen de los procesos relevantes de la ONU necesitan abordarlas de manera más eficaz. Estos esfuerzos deben ser guiados por enfoques basados en los derechos humanos y en los derechos para establecer un ambiente de TIC pacífico, que incluye el principio de inclusión y participación significativa de las partes interesadas. Las modalidades de acreditación que han permitido el veto de más de 30 partes interesadas no gubernamentales de participar en el Grupo de trabajo de

composición abierta de la ONU (OEWG por sus iniciales en el inglés) sobre la TIC, por ejemplo, deben mejorarse para permitir la participación significativa de todas las partes interesadas relevantes. A pesar del progreso reciente en modalidades de participación del OEWG, hay mucho espacio para mejorar la calidad.

Contra este telón de fondo, establecemos colectivamente las siguientes llamadas a la acción:

- Detectar el despliegue y uso de las capacidades, actividades, estrategias y doctrinas dañinas del ciber. Estamos particularmente preocupados sobre las acciones dirigidas contra infraestructura y servicios críticos, que incluye la atención médica e infraestructura de información; el núcleo público del internet, acciones contra el sector humanitario, el uso de ciber mercenarias y los que impactan a las personas, especialmente civiles.
- Tomar acción urgente para implementar las normas cibernéticas acordadas y operacionalizar los principios de creación de capacidad cibernética que se acordaron el OEWG de los años 2019-2021, en cooperación y consulta con partes interesadas no gubernamentales.
- Tomar acción rápida para establecer mecanismos que fomenten la transparencia y cierren las brechas de rendición de cuentas. Deliberaciones ad-hoc como las que existen actualmente dentro de la ONU no van suficientemente lejos para abordar de manera significativa las amenazas actuales y futuras, se necesita un foro permanente de la ONU con la participación significativa de las partes interesadas. En este contexto, el propósito para un programa de acción cibernética merece una consideración acelerada.
- Llevar a cabo debates e intercambios centrados sobre cómo la ley internacional se aplica en el ambiente TIC. Es alentador que Estados adicionales están publicando sus interpretaciones nacionales y entendimientos sobre cómo la ley internacional gobierna su comportamiento cibernético, pero se necesita más ambición. En particular, los estados deben proponer *opinio juris* que reafirma la aplicabilidad de las leyes internacionales de derechos humanos en el ciberespacio en todo momento. La comunidad internacional que incluye actores no gubernamentales también podría mapear vacíos en la ley existente y producir recomendaciones para abordarlos, con miras a aprovechar, no duplicar, el trabajo existente en esta área.
- La tendencia creciente de los estados para atribuir responsabilidades para operaciones cibernéticas es positiva, pero apoyaríamos más transparencia en las políticas de criterio y atribución usadas para fomentar el uso de ley internacional o normas de la ONU cuando se denuncie acciones cibernéticas dirigidas y patrocinadas por el estado para crear conciencia y apoyo a las limitaciones legales y normativas.
- Reconocer el impacto en cuanto a derechos humanos de las operaciones cibernéticas internacionales y abstenerse de usar leyes relacionadas con seguridad, politicas y practicas cibernéticas como pretexto para violar derechos humanos y libertades

fundamentales. Por esto, los Estados deben reconocer y dirigirse de los impactos diferenciales de operaciones cibernéticas sobre individuos y grupos en la sociedad ya quienes están en posiciones de vulnerabilidad o marginalización, por ejemplo los periodistas, defensores de derechos humanos, comunidad LGBTI y mujeres entre otros. Salidas relevantes de la comunidad de derechos humanos de la ONU, incluyendo el Consejo de Derechos Humanos y la Oficina del Alto Comisionado de Derechos Humanos, ofrecen ayuda a este respecto.

- Asegurar la participación regular y significativa de partes interesadas no gubernamentales en el OEWG actual y en futuros foros de la ONU. Actores diversos tienen un papel establecido para jugar en la operacionalización y promoción de las normas cibernéticas y la ley internacional relevante, construyendo capacidad y resiliencia, construyendo confianza en el monitoreo y respuesta a incidentes cibernéticos. Se necesita integrar mejor esta experiencia y pericia en los diálogos cibernéticos de la ONU.
- Buscar complementariedad y comunicación entre los varios procesos en cuestiones relacionadas con la cibernética y seguridad digital, que incluye los que se establecieron el Primer y Tercer Comité, el Secretario General de la ONU y organismos de derecho humano y cuerpos técnicos también.