145th IPU Assembly

Kigali, Rwanda
11-15 October 2022

Versión original: inglés/francés - Traducción: Lic. Carina Galvalisi Kemayd
www.secretariagrulacuip.org

Comisión Permanente de
Paz y Seguridad Internacional

C-I/145/6-Inf.1
13 de septiembre de 2022

Audiencia de expertos sobre el tema *Ciberataques y ciberdelitos: los nuevos riesgos para la seguridad mundial*

Viernes 14 de octubre de 2022, 14:30 – 16:30
(Sala MH1, Planta Baja, Kigali Convention Centre (KCC))

Nota conceptual

Vivimos hoy en una situación de conflictos globales a gran escala. Ningún gobierno o parlamento del mundo podría prever el sufrimiento de todos los ciudadanos de nuestro planeta ante una pandemia como la de COVID-19.

Para proteger a nuestros ciudadanos, todos los gobiernos tomaron la decisión de someter a millones de personas en el mundo a medidas restrictivas y bloqueos.

A raíz del confinamiento de la población en sus hogares, hubo un aumento en las interconexiones a redes y en la adquisición de dispositivos, cámaras, computadoras y teléfonos inteligentes para poder conectarse a empresas y escuelas, o simplemente para comunicarse con familiares y amigos.

Esta digitalización forzada permitió a la población mantener vínculos comunicativos sociales y profesionales con los centros de trabajo, escuelas y universidades, y especialmente con las instituciones públicas de salud y los medios de comunicación. De esta forma, las personas pudieron conocer en tiempo real la evolución de la pandemia y las medidas que se estaban tomando en sus respectivos países.

La digitalización a un ritmo acelerado y forzada ha abierto nuevos espacios que mucha gente desconocía hasta ahora. Sin embargo, a nivel individual y colectivo, también han aparecido nuevos espacios más riesgosos donde los ciberdelincuentes han aumentado su radio de acción utilizando nuevos sistemas de ciberataque.

Por otro lado, el grave conflicto que estamos presenciando en Ucrania ha dado lugar a hostilidades que Europa no experimentaba desde la Segunda Guerra Mundial. Ha revelado que los ciberataques también se pueden utilizar para hacer la guerra en períodos de máxima tensión.

Debemos trabajar para prohibir las armas autónomas letales (también conocidas como “robots asesinos”), priorizar la protección de toda la infraestructura nuclear de posibles ciberataques externos y evitar una nueva escalada en la amenaza nuclear global.

Las campañas masivas de desinformación y propaganda utilizan las plataformas digitales para contaminar e influir en grupos, regiones o países. Las campañas se realizan a través de ciberactivistas organizados conscientes de la ausencia de marcos de cooperación jurídica internacional.

Los ataques directos a los sistemas informáticos de la infraestructura crítica de un país ponen en riesgo las redes básicas de distribución de bienes esenciales en nuestras sociedades.

Todo esto nos debe hacer reflexionar y profundizar en la realidad global que nos rodea como parlamentarios. Conocer la verdad hoy se está convirtiendo en un bien cada vez más preciado.

Un nuevo contexto digital también requiere la acción de nuestros parlamentos y las Naciones Unidas. Esto permitirá maximizar los beneficios y potencialidades de nuestra sociedad del conocimiento, al mismo tiempo que se minimizan los graves riesgos que nos amenazan.

Según el artículo 19 de la Declaración Universal de los Derechos Humanos, toda persona tiene derecho a recibir y difundir información e ideas por cualquier medio, sin consideración de fronteras. Por tanto, debemos garantizar que todos los ciudadanos de nuestras sociedades puedan acceder libremente a una información objetiva, veraz y de calidad.

En el espíritu de la Declaración Universal de los Derechos Humanos, debemos asegurarnos de que se desarrolle un discurso público para que, en lugar de confrontar, dividir, polarizar o destruir nuestra convivencia con mensajes virales de odio, nuestras democracias puedan fortalecerse cada vez más.

Debemos tener derecho a proteger nuestros datos e información personal, que se utilizan para manipular y cambiar nuestro comportamiento, controlarnos, violar nuestros derechos humanos y socavar las instituciones democráticas.

Es necesario legislar para definir los límites de los algoritmos opacos y el uso de perfiles psicográficos por parte de las grandes corporaciones para evitar que organizaciones malintencionadas y ciberdelincuentes utilicen las redes sociales para influir y manipular las tendencias de los votantes.

Debemos alentar al sector público, al sector privado y a la sociedad civil a adoptar nuevos marcos legislativos y de autorregulación que desarrollen un espacio seguro para la cooperación digital global.

Como parlamentarios debemos establecer marcos de cooperación jurídica internacional para poder combatir de manera efectiva a los ciberdelincuentes que actúan fuera de cualquier tipo de control y que pueden servir a oscuros intereses para atacar infraestructuras críticas en nuestros países.

Conscientes de las limitaciones de las capacidades de los países para perseguirlos, los ciberdelincuentes actúan globalmente y desarrollan ataques a gran escala contra los usuarios. Despliega todo tipo de ingeniería social y técnicas de ataque. Estos incluyen: ataques a contraseñas personales, como phishing, vishing, smishing y spam; ataques a las conexiones, como wifi falso, suplantación de identidad, cookies, DDoS, SQL y sniffing; y ataques de malware, como virus, adware, spyware, troyanos, puertas traseras, keyloggers, ladrones, ransomware, rootkits, botnets, rogueware, cryptojacking y otras aplicaciones maliciosas.

En 2015, los Miembros de la UIP adoptaron una resolución en la Asamblea de Hanói sobre la ciberguerra, que también abordó el delito cibernético. La resolución pedía una convención internacional sobre estos crímenes.

En cuanto a nuestros parlamentos, debemos ofrecer estructuras operativas capaces de proteger a sectores especialmente vulnerables (como mujeres, jóvenes, niños, empresas e infraestructura crítica) y buscar desarrollar iniciativas que nos permitan identificar, catalogar, analizar y prevenir los ciberataques.

En el contexto de la Convención sobre Ciberdelincuencia, la UIP puede y debe hacer una valiosa contribución a las Naciones Unidas en el esfuerzo global de brindar servicios para prevenir, sensibilizar, detectar y responder adecuadamente a los incidentes de ciberseguridad en cualquier país del mundo.