Servicio de traducción al español – GRULAC - Unión Interparlamentaria
Versión original: inglés/francés - Traducción: Lic. Carina Galvalisi Kemayd
www.secretariagrulacuip.org

Unión Interparlamentaria
ommier 5, C.P. 330, CH-1218 Le Grand-Saconnex/Geneva, Switzerland

LA CIBERGUERRA: UNA AMENAZA GRAVE PARA LA PAZ Y LA SEGURIDAD MUNDIAL

Resolución aprobada por consenso[i] por la 132ª Asamblea de la UIP
(Hanói, 1º de abril de 2015)

La 132ª Asamblea de la Unión Interparlamentaria,

Consciente que las tecnologías de la información y de la comunicación (TIC) constituyen un medio de inclusión y de desarrollo, y que estas no deben ser utilizadas por los Estados u otros actores no estatales para violar el derecho internacional, en particular los objetivos y principios de la Carta de las Naciones Unidas relativos a la soberanía, la no intervención, la igualdad soberana de los Estados, la solución pacifica de las controversias y el principio de abstención de recurrir a la amenaza o al empleo de la fuerza,

Reconociendo el trabajo realizado por el Grupo de Expertos Gubernamentales de la ONU encargado de examinar el progreso en el área de la información y de las telecomunicaciones en el contexto de la seguridad internacional,

Considerando que el acceso de los individuos al ciberespacio implica, entre otros, una amplia gama de comunicaciones digitales, por medio de sistemas satelitales, de redes de fibra óptica, de programas informáticos avanzados, así como un intercambio sistemático de información, de datos gráficos, audiovisuales e informatizados, de herramientas y equipamientos inteligentes, software, sistemas operativos avanzados, y la posibilidad de utilizarlos para sus propios fines,

Reconociendo que el uso inapropiado de la tecnología puede tener efectos adversos a nivel nacional, regional, y aun mundial, y que es necesario establecer un plan internacional de autoridades y mecanismos legales para reglamentar la utilización y la destinación,

Convencida, en vista de las inmensas ventajas socioeconómicas que el ciberespacio aporta al conjunto de los ciudadanos del mundo, que es esencial asegurar la previsibilidad, la seguridad de la información y la estabilidad en esta área,

Habiendo considerado las resoluciones 31/72 de 10 de diciembre de 1976 (sobre una convención sobre la prohibición de utilizar técnicas de modificación del medio ambiente para fines militares o todos otros fines hostiles), 55/63 de 4 de diciembre de 2000 (sobre la lucha contra la explotación de las tecnologías de la información para fines criminales),

69/28 de 2 de diciembre de 2014 (sobre el progreso de la informática y de las telecomunicaciones y la seguridad internacional) y 57/239 (sobre la creación de una cultura mundial de la ciberseguridad) de la Asamblea General de las Naciones Unidas,

Reconociendo la importancia de los acuerdos regionales e internacionales sobre el cibercrimen transnacional organizado, el intercambio de información y la asistencia administrativa, incluyendo la Convención de 1977 sobre la prohibición de utilizar técnicas de modificación del medio ambiente para fines militares o todos otros fines hostiles, de la Convención Árabe de 2010 sobre la lucha contra las infracciones sobre las tecnologías de la información, de la Convención del Consejo de Europa sobre el cibercrimen y de su Protocolo Adicional (relativo a la penalización de los actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos), así como el Acuerdo de 2010 de la Organización de Shanghái para la cooperación en el área de la seguridad internacional de la información, y *reconociendo también* la importancia de la cooperación internacional para prevenir la ciberguerra,

Plenamente consciente que algunos conceptos, definiciones y normas de la ciberpolítica, en particular en lo que concierne a la ciberguerra, así como a la paz y la seguridad internacionales, no son comúnmente comprendidos y no han sido todavía clarificados a nivel nacional, regional y multilateral, y que no existe todavía consenso internacional en ciertas áreas,

Recibiendo con satisfacción los progresos realizados en los foros internacionales en lo que concierne a la elaboración de una percepción común de comportamiento aceptable de parte de los Estados en el ciberespacio, en particular en el seno del Grupo de Expertos Gubernamentales de la ONU encargado de examinar el progreso en el área de la información y las telecomunicaciones en el contexto de la seguridad internacional, así como las otras iniciativas bilaterales, regionales y multilaterales en esta área,

Reconociendo que ciertos principios del derecho internacional público, en particular los enunciados en la Carta de las Naciones Unidas, las Convenciones de Ginebra de 1949 y sus protocolos adicionales, la Declaración Universal de los Derechos Humanos y el Pacto Internacional de los derechos civiles y políticos, así como en la Convención sobre la eliminación de todas las formas de discriminación contra la mujer, son pertinentes y aplicables al ciberespacio y son esenciales para el mantenimiento de la paz y de la estabilidad internacionales y para la promoción de un ambiente informático abierto, seguro, pacífico y accesible, tanto para las mujeres como para los hombres,

Considerando que el ciberespacio sobrepasa la Internet, que el uso de hardware, software, de datos y de sistemas de información puede tener efectos que van mas allá de las redes y de la infraestructura informática, y es percibido como un instrumento de crecimiento económico, y que existen desigualdades en el ambiente informático, en particular desigualdades entre los sexos,

Perfectamente consciente del hecho de que las diferentes áreas de la ciberpolítica son distintas pero están inextricablemente ligadas y que pueden tener un impacto en las dimensiones de la paz y la seguridad internacionales del ciberespacio, y viceversa,

Considerando que la utilización oculta e ilegal, por los individuos, las organizaciones y los Estados, de los sistemas informáticos de los países extranjeros para agredir a

terceros países, es una cuestión que suscita una viva preocupación, en razón de los riesgos de conflictos internacionales conexos,

Considerando también que el ciberespacio puede ser explotado como una nueva dimensión del conflicto, así como también un nuevo campo de actividad en el que numerosos componentes del ciberespacio, si no la mayoría, pueden tener aplicaciones a la vez civiles y militares,

Consciente de que el ciberespacio no es un lugar aislado y que las actividades de desestabilización en el ciberespacio pueden tener efectos graves en otras aéreas de la vida de la sociedad mundial, entrañar otras formas de inseguridad o de conflictos tradicionales, o hacer surgir nuevos tipos de conflicto, *convencida además* que una cooperación regional e internacional es necesaria para luchar contra las amenazas resultantes de una utilización maliciosa de las TIC,

Convencida que los Estados deben alentar al sector privado y a la sociedad civil a jugar un rol apropiado para mejorar la seguridad de las TIC y su utilización, en particular en lo que concierne a la seguridad de la cadena de aprovisionamiento de los productos y servicios informáticos,

Consciente de que los sistemas informáticos militares concernientes al despliegue y empleo de la fuerza están expuestos a los actos de ciberguerra que podrían permitir a terceros países interceptar y desplegar estos sistemas para causar un uso no autorizado, ilegal y destructivo de la fuerza, *preocupada* de que los sistemas militares totalmente autónomos (“robots asesinos”) son especialmente vulnerables a estos despliegues no autorizados en la medida en que las decisiones finales concernientes a los objetivos no necesitan validación humana, y *particularmente preocupada* de que la piratería de los sistemas de comando y de control de las armas nucleares podrían llevar al lanzamiento y a la detonación de armas nucleares y causar catástrofes sin precedentes,

Constatando que la utilización de las TIC ha reconfigurado el marco de seguridad nacional e internacional y que estas tecnologías pueden ser utilizadas para fines malintencionados y para violar los derechos humanos y civiles, y *constatando también* que en estos últimos años ha aumentado considerablemente el riesgo de que las TIC sean utilizadas por actores estatales y no estatales para realizar actividades criminales y cometer particularmente actos de violencia contra las mujeres y las niñas, así como actividades de desestabilización,

Consciente de las repercusiones que podrían tener la utilización ilícita de las TIC sobre la infraestructura de los Estados, la seguridad nacional y el desarrollo económico, y *consciente* de que la única solución viable para prevenir estas nuevas amenazas y abordarlas, consolidar las ventajas de las TIC, prevenir los eventuales efectos negativos, promover la utilización pacífica y legitima, y asegurar que el progreso científico tenga por objetivo preservar la paz y contribuir al bienestar y al desarrollo de los pueblos reside en la cooperación entre todos los Estados que permita también evitar que el ciberespacio no se transforme en un campo de operaciones militares,

Considerando que la ciberguerra puede comprender, sin necesariamente limitarse a esto, operaciones contra un ordenador o un sistema informático a través de la utilización de un flujo de datos como medio o método de guerra dirigida a reunir información para fines de desestabilización económica, política o social, o que razonablemente puede apuntar a causar muerte, heridas, destrucción o daño durante los conflictos armados, pero no solamente en estos,

Consciente de que las medidas de ciberdefensa y de lucha contra el cibercrimen son complementarias y *notando a este respecto* que la Convención del Consejo de Europa sobre el cibercrimen (Convención de Budapest), único tratado internacional sobre los crímenes cometidos por medio de Internet o de otras redes informáticas, está abierto a la adhesión, inclusive por terceros países,

Notando que no se conoce todavía completamente la utilización militar del ciberespacio y los impactos de ciertas actividades, y *notando también* que numerosas ciberactividades pueden tener por efecto desestabilizar las condiciones de seguridad, en función de su naturaleza, nivel, potenciales consecuencias y otros elementos,

Preocupada de que los planificadores militares proponen mantener la lógica de disuasión nuclear entre otros métodos para hacer frente a la amenaza existencial de un ciberataque,

Reconociendo que una falta de comunicación estratégica entre Estados, la ausencia de atribución rápida de responsabilidades y una percepción limitada de las prioridades de los aliados y de los adversarios puede dar lugar a errores de juicio, de apreciación y malentendidos en el ciberespacio, y de ahí la importancia de instaurar medidas de confianza para mejorar la transparencia, la previsibilidad y la cooperación entre los Estados,

Considerando que los riesgos para la paz y la seguridad internacionales han aumentado con el desarrollo y la difusión de técnicas y herramientas maliciosas sofisticadas por los actores estatales y no estatales,

Oponiéndose a que los Estados se sirvan del ciberespacio para aplicar medidas económicas, restrictivas o discriminatorias contra otros Estados, con el fin de limitar el acceso de estos últimos a la información o a los servicios,

Condenando la utilización de las TIC en contravención del derecho internacional, de los objetivos y principios de la Carta de las Naciones Unidas y de las normas de coexistencia entre los Estados reconocidas a nivel internacional,

Condenando también la utilización de la TIC por los grupos criminales o terroristas para comunicar, recabar información, reclutar, organizar, planificar y coordinar los ataques, promover sus ideas y sus acciones y solicitar financiamiento, *consciente* de que, al hacer esto, estos grupos con frecuencia explotan la vulnerabilidad de ciertos grupos sociales, y *condenando además* la utilización del ciberespacio para causar la desestabilización y amenazar la paz y la seguridad internacionales,

Notando la necesidad de trabajar para la conclusión de una convención internacional sobre Internet a fin de evitar que esta sea utilizada por terroristas u organizaciones terroristas para llevara a cabo actividades ilegales, en particular para recaudar fondos, reclutar miembros o difundir ideas que inciten a la violencia o al odio,

Recordando que los actos de violencia sexual en periodo de guerra o de conflicto son considerados como crímenes de guerra y *consciente* de que la difusión de estos actos por medio de las TIC para intimidar, amenazar o aterrorizar a los ciudadanos, las comunidades o los países y forzarlos a someterse constituye un crimen de ciberguerra,

Considerando que es necesario alcanzar un equilibrio entre el control del ciberespacio para fines de la seguridad y el respeto de la vida privada, de los secretos de Estado, de la propiedad intelectual, así como de las prioridades en materia de desarrollo de la

administración en línea del comercio electrónico,

Considerando también que es necesario desarrollar a nivel nacional, regional e internacional las medidas concretas para reforzar la confianza en el área de las TIC,

Condenando toda utilización voluntariamente indebida de las tecnologías, inclusive, pero no únicamente, para fines de espionaje financiado por los Estados,

1. *Recomienda* que los parlamentos refuercen sus capacidades a fin de comprender mejor la complejidad de la seguridad nacional e internacional en el ciberespacio y de tomar en cuenta la interconexión entre los diferentes aspectos de la elaboración de la ciberpolítica;

2. *Alienta* a los parlamentos a trabajar con los otros poderes del Estado, la sociedad civil y el sector privado para una apreciación general de la dependencia, así como de los riesgos y las dificultades en el ciberespacio a nivel nacional, para reducir los efectos negativos de la ciberdependencia, en particular en lo que respecta al desarrollo de la administración en línea y a la seguridad nacional, y a promover la adopción de estrategias nacionales de ciberseguridad,

3. *Exhorta* a todos los parlamentos a revisar el marco jurídico de su país a fin de adaptarlo mejor a las nuevas amenazas en materia de criminalidad, de terrorismo y/o de guerra susceptibles de derivarse de la naturaleza evolutiva del ciberespacio;

4. *Exhorta también* a los parlamentos a luchar a través de la acción legislativa contra los actos de violencia sexual cometidos contra las mujeres y las niñas en tiempos de guerra y conflicto, que constituyen crímenes de guerra, así como contra la difusión de estos actos por medio de las TIC, que constituyen un crimen de ciberguerra;

5. *Alienta* a los parlamentos a proceder a un control escrupuloso de las finanzas públicas para asegurar que suficientes recursos sean asignados para la ciberseguridad;

6. *Alienta también* a los parlamentos a hacer uso de todas las herramientas de control a su disposición para asegurar que las actividades vinculadas al ciberespacio sean sometidas a un examen riguroso y a adoptar las leyes nacionales que sancionen más fuertemente los ciberataques, teniendo debidamente en cuenta la Constitución y aplicando medidas de precaución, así como los mecanismos de gobernanza y las estructuras existentes para proteger la libertad de expresión y no comprometer la facultad de los ciudadanos de utilizar las herramientas informáticas;

7. *Recomienda* a los parlamentos de los Estados que aún no lo han hecho, a exigir de su respectivo gobierno que declare expresamente que el derecho internacional, particularmente el derecho de los conflictos armados, se aplique a la ciberguerra a fin de asegurar que se establezcan límites a la utilización de las ciberoperaciones como medio o método de guerra, al tiempo que nota que las modalidades de aplicación exacta están todavía en discusión a nivel internacional;

8. *Alienta* a los parlamentos a trabajar con los otros poderes del Estado y con la sociedad civil en la elaboración de una estrategia de ciberseguridad que englobe

la ciberdefensa, el fortalecimiento de las capacidades y la lucha contra el ciberterrorismo;

9. *Invita* a los parlamentos a apoyar la difusión de información sobre la ciberseguridad y sobre las buenas prácticas entre todas las partes interesadas en su país;

10. *Llama* a todos los parlamentos a asegurar una participación significativa de todas las partes interesadas, en particular el sector privado, la academia, la comunidad técnica y la sociedad civil, incluyendo las organizaciones y asociaciones femeninas, en el tratamiento de las ciberamenazas ligadas a la utilización de las TIC;

11. *Recomienda* que los parlamentos de los Estados dotados de armas nucleares llamen a sus respectivos gobiernos a renunciar a las políticas de lanzamiento de alerta, a retirar las armas nucleares del estado de disponibilidad operacional y a extender el plazo de toma de decisión concerniente a su empleo a fin de evitar la activación y el despliegue no autorizado de sistemas de armas nucleares en el marco de los ciberataques, conforme a los acuerdos en curso de negociación para prohibir el empleo de las armas nucleares y asegurar su eliminación;

12. *Llama* a todos los parlamentos a asegurar que las leyes y las reglamentaciones nacionales no protejan a los individuos que hacen utilización criminal de la cibertecnologia para fomentar los conflictos internacionales y no les garanticen inmunidad ni les aseguren refugio;

13. *Alienta* a los parlamentos nacionales a promover una cooperación y una asociación estrecha entre el sector público y privado, de manera de mejorar la eficacia de las estrategias de ciberseguridad y de ciberdefensa a nivel nacional;

14. *Recomienda* la implementación de un plan estratégico de información en el que estarían asociados el sector de la enseñanza, las comunidades organizadas y los ciudadanos, a fin de sensibilizar sobre los beneficios y la utilidad de la integración en el ciberespacio, así como sobre las potenciales repercusiones de una utilización indebida de este ultimo;

15. *Recomienda también* que los Estados respeten el derecho internacional y la Carta de las Naciones Unidas en su utilización de las TIC y que prevean, a nivel legislativo y ejecutivo, las medidas de cooperación para favorecer la paz, la estabilidad y la seguridad internacionales, así como una definición común del derecho internacional aplicable, y las normas, reglas y principios derivados en cuanto al comportamiento a adoptar por los Estados;

16. *Alienta* a los parlamentos a promover la adhesión lo más amplia posible a la Convención del Consejo de Europa sobre el Cibercrimen (Convención de Budapest), de manera de reforzar la legislación nacional y mejorar la eficacia de la cooperación internacional contra el cibercrimen;

17. *Recomienda* que los parlamentos presionen por la formulación y adopción a nivel regional e internacional de una reglamentación y un control suficiente para hacer que la utilización del ciberespacio sea plenamente compatible con el derecho internacional, la Declaración Universal de los Derechos Humanos y el Pacto Internacional de los Derechos Civiles y Políticos, así como las normas de coexistencia reconocidas a nivel internacional y las medidas concretas de fortalecimiento de la confianza para aumentar la transparencia, la previsibilidad y

la cooperación y para reducir los malentendidos, lo que limitaría el riesgo de conflicto por medio del ciberespacio;

18. *Invita* a los parlamentos a apoyar la utilización de instrumentos de ayuda y otros medios de fortalecimiento de las capacidades para prevenir y combatir las ciberamenazas;

19. *Exhorta* a la UIP, así como a las organizaciones internacionales competentes, a apoyar la cooperación parlamentaria a fin de promover los acuerdos internacionales que garanticen el mejor uso de las TIC por los países, así como una utilización segura y apropiada del ciberespacio, de intercambio de las buenas prácticas en cuanto a las medidas que permitan reforzar la confianza y, por tanto, favorecer la paz, la estabilidad y la seguridad internacionales, pues estas reducen los riesgos para la seguridad que se desprenden de la utilización de las TIC, y a desarrollar sistemas de colaboración;

20. *Alienta* a los parlamentos a jugar un rol positivo en la creación de un ambiente seguro para apoyar una utilización pacífica del ciberespacio y para asegurar que la libertad de expresión y el intercambio de información sean conciliadas de manera apropiada con las preocupaciones de seguridad y de seguridad pública;

21. *Alienta también* a los parlamentos a trabajar con su gobierno en la elaboración de acuerdos internacionales destinados a prevenir la ciberguerra, a extender el conjunto del derecho internacional relativo a la paz y la seguridad al ciberespacio, al establecimiento de normas mundiales y al control de las respuestas nacionales e internacionales a los ciberataques a fin de asegurar que estas sean compatibles con estas normas y acuerdos;

22. *Alienta además* la cooperación internacional a fin de brindar a los países en desarrollo una asistencia técnica y un fortalecimiento de las capacidades en lo que concierne a la prevención, así como a la investigación, la persecución y la sanción de los infractores, y a asegurarles una mayor seguridad de las redes frente a la ciberguerra;

23. *Llama* a la UIP a instar a la ONU a adoptar una resolución que prohíba el control ilegal de las infraestructuras esenciales, tales como las redes de aprovisionamiento de agua, electricidad y las redes hospitalarias, así como los ciberataques contra estas infraestructuras;

24. *Alienta* a la ONU a mejorar la ciberseguridad por medio de un registro mundial de los ciberataques;

25. *Recomienda* revisar y actualizar los instrumentos jurídicos, los acuerdos, y los acuerdos de cooperación, en particular en lo que concierne al ciberespacio, la ciberseguridad, la tecnología y las telecomunicaciones;

26. *Sugiere* que, sobre la base de la presente resolución, la UIP proponga que la Asamblea General de las Naciones Unidas convoque una conferencia sobre la prevención de la ciberguerra que adoptaría una posición común sobre las cuestiones pertinentes y redactaría una convención internacional sobre la prevención de la ciberguerra.

---

[i] *La delegación de Venezuela expresó una reserva a la utilización del término "ciberguerra".*