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

146ª Asamblea de la UIP
Manama (11–15 de marzo de 2023)

Comisión Permanente de
Paz y Seguridad Internacional

C-I/146/M
17 de enero de 2023

Los ciberataques y los ciberdelitos: los nuevos riesgos para la seguridad mundial

<u>Memorándum explicativo</u> presentado por los co-Relatores
Sr. J. Cepeda (España) y Sra. S. Falaknaz (Emiratos Árabes Unidos)

1. Vivimos en un mundo cibernético. Millones de personas interactúan entre sí a través de Internet utilizando todo tipo de dispositivos y compartiendo sus datos, información personal, identidad y actividad diaria con el mundo. Nuestra vida cotidiana, nuestros datos personales, nuestros servicios de salud, nuestras infraestructuras y nuestra seguridad se rigen por redes ubicadas en el ciberespacio.

2. A medida que las tecnologías han avanzado y ha aumentado nuestra dependencia de ellas, también han aumentado los ciberdelitos y ciberataques contra ciudadanos, grupos vulnerables, instituciones, gobiernos o Estados, así como la necesidad de velar por nuestra seguridad.

3. Las numerosas medidas de contención adoptadas en todo el mundo debido a la pandemia de COVID-19 han fomentado la compra y el uso de dispositivos electrónicos que permiten a los ciudadanos mantenerse en contacto con el mundo exterior. Esta transformación digital forzada ha provocado un fuerte aumento de la ciberdelincuencia.

4. Los parlamentos son conscientes del riesgo que esta situación representa para los ciudadanos. Por ello, los co-Relatores han elaborado esta resolución, con el fin de proteger a los ciudadanos frente a un ciberespacio hostil y sensibilizar a la comunidad internacional sobre la necesidad de combatir la ciberdelincuencia y los ciberataques, cooperando y compartiendo una visión común sobre cómo actuar con eficacia contra los delincuentes y piratas informáticos, que no conocen fronteras ni límites.

5. Esta resolución también tiene como objetivo examinar los desafíos de la lucha contra el delito cibernético y los ataques cibernéticos, fortalecer el papel de los parlamentos frente a los riesgos asociados y contribuir a los esfuerzos internacionales en esta área.

6. La lucha contra el delito cibernético y los ataques cibernéticos enfrenta varios desafíos, incluidos los desacuerdos sobre las definiciones, la legislación obsoleta y la alta prevalencia de prácticas que comprometen la confidencialidad, la integridad y la disponibilidad de los datos informáticos. Las diferencias en la legislación entre países a menudo retrasan los procedimientos judiciales. La rápida evolución de estos delitos requiere una mayor cooperación internacional.

7. Ya se han lanzado varias iniciativas de ciberdelincuencia a nivel regional e internacional, incluido el establecimiento por parte de la Asamblea General de las Naciones Unidas de un comité especial para desarrollar una convención internacional integral para combatir el uso de la información y las comunicaciones con fines delictivos. Esta convención será adoptada por la Asamblea General en su septuagésimo octavo período de sesiones en 2024. La UIP también ha abordado el tema de las interacciones conflictivas en el ciberespacio en su resolución titulada *La ciberguerra: una grave amenaza para la paz y la seguridad mundiales* (2015).

8. La naturaleza de estos delitos y su proliferación han dado lugar a nuevas áreas de acción y nuevas iniciativas a nivel regional e internacional, por ejemplo:

   a) El Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa, aprobado en 2021, que establece un escudo legal para la protección de los derechos humanos, el estado de derecho y los datos personales;

   b) Las nuevas iniciativas impulsadas por determinadas instituciones para obligar a los fabricantes y proveedores de productos o servicios TIC que operen en su territorio a ofrecer "sistemas de certificación seguros" o la creación de nuevos sistemas de identificación y autenticación electrónicos seguros y fiables, por ejemplo monederos digitales personales mediante la tecnología de la cadena de bloques e integrada en los teléfonos móviles, que ofrecen nuevas soluciones de garantías, trazabilidad e identidad en Internet demandadas por determinados organismos, como INTERPOL, para luchar contra la delincuencia.

9. A los efectos de la elaboración de este proyecto de resolución, los co-Relatores participaron en las siguientes reuniones:

   - la segunda sesión del citado Comité Especial de las Naciones Unidas, en Viena en mayo y junio de 2022;

   - dos reuniones de consulta entre sesiones de múltiples partes interesadas organizadas por el Presidente del Comité Especial (junio y noviembre de 2022), durante las cuales compartieron información sobre el trabajo realizado por la UIP en el campo de la lucha contra el delito cibernético y los ataques cibernéticos;

   - la audiencia de expertos sobre el tema de la resolución, organizada por la Comisión Permanente de Paz y Seguridad Internacional durante la 145ª Asamblea de la UIP en Kigali, en octubre de 2022, durante la cual recibieron aportes de expertos y contrapartes de diferentes regiones del mundo, así como así como del Foro de Jóvenes Parlamentarios;

   - El componente parlamentario del Foro de Gobernanza de Internet, realizado en Etiopía en diciembre de 2022, cuyo objetivo era resaltar la importancia de tener una visión parlamentaria para abordar futuras amenazas cibernéticas que los ciudadanos puedan enfrentar y crear un espacio digital más seguro;

   - la audiencia en línea sobre el tema *Creación de un ciberespacio seguro para la democracia*, organizada en diciembre de 2022 por la UIP en colaboración con el Presidente del Comité Especial para facilitar la inclusión de las opiniones de los parlamentarios en la preparación de la Convención sobre Ciberdelincuencia y para solicitar aportes para el desarrollo de esta resolución de la UIP.

10. Los co-Relatores también participaron en reuniones bilaterales con diversas organizaciones, como la Subdivisión de Crimen Organizado y Tráfico de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) e INTERPOL, y pudieron conocer *in situ* los sistemas de protección establecidos para combatir los ciberataques en diferentes países como Albania, Argentina, Costa Rica, Emiratos Árabes Unidos, España, México y República Dominicana, donde también pudieron conocer el trabajo que realizan los servicios de seguridad e inteligencia, así como las medidas adoptadas por los parlamentos y otras instituciones.

11. Todas estas reuniones y visitas permitieron identificar los diferentes niveles donde es necesario actuar:

    a) Ciberataques entre estados en el contexto de guerras híbridas. El tema del conflicto y la guerra en el ciberespacio ya ha sido considerado por la UIP en su resolución de 2015 titulada *La ciberguerra: una amenaza grave para la paz y la seguridad mundiales*, que subraya que la defensa cibernética y la lucha contra el delito cibernético son complementarias. Es importante tener en cuenta que los gobiernos pueden utilizar los servicios de actores no estatales para llevar a cabo ataques cibernéticos contra terceros países, lo que puede conducir a una escalada y representar una amenaza para la paz mundial.

    b) Campañas de ciberataques en forma de ciberespionaje, robo de propiedad intelectual, extorsión de datos e información en poder de organismos gubernamentales, parlamentos, instituciones públicas o privadas (ataques de *ransomware*), o ataques realizados por ciberdelincuentes contra la infraestructura estratégica de un país. Algunas de estas campañas se pueden definir como "amenazas persistentes avanzadas", es decir, ciberataques complejos a gran escala en los que los intrusos se establecen de forma ilícita y permanente en una red para recuperar datos altamente sensibles.

    c) Ataques de ciberdelincuencia, en forma de delitos en línea, llevados a cabo por delincuentes que se dedican a actividades delictivas realizadas a través de Internet u otras herramientas de comunicación digital y que tienen como objetivo principal a los ciudadanos. Estos ataques tienen una variedad de objetivos, que incluyen el robo de identidad, el fraude, la distribución de material ilegal o protegido por derechos de autor, el tráfico de drogas, el lavado de dinero, los delitos de odio, la propaganda, el adoctrinamiento extremista y la explotación sexual de mujeres y niños, y utilizan diferentes tácticas, técnicas y métodos, como la suplantación de identidad, la piratería, la utilización de robots informáticos o los ataques de denegación de servicio, haciendo del ciberespacio un lugar inseguro y hostil para todos los ciudadanos del mundo.

12. Ya se trate de ataques cibernéticos a gran escala llevados a cabo por grupos organizados o delitos en línea perpetrados por delincuentes, la respuesta al delito cibernético solo puede basarse en la cooperación internacional, logrando que los países pongan en común su información y conocimientos sobre las tácticas, técnicas y procedimientos utilizados por estos piratas informáticos

13. El proyecto de resolución:

- pide a los parlamentos que adopten nuevas leyes y desarrollen la cooperación internacional para combatir el delito cibernético y los ataques cibernéticos, dado el aumento constante de este tipo de actividades contra ciudadanos, grupos vulnerables, instituciones, gobiernos o Estados, su vínculo con libertades fundamentales como la privacidad y la libertad de expresión, el hecho de que no deben menoscabar ni disminuir la capacidad de los ciudadanos para disfrutar de estas libertades, y sus consecuencias para la paz y la seguridad internacional y la estabilidad económica mundial;

- alienta a los parlamentos a apoyar los esfuerzos de las Naciones Unidas para adoptar una nueva convención sobre el delito cibernético y utilizarla para fortalecer la legislación nacional y aumentar la cooperación internacional en la lucha contra el delito cibernético y los ataques cibernéticos;

- pide a los parlamentos que hagan el mejor uso de sus herramientas de supervisión para garantizar que el ejecutivo actúe contra el rápido aumento de la ciberdelincuencia respetando la privacidad de los usuarios en el ciberespacio;

- también pide a la Secretaría de la UIP que desempeñe un papel clave para ayudar a los parlamentos a desarrollar su capacidad mediante la organización de conferencias,

talleres y seminarios especializados que puedan ayudar a crear conciencia sobre la naturaleza compleja y rápidamente cambiante del delito cibernético y los ataques cibernéticos y para combatir estos fenómenos.