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/DR
17 de enero de 2023

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

***Proyecto de resolución* presentado por los co-Relatores**
Sr. J. Cepeda (España) y Sra. S. Falaknaz (Emiratos Árabes Unidos)

La 146ª Asamblea de la Unión Interparlamentaria,

1) *Condenando* todas las formas de ciberdelitos y ciberataques, y *reafirmando* la necesidad de combatir estos actos a través de la cooperación internacional y la elaboración de marcos jurídicos apropiados,

2) *Considerando* que debemos generar confianza entre los países frente a los ciberdelincuentes, que no conocen fronteras ni límites,

3) *Observando* la creciente dependencia del ciberespacio de personas, instituciones y Estados,

4) *Consciente* del aumento de la ciberdelincuencia y los ciberataques vinculados a la aceleración de la transformación digital, en particular la impuesta por la pandemia de COVID-19,

5) *Tomando nota* de la responsabilidad de los parlamentos de proteger a los ciudadanos en el ciberespacio utilizando nuevas infraestructuras y recursos, de la misma manera que en el mundo físico,

6) *Recordando* las siguientes resoluciones de la Asamblea General de las Naciones Unidas: 31/72 de 10 de diciembre de 1976 titulada *Convención sobre la prohibición del uso de técnicas de modificación ambiental con fines militares o cualquier otro propósito hostil*, 55/63 de 4 de diciembre de 2000 y 56/121 de 19 de diciembre de 2001 titulada *Combatir la explotación de la tecnología de la información con fines delictivos*, 57/239 de 31 de enero de 2003 titulada *Creación de una cultura mundial de la ciberseguridad*, y 69/28 de 2 de diciembre de 2014 titulada *Avances en la tecnología de la información en el contexto de la seguridad internacional*,

7) *Subrayando* la importancia de los convenios regionales sobre ciberdelincuencia, delincuencia organizada transnacional, intercambio de información y asistencia administrativa, en particular, el *Convenio del Consejo de Europa sobre ciberdelincuencia*, de 23 de noviembre de 2001 y su *Protocolo adicional relativo a la tipificación como delito de los actos de carácter racista y xenófobo cometidos a través de sistemas informáticos*, de 28 de enero de 2003, el *Acuerdo de Cooperación para Garantizar la Seguridad Internacional de la Información entre los Estados Miembros de la Organización de Cooperación de Shanghai*, de 16 de junio de 2009; y la *Convención Árabe sobre la lucha contra los delitos relacionados con las tecnologías de la información*, de 21 de diciembre de 2010,

8) *Recordando* el trabajo de la UIP sobre los diversos nuevos riesgos a los que están expuestas nuestras sociedades cada vez más digitalizadas, en particular las resoluciones de la UIP tituladas *La ciberguerra: una grave amenaza para la paz y la seguridad mundiales* (adoptada el 1º de abril de 2015 en la 132ª Asamblea, en Hanói) y *La legislación en todo el mundo para combatir la explotación y el abuso sexuales de niños en línea* (adoptada el 30 de noviembre de 2021 en la 143ª Asamblea, en Madrid), que también recuerda el Convenio del Consejo de Europa titulado *La protección de los niños contra la explotación y abuso sexuales* (Convenio de Lanzarote) de 25 de octubre de 2007,

9) *Preocupada* por la falta de instrumentos jurídicos universales destinados a reprimir la ciberdelincuencia y los ciberataques,

10) *Acogiendo con beneplácito* los esfuerzos realizados por las Naciones Unidas para adoptar, a través de la resolución 74/247 de la Asamblea General, de 27 de diciembre de 2019, una convención internacional integral para combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos, y acogiendo con beneplácito la creación de un comité especial para redactar esta convención,

11) *Acogiendo con beneplácito* el hecho de que la UIP esté participando en el proceso de consulta de múltiples partes interesadas de este comité especial para hacer que la voz de los parlamentos sea escuchada,

12) *Tomando nota* de la necesidad de aplicar un enfoque integral y global al problema de la ciberdelincuencia y los ciberataques, en particular mediante el desarrollo de un marco jurídico internacional para combatir la ciberdelincuencia y los ciberataques y sus graves consecuencias para los ciudadanos, y para proteger la paz, la seguridad mundiales y la estabilidad económica,

13) *Reconociendo* que los legisladores y los gobiernos deben tomar urgentemente medidas más fuertes a nivel nacional para combatir el cibercrimen y los ciberataques, dada su multiplicación y rápida evolución,

14) *Reconociendo también* que es necesaria una acción parlamentaria conjunta de alcance internacional para ofrecer un escudo protector a los ciudadanos, gobiernos y países, quienes son todos partes interesadas en esta tarea,

15) *Reconociendo* que las mujeres, los jóvenes y los niños son los más vulnerables y las primeras víctimas de los ataques en Internet, y son afectados personal, social, cultural y económicamente por las acciones de los ciberdelincuentes,

16) *Notando* la naturaleza de las amenazas y los riesgos de la ciberdelincuencia transnacional y los ciberataques para la paz y la seguridad internacionales, así como el rápido desarrollo del ciberespacio, por lo que los métodos utilizados por los ciberdelincuentes son cada vez más sofisticados,

17) *Notando también* que los delitos y los ataques cibernéticos abarcan no solo los ataques a las tecnologías de la información y la comunicación (TIC), las violaciones de la privacidad y la creación y despliegue de software malicioso, sino también los ataques a la infraestructura nacional estratégica, así como otros actos que pueden ocurrir fuera de línea y ser facilitados por las TIC, incluido el fraude en línea, la compra de drogas, el lavado de dinero, los delitos de odio, la propaganda, el adoctrinamiento extremista y la explotación sexual de mujeres y niños a través de Internet, todo lo cual tiene un impacto negativo en la seguridad global y la estabilidad económica,

18) *Considerando* que la mayoría de las leyes nacionales fueron adoptadas mucho antes de que aparecieran los ciberdelitos y los ciberataques y, por lo tanto, no siempre permiten responder con eficacia a estas amenazas,

1. *Pide* a la comunidad internacional, a través de las Naciones Unidas, que adopte una definición global común de ciberdelincuencia y ciberataques, que abarque todas las variantes de estas actividades y las acciones que pueden provocar;

2. *Alienta* a los parlamentos a pedir al ejecutivo que apoye los esfuerzos de las Naciones Unidas para adoptar una nueva convención sobre ciberdelincuencia participando activamente en su redacción;

3. *Insta* a los parlamentos y los gobiernos a que insistan en la necesidad de incluir en la convención una definición integral de ciberdelincuencia y ciberataques, así como mecanismos para apoyar la cooperación internacional para combatir la ciberdelincuencia y los ciberataques;

4. *Invita* a los parlamentos y gobiernos a utilizar esta convención, una vez adoptada, como un medio para fortalecer la legislación nacional y aumentar la cooperación internacional para combatir la ciberdelincuencia y los ciberataques;

5. *Pide* a los parlamentos que promulguen nuevas leyes sobre ciberdelitos y ciberataques, dada la escala y frecuencia cada vez mayores de tales actividades y sus implicaciones para la paz y la seguridad internacionales y la estabilidad económica mundial;

6. *Alienta* a los parlamentos a hacer pleno uso de su función de supervisión para garantizar que los gobiernos cuenten con las herramientas necesarias para combatir el rápido aumento de la ciberdelincuencia y los ciberataques y para proteger la seguridad digital, la identidad, la privacidad y los datos de los ciudadanos, especialmente de las personas más vulnerables;

7. *Recomienda firmemente* a los parlamentos establecer marcos legislativos para proteger la infraestructura de Internet, en particular los cables submarinos, las redes satelitales y los servicios esenciales de Internet, así como los grandes centros de datos públicos y privados que brindan servicios en la nube, los que a su vez deberían intercambiar información sobre los ciberincidentes, en tiempo real, a través de los organismos nacionales y supranacionales pertinentes;

8. *Alienta* a los parlamentos a promover un ciberespacio seguro instando al ejecutivo a cooperar para erradicar el ciberdelito y evitar que los ciberdelincuentes actúen, respondiendo a las solicitudes de asistencia, cuando sea posible en tiempo real, asegurando la cadena de suministro de las empresas en su país, a informar de posibles vulnerabilidades a terceras partes para ayudarlos a prevenir futuros incidentes y, en particular, a apoyar y proteger a todos los equipos de respuesta a incidentes cibernéticos dentro y fuera de las fronteras de su país;

9. *Alienta también* a los parlamentos a elaborar leyes que promuevan servicios transversales de ciberseguridad centrados en la prevención (concientización, auditoría y capacitación) y detección de incidentes (24 horas al día, 7 días a la semana) y que permitan una respuesta inmediata y efectiva a las amenazas cibernéticas;

10. *Recomienda* que los parlamentos establezcan instituciones y órganos apropiados, por ejemplo, centros nacionales de ciberseguridad, equipos de respuesta rápida en el área informática, equipos de respuesta a incidentes de seguridad informática y centros de operaciones de seguridad, cuando aún no existan en su país;

11. *Recomienda también* que todos los parlamentos se aseguren de que estas instituciones y órganos cuenten con suficientes recursos presupuestarios y personal especializado para poder responder con flexibilidad y eficacia a los ciberataques y para proteger las infraestructuras estratégicas, las instituciones públicas, las empresas y los ciudadanos;

12. *Insta* a los parlamentos a que promuevan la coordinación internacional entre estas instituciones y organismos y la creación de un centro de operaciones de seguridad global bajo la égida de las Naciones Unidas para monitorear, prevenir y detectar amenazas cibernéticas de manera continua, para investigarlas y combatirlas;

13. *Recomienda* que esta entidad ayude a todos los países, en particular a aquellos con menos recursos, a desarrollar sus capacidades de acción y reacción, a poner en común su información, sus conocimientos y los resultados de sus investigaciones, para anticiparse a futuros desafíos tecnológicos como la computación cuántica, 5G, metaverso e inteligencia artificial, y dar la voz de alarma en caso de violación de la Declaración Universal de los Derechos Humanos, en cualquier circunstancia;

14. *Pide* a los parlamentos que fomenten la inversión en investigación y desarrollo, incluyendo disposiciones específicas sobre ciberseguridad en proyectos de ley y propuestas legislativas, y proporcionando suficientes créditos presupuestarios, para anticipar posibles ciberamenazas emergentes y protegerse de ellas;

15. *Alienta* a los parlamentos a construir alianzas con empresas, instituciones académicas y todas las demás partes interesadas, incluida la sociedad civil, para desarrollar un ecosistema de ciberseguridad fuerte y colaborativo;

16. *Alienta también* a los parlamentos a crear espacios legislativos que permitan a los parlamentos, los gobiernos, las empresas, el mundo académico y la sociedad civil cooperar en tiempo real para defender el interés general de todos los Estados;

17. *Pide* a los parlamentos y parlamentarios que trabajen activamente para desarrollar, a nivel nacional, una comprensión común y actualizada de la naturaleza de la ciberdelincuencia y los ciberataques tal como los experimentan los ciudadanos, las organizaciones y las instituciones;

18. *Insta* a los parlamentos a contribuir al desarrollo de una verdadera "cultura de ciberseguridad" mediante el desarrollo de programas educativos destinados a capacitar a las generaciones futuras, desde la infancia, en el uso de las herramientas tecnológicas, tanto en términos de las amplias oportunidades que ofrecen como de los importantes riesgos asociados a ellas;

19. *Recomienda* que los parlamentos refuercen la protección de las mujeres, los jóvenes y otros grupos vulnerables en el ciberespacio, asegurando el respeto de los derechos humanos e incluyendo en las políticas educativas relacionadas con el uso de las redes sociales mecanismos para prevenir la violencia de género;

20. *Insta* a los parlamentos a que tomen las medidas necesarias para proteger los momentos cruciales de la democracia, en particular los períodos en que los ciudadanos ejercen su derecho al voto, a fin de evitar ataques e injerencias encaminadas a influir, modificar o violar la libre formación de la opinión de los ciudadanos durante los procesos electorales;

21. *Pide* a la comunidad internacional que tome medidas para proteger la democracia garantizando que todos los parlamentos del mundo, como instituciones que representan la voluntad del pueblo, gocen de una protección especial a través de su inclusión en las listas de infraestructura nacional crítica y servicios esenciales;

22. *Pide* a los parlamentos que examinen más de cerca la naturaleza compleja y cambiante de la ciberdelincuencia y los ciberataques mediante la organización de seminarios, talleres y conferencias especializados sobre este tema;

23. *Invita* a la Secretaría de la UIP, junto con las organizaciones interesadas, a promover esta nueva visión de la ciberseguridad apoyando a los parlamentos en sus esfuerzos de creación de capacidad;

24. *Recomienda* que la UIP, como organización mundial de los parlamentos, pueda desempeñar un papel de liderazgo en la gobernanza internacional de Internet y la resiliencia cibernética, participando en todos los foros internacionales pertinentes,

incluidos los organizados por las Naciones Unidas, para hacer oír la voz de los parlamentos, a fin de prever toda amenaza cibernética a la seguridad, los medios de subsistencia o la forma de vida de los ciudadanos, y poder prepararse, resistir, responder y superarlas.