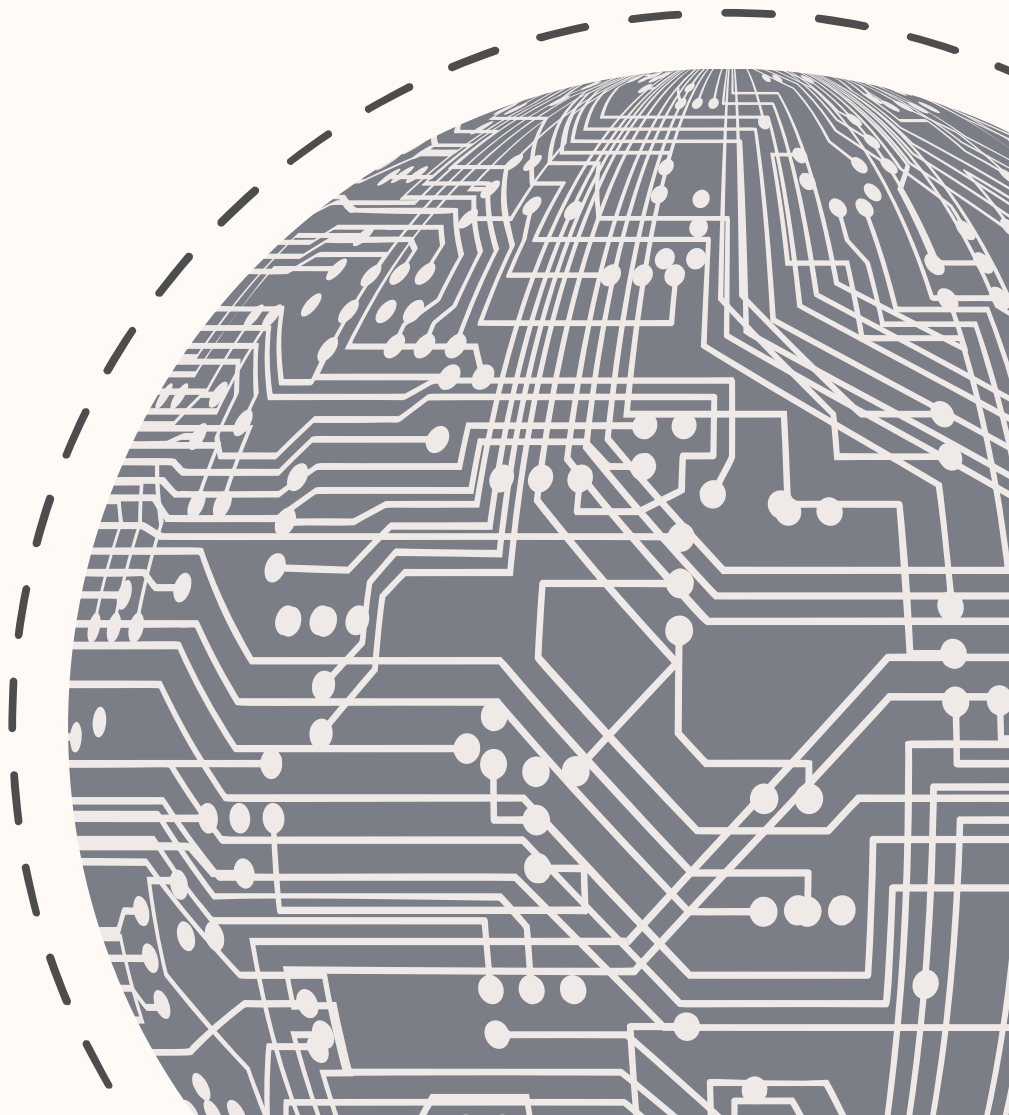
Cancillería

Posición Nacional de Colombia sobre la APLICACIÓN DEL DERECHO INTERNACIONAL AL CIBERESPACIO

2025



Cancillería

Laura Camila Sarabia Torres
Ministra de Relaciones Exteriores

Mauricio Jaramillo Jassir
Viceministro de Asuntos

Andrea Jiménez Herrera
Directora de Asuntos Jurídicos Internacionales

Jhon Jairo Camargo Motta
Director de Asuntos Políticos Multilaterales

Rosario Gutiérrez Bernal
Coordinadora GIT Consultoría para Asuntos en Derecho Internacional

Laura Quintero Buriticá
Coordinadora GIT de Prevención del Delito

Álvaro Frías Galván
Tercer Secretario GIT Consultoría para Asuntos en Derecho Internacional

Lucía Solano Ramírez
Consejera – Asesor Legal Misión Permanente de Colombia ante la ONU en Nueva York

Nathalia Trujillo Castro
Pasante

2025

Cancillería

TABLA DE CONTENIDOS

Cancillería

1. Introducción

La aplicación del Derecho Internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados se ha debatido en las Naciones Unidas, en el marco de los entonces Grupos de Expertos Gubernamentales (GEG), el anterior Grupo de Trabajo de Composición Abierta sobre la Seguridad y en el Uso de las Tecnologías de la Información y, actualmente, en el Grupo de Trabajo de Composición Abierta sobre Seguridad y en el uso de las Tecnologías de la Información y las Comunicaciones (2021-2025) (GTCA), creado en virtud de la Resolución 75-240 de la Asamblea General.

Como han señalado los Informes Periódicos Anuales del GTCA, sus sesiones se han celebrado en un entorno geopolítico difícil, con una creciente preocupación por el uso malicioso de las tecnologías de la información y la comunicación (en adelante TICs) por parte de actores estatales y no estatales, dirigido contra infraestructuras críticas y servicios esenciales. En este escenario, los Estados, incluido Colombia, han recordado y reafirmado que el Derecho Internacional, en particular la Carta de las Naciones Unidas, es aplicable al ciberespacio y es esencial para mantener la paz, la seguridad y la estabilidad y promover un entorno de TICs abierto, seguro, estable, accesible y pacífico.

En este contexto, a continuación, se expone la posición de Colombia sobre este tema con el propósito de contribuir a al avance de un marco robusto e inclusivo para la aplicación del Derecho Internacional en el uso de las TICs, que lleven a evitar malentendidos y a aumentar la previsibilidad y la estabilidad en el ciberespacio. Para ello, Colombia ha tenido en cuenta las medidas recomendadas en el GTCA donde se ha invitado a los Estados a compartir voluntariamente sus opiniones y posiciones nacionales sobre esta materia.

Así las cosas, este documento de posición nacional expone la visión actual de la República de Colombia sobre la aplicación del Derecho Internacional en el ciberespacio y refleja muchas de las posiciones expresadas por Colombia en diversos foros multilaterales. No pretende hacer un análisis exhaustivo sobre el tema, sino ilustrar la posición general del Estado sobre algunos temas específicos relacionados con este asunto.

Adicionalmente, valga mencionar que este documento fue preparado por el Ministerio de Relaciones Exteriores de la República de Colombia[1]en consulta con el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones y la Consejería Presidencial para la Transformación Digital, así como múltiples partes interesadas.

***

2. Aplicación del Derecho Internacional

Colombia considera que, para alcanzar y mantener la paz, la estabilidad y la seguridad internacionales, es esencial que los Estados cumplan con las obligaciones que les impone el Derecho Internacional. En este sentido, todas las actividades desarrolladas por los Estados en el ciberespacio deben regirse y, de hecho, se rigen por el Derecho Internacional. Esto incluye el acatamiento de los principios y de las obligaciones consagradas en la Carta de las Naciones Unidas, tales como la igualdad soberana, no intervención en los asuntos internos de otros Estados, el arreglo pacífico de las controversias internacionales a fin de preservar la paz y la seguridad internacionales, la prohibición de la amenaza o el uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas. Lo anterior, también conlleva el respeto por los Derechos Humanos y las libertades fundamentales.

De igual manera, como se expone más adelante, Colombia considera que el comportamiento de los Estados en el marco de las TICs debe cumplir con las obligaciones, normas y principios del Derecho Internacional de los Derechos Humanos (DIDH) y del Derecho Internacional Humanitario (DIH), incluyendo las normas del Derecho Internacional Consuetudinario. También, implica que los Estados deben cumplir con otras normas del Derecho Internacional Consuetudinario aplicables, como por ejemplo, la responsabilidad de los Estados en el uso de las TICs.

Como se refleja en los Informes Periódicos Anuales del GTCA[2], el uso de las TICs en futuros conflictos interestatales es cada vez más probable, al igual que el continuo aumento de incidentes de uso malintencionado de las TICs por parte de agentes estatales y no estatales, incluidos grupos terroristas y criminales.

Así pues, es prioritario avanzar en el debate sobre la aplicación del Derecho Internacional Humanitario y de otras normas y principios pertinentes del Derecho Internacional Público, en relación con dichas actividades en el ciberespacio.

Además, el uso de las TICs de manera incompatible con las obligaciones que les asisten a los Estados en virtud del Derecho Internacional, y contraviniendo las medidas de fomento de la confianza, socava la paz y la seguridad internacionales, la confianza y la estabilidad entre los Estados.

Colombia actúa de manera coherente con y respeta las once normas voluntarias no vinculantes[3] aplicables en el contexto del ciberespacio, contribuyendo al logro de los propósitos del Derecho Internacional, reconociendo que tanto los regímenes voluntarios como los vinculantes son esenciales para fomentar un ciberespacio seguro y estable. Estas normas, aunque no tienen carácter obligatorio, constituyen un importante conjunto de compromisos dedicados al comportamiento responsable de los Estados, que complementan y confirman ciertas reglas del Derecho Internacional convencional o consuetudinario.

Asimismo, es importante destacar la necesidad de mejorar y perfeccionar la cooperación internacional en el ciberespacio guiada por el Derecho Internacional. Colombia entiende que el ciberespacio se erige como un bien común global - creado por el ser humano - gracias, entre otras cosas, a la prestación de asistencia técnica y la creación de capacidades, incluida la transferencia de tecnología.

3. Soberanía

En Colombia, el concepto de soberanía, entendida como independencia[4], es un elemento fundacional de sus relaciones exteriores, tal como lo señala la Constitución Política[5]. Colombia entiende que la soberanía conlleva una dimensión tanto interna como externa y que confiere derechos e impone deberes a los Estados en virtud del Derecho Internacional.

La Corte Constitucional de Colombia[6] ha afirmado que la evolución de la noción de soberanía no desvirtúa sus principios fundamentales. Al respecto, este Alto Tribunal ha destacado tres dimensiones clave: (i) la soberanía como independencia; (ii) el entendimiento de que contraer obligaciones internacionales no menoscaba la soberanía, y que ésta no puede invocarse para eludir obligaciones legalmente adquiridas; y (iii) el principio de inmediatez, según el cual el ejercicio de la soberanía está sujeto al Derecho Internacional sin interferencia de otros Estados. En este sentido, Colombia reconoce que la soberanía implica tanto derechos como deberes y es susceptible de violaciones que pueden constituir hechos ilícitos internacionales.

La soberanía de los Estados está consagrada en instrumentos internacionales y regionales de gran relevancia como la Carta de las Naciones Unidas, la Carta de la Organización de los Estados Americanos y el Acta Constitutiva de la Unión Africana, y ha sido reforzada por decisiones judiciales de instituciones como la Corte Internacional de Justicia, como piedra angular del Derecho Interno.

En tal virtud, Colombia coincide con la conclusión incluida en el informe del Grupo de Expertos Gubernamentales de las Naciones Unidas[7], en el sentido de que la soberanía y las normas y principios internacionales conexos son aplicables a la realización de actividades relacionadas con las TICs por parte de los Estados, así como también a la jurisdicción de estos sobre la infraestructura de las TICs dentro de su territorio.

Así, los Estados ejercen jurisdicción sobre la infraestructura de las TICs dentro de su territorio, entre otras cosas, estableciendo políticas y leyes que son inherentes a su función de Estados, así como también, disponiendo de los mecanismos necesarios para proteger la infraestructura de las TICs dentro de su territorio de las amenazas relacionadas con este ámbito.

No obstante lo anterior, Colombia reconoce las características especiales del ciberespacio y los retos particulares que se plantean en relación con la aplicación del principio de soberanía. Lo anterior, supone un desafío mayúsculo que radica en equilibrar la soberanía nacional con la cooperación y el respeto a las normas internacionales, especialmente en el ámbito cibernético, donde los intereses nacionales y globales a menudo entran en conflicto. Así, es necesario que los Estados desarrollen aún más sus consideraciones jurídicas sobre cómo se aplica la soberanía en el contexto cibernético, particularmente en instancias que involucran múltiples jurisdicciones y donde el componente territorial está ausente o es complejo.

4. Prohibición de Intervención

La obligación de no intervención, un principio del Derecho Internacional Consuetudinario, prohíbe a los Estados interferir de manera coercitiva en las funciones inherentes de otros Estados[8], incluyendo sus sistemas políticos, económicos o sociales y su política exterior.

Un acto, incluida una operación cibernética que afecte asuntos dentro del "domaine réservé"[9] de un Estado y sea de naturaleza coercitiva[10] puede violar el principio de no intervención[11].

De acuerdo con el principio de no intervención, los Estados no deben intervenir directa o indirectamente en los asuntos internos o externos de otro Estado, ni siquiera a través de las TICs. Tal sería el caso, por ejemplo, de la injerencia en los sistemas electorales de otro Estado, o de las actividades cibernéticas dirigidas a interferir en el funcionamiento de los sistemas de organismos o instituciones públicas de otro Estado.

5. Debida Diligencia

Derivado del principio de soberanía de los Estados, la obligación de debida diligencia ha sido reconocida por instancias como la Corte Internacional de Justicia en el caso del Canal de Corfú[12].

La debida diligencia impone a los Estados la obligación de no permitir, a sabiendas de que su territorio es utilizado para actos contrarios a los derechos de otros Estados, y asimismo los obliga tomar todas las medidas posibles para prevenir y mitigar las actividades que afecten los derechos de otros Estados y que les produzcan graves consecuencias adversas. Colombia considera que, con arreglo al Derecho Internacional, este deber también aplica en el ciberespacio.

En este sentido, Colombia invita a los Estados a tomar las medidas apropiadas para proteger sus infraestructuras críticas de las amenazas relacionadas con las TICs y para garantizar que su territorio no sea utilizado por actores no estatales para cometer actos ilícitos. Colombia también considera que los Estados deben fomentar la divulgación responsable de las vulnerabilidades de las TICs y tomar las medidas apropiadas dentro de sus jurisdicciones y a través de la cooperación internacional para garantizar la integridad de la cadena de suministro y para prevenir la proliferación de técnicas y herramientas TICs maliciosas o de funciones ocultas y dañinas.

Sin embargo, Colombia comparte la posición de que la obligación de debida diligencia requiere de un análisis profundo desde el punto de vista técnico, político y jurídico de las capacidades de los Estados.

6. Solución Pacífica de Controversias

Colombia considera que en el contexto de las TICs, los Estados Parte en toda controversia internacional que pueda poner en peligro el mantenimiento de la paz y la seguridad, o en caso de desacuerdos sobre la aplicación o interpretación del Derecho Internacional, deben buscar primero una solución por los medios pacíficos establecidos en el Artículo 33 de la Carta de las Naciones Unidas[13], a saber: negociación, investigación, mediación, conciliación, arbitraje, arreglo judicial, recurso a organizaciones o acuerdos regionales u otros medios pacíficos de su elección. Esta obligación no es absoluta y no excluye otras obligaciones o derechos jurídicos internacionales, como el derecho fundamental a la legítima defensa.

Lo anterior se basa en las obligaciones derivadas del Artículo 2(3) y del Capítulo VI de la Carta de las Naciones Unidas[14].

7. Derecho Internacional de los Derechos Humanos

El Derecho Internacional de los Derechos Humanos se aplica a las actividades en el ciberespacio. Las iniciativas estatales que se establezcan con el fin de garantizar la seguridad de las tecnologías de la información y las comunicaciones, así como todas las acciones en el ciberespacio, deben respetar los Derechos Humanos y las libertades fundamentales consagradas en instrumentos internacionales como el Pacto de Derechos Civiles y Políticos, el Pacto de Derechos Económicos, Sociales y Culturales, la Convención Americana sobre Derechos Humanos y la Declaración Universal de Derechos Humanos, y en el Derecho Internacional Consuetudinario.

Además de lo anterior, Colombia considera que para garantizar el uso seguro de las TICs, los Estados deben cumplir con las Resoluciones 20/8, 26/13 y 47/16 del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los Derechos Humanos en Internet, así como las Resoluciones 68/167, 69/166, 77/211 y7 5/176 de la Asamblea General sobre el derecho a la privacidad en la era digital, con el fin de garantizar el pleno respeto de los Derechos Humanos.

Además, dadas ciertas prácticas generalizadas, Colombia cree que es esencial reconocer los desafíos y vulnerabilidades únicas que enfrentan las mujeres y otros grupos marginados en línea en función de su orientación sexual, identidad y expresión de género, y características sexuales (SOGIESC por sus siglas en inglés)[15]. El reconocimiento de estos desafíos incluye abordar, por ejemplo, la violencia de género, el acoso digital y la brecha digital de género. Por lo tanto, la incorporación de una perspectiva con enfoque de género en todos los esfuerzos pertinentes garantiza que los marcos jurídicos internacionales sean inclusivos y equitativos, salvaguardando los derechos de todas las personas.

Cancillería

Colombia entiende que también es necesario reconocer los Derechos Humanos que a menudo se ven afectados como resultado de actividades cibernéticas, incluyendo, entre otros, el derecho a la privacidad y el derecho a la libertad de opinión y expresión.

8. 1.Derecho Internacional Humanitario

Dados los retos y realidades únicas que Colombia ha enfrentado a lo largo de su historia, el DIH se constituye en un área del Derecho Internacional de especial relevancia para nuestro país, considerando que su aplicación es crucial para garantizar la protección de los civiles y la regulación efectiva de los conflictos armados.

El DIH se aplica en situaciones de conflicto armado, ya sea de carácter internacional o no internacional y a todas las partes del conflicto[16]. En opinión de Colombia, el DIH y sus principios, en particular, humanidad, necesidad, proporcionalidad y distinción, se aplican al uso de las TICs por parte de los Estados en los conflictos armados.

Las infraestructuras civiles críticas que permiten la prestación de servicios esenciales dependen cada vez más de sistemas digitalizados. La preservación de dichas infraestructuras y servicios frente a operaciones cibernéticas o daños incidentales es vital para proteger a la población civil. Es necesario alcanzar un entendimiento común sobre qué acciones o conductas que involucran el uso de las TICs o son desarrolladas en el contexto del ciberespacio están prohibidas y cómo los civiles y los bienes civiles pueden ser protegidos de la mejor manera en tiempos de conflicto armado.

El DIH ofrece protección específica a determinadas infraestructuras y servicios, como, por ejemplo, los servicios médicos, las operaciones humanitarias, los bienes culturales, el medio ambiente, las obras e instalaciones que contienen fuerzas peligrosas y los bienes indispensables para la supervivencia de la población civil, independientemente del tipo de operación de que se trate.

8.1. Bienes Protegidos

La cuestión de lo que constituye un bien protegido en virtud del DIH es también de suma importancia. Las operaciones cibernéticas contra datos civiles pueden tener graves consecuencias para los civiles, que deben abordarse y debatirse en el marco del DIH. Sin embargo, Colombia considera que, en general, los datos de civiles están protegidos de las operaciones cibernéticas directas, a menos que, en el marco de la implementación de las normas de DIH, se conviertan en un objetivo militar legítimo.

8.2. Sobre el Concepto de Ataque

La definición de "ataque" es de central importancia para la aplicación del DIH. Los Estados deben continuar desarrollando sus consideraciones jurídicas para clarificar el alcance del concepto de "ataque" con arreglo al DIH, en el contexto cibernético.

Sin embargo, Colombia considera que, en el contexto del ciberespacio, el concepto de "ataque" del DIH debe entenderse tal y como se define en el artículo 49(1) del Protocolo Adicional I a los Convenios de Ginebra[17].

Actualmente es ampliamente aceptado que, en el contexto cibernético, la noción de "ataque" incluye las operaciones cibernéticas de las que se espera razonablemente que causen la muerte o lesiones a personas, o la destrucción o daños a bienes. No obstante lo anterior, las opiniones están divididas en cuanto a si las operaciones que sólo dan lugar a una pérdida de funcionalidad del sistema u del bien atacado, sin causar daños físicos, constituyen un ataque con arreglo al DIH. En este sentido, es necesario aclarar este punto (en términos de duración y naturaleza de la pérdida de funcionalidad causada) en el que una operación cibernética constituye un ataque.

Sin embargo, en términos de evaluar un "ataque" en el contexto del ciberespacio, Colombia actualmente identifica una operación cibernética como un "ataque" si se puede esperar razonablemente que cause lesiones o la muerte a personas, o daño o destrucción de bienes, incluyendo aquellos que generen pérdida de funcionalidad sin daño físico directo.

Adicionalmente, en opinión de Colombia, a efectos de analizar el alcance del concepto de "ataque", las operaciones cibernéticas pueden dañar bienes al menos de dos maneras. En primer lugar, pueden afectar la prestación de servicios a la población civil, por ejemplo, en casos de operaciones cibernéticas contra redes eléctricas y el sector salud o dirigidas a interrumpir la logística involucrada en el transporte y entrega de ayuda humanitaria. En segundo lugar, pueden causar daños físicos a la propia infraestructura.

8.3. Protección y Participación de Civiles

Colombia considera que es necesario tener en cuenta todas las normas existentes del DIH, incluyendo los principios de necesidad militar y humanidad, y todas las demás medidas necesarias para proteger a la población civil.

En este sentido, es importante analizar los impactos específicos que las operaciones cibernéticas pueden tener sobre personas en situación vulnerable, como los niños, niñas y adolescentes, las mujeres y la comunidad LGBTQ+/SOGIESC, entre otros, bajo las normas aplicables del DIH.

Sin perjuicio de lo anterior, también es necesario llevar a cabo un análisis jurídico detallado acerca de las implicaciones de la participación de civiles en la planificación y ejecución de actividades o de las operaciones cibernéticas, para encontrar entendimientos comunes de cuándo su conducta podría equivaler a una participación directa en las hostilidades.

8.4. Precaución

De conformidad con las normas del DIH, tanto la planificación como la ejecución de operaciones cibernéticas lícitas deben llevarse a cabo respetando el principio de precaución[18] para evitar y, en cualquier caso, reducir al mínimo la pérdida incidental de vidas de civiles, las lesiones a civiles o los daños a bienes de carácter civil.

9. Amenaza o Uso de la Fuerza

En su uso de las TICs, y de conformidad con el párrafo 4 del Artículo 2 de la Carta de las Naciones Unidas[19], los Estados se abstendrán, en sus relaciones internacionales, de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas.

La posición de Colombia es que ciertas operaciones cibernéticas podrían equivaler a una amenaza o al uso de la fuerza. Sin embargo, varias cuestiones sobre este tema siguen abiertas a análisis y deben ser abordadas con mayor profundidad por los Estados, en particular las relacionadas con el umbral de lo que constituye fuerza en el ciberespacio.

10. Responsabilidad de los Estados

Los hechos internacionalmente ilícitos cometidos por un Estado, de acuerdo con los criterios del Derecho Internacional Consuetudinario sobre Responsabilidad del Estado reflejados en los Artículos sobre la Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (ARSIWA por sus siglas en inglés) de la Comisión de Derecho Internacional, se entienden como aquellas acciones u omisiones atribuibles a un Estado en virtud del Derecho Internacional y que constituyen una violación de una obligación internacional del Estado.

Por lo tanto, Colombia considera que los hechos internacionalmente ilícitos cometidos en el contexto del ciberespacio o por medio de las TICs por parte de un Estado contra otro(s) Estado(s), por acción u omisión, comprometen su responsabilidad internacional. Sin embargo, Colombia reconoce que, en la práctica, invocar la responsabilidad de un Estado por un hecho internacionalmente ilícito, implica complejas consideraciones técnicas, jurídicas y políticas[20]

11. Atribución

Colombia considera que el principio de responsabilidad del Estado se aplica en el contexto de las operaciones cibernéticas y, por lo tanto, los Estados pueden ser internacionalmente responsables si cualquier órgano del Estado, o cualquier persona o entidad con competencia legal para ejercer autoridad en nombre del Estado, o cualquier persona o entidad que actúe bajo instrucciones, dirección o control de una autoridad del Estado, ha llevado a cabo operaciones cibernéticas en violación de las obligaciones internacionales del Estado.

Colombia es consciente de que las limitaciones desde el punto de vista tecnológico son desafiantes, dado que estas actividades a menudo son realizadas por terceros (proxies o actores no estatales), lo que puede dificultar la atribución de responsabilidad a un Estado determinado.

A pesar de la dificultad inherente en materia de atribución y en consecuencia, a la determinación de la responsabilidad internacional de los Estados en caso de una operación cibernética, el Estado que se considere afectado, antes de proceder a la adopción de contramedidas, debería llevar a cabo todas las acciones necesarias para identificar el origen de la actividad cibernética, antes de atribuir la responsabilidad a un Estado, de conformidad con los estándares de prueba y mecanismos de cooperación internacional para la atribución de ataques.

12. Respuestas del Estado y Circunstancias que Excluyen la Ilicitud

Los Estados pueden reaccionar ante actividades u operaciones cibernéticas llevadas a cabo por otro Estado mediante acciones que, de otro modo, serían contrarias a sus obligaciones internacionales, pero cuya ilicitud queda excluida a la luz del Derecho Internacional en consideración a circunstancias específicas.

Lo anterior, se entiende sin perjuicio de la necesidad de buscar inicialmente una solución de conformidad con los principios y normas establecidos del Derecho Internacional. Incluso cuando pueda haber motivos suficientes para atribuir la responsabilidad a un Estado, se invita al Estado afectado a que, en primer lugar, entable un diálogo directo con el Estado presuntamente responsable o, si procede, se valga de un tercer Estado para facilitar esas conversaciones, en consonancia con los principios de negociación, mediación y solución pacífica prescritos en la Carta de las Naciones Unidas.

12.1. Legítima Defensa

Un Estado que sea blanco de una actividad u operación cibernética que equivalga a un ataque armado puede invocar su derecho inherente de legítima defensa, de conformidad con el derecho consuetudinario a la legítima defensa, tal como se describe en el Artículo 51 de la Carta de las Naciones Unidas[21] y como se refleja en el Artículo 21 de la ARSIWA[22].

Colombia considera que, al ejercer el derecho a la legítima defensa en respuesta a una actividad u operación cibernética que equivalga a un ataque armado, los Estados deben respetar los umbrales y las limitaciones establecidas en el Artículo 51 de la Carta de las Naciones Unidas.

12.2. Contramedidas

De conformidad con los principios del Derecho internacional, en caso de que un Estado sea declarado responsable de una operación cibernética que constituya un hecho internacionalmente ilícito, el Estado afectado tiene derecho a adoptar contramedidas[23] para garantizar el cese o la reparación de la conducta ilícita del primero. Estas contramedidas deben ser proporcionales al daño sufrido y pueden adoptarse en el contexto del ciberespacio o fuera de él.

En caso de incumplimiento de las obligaciones erga omnes, los Estados distintos del Estado perjudicado también podrán tomar contramedidas contra el Estado responsable de la operación cibernética.

12.3. Retorsión

Los Estados pueden responder a actos inamistosos o ilícitos llevados a cabo por otros Estados en el contexto del ciberespacio, adoptando medidas conocidas como retorsiones. Estas acciones, aunque potencialmente percibidas como inamistosas, no violan el Derecho Internacional. Ejemplos de retorsiones incluyen la ruptura o limitación de relaciones diplomáticas y la imposición de restricciones comerciales.

La retorsión también puede incluir acciones cibernéticas específicas, como la emisión de advertencias a operaciones cibernéticas de otro Estado.

13.Nuevos Desarrollos

En el ciberespacio, cada día se producen nuevos avances y, por lo tanto, los requisitos para los Estados en relación con su aplicación del Derecho Internacional siguen evolucionando. Por ejemplo, la aparición de Embajadas “virtuales”, “digitales” o de “datos”, implica la necesidad de que los Estados acuerden las circunstancias específicas en las que se les aplica la inmunidad diplomática internacional.

14. Observaciones Finales

Este documento de posición nacional resalta la visión actual de la República de Colombia sobre la aplicación del Derecho Internacional al uso de las TICs por parte de los Estados. Dada la amplitud del Derecho Internacional, sólo se cubren algunos aspectos sobresalientes, particularmente aquellos de relevancia específica para nuestro país por su historia, contexto y otros factores claves, donde Colombia cuenta con mayores elementos para desarrollar su posición en este momento.

Colombia continúa analizando este tema y seguirá aportando mayores elementos de juicio sobre la aplicación del Derecho Internacional al ciberespacio, incluso mediante la publicación de secciones dedicadas a temas específicos o el desarrollo de ejemplos concretos.

Por último, Colombia considera que cualquier ambigüedad sobre la forma en que se aplica el Derecho Internacional en el contexto cibernético debe abordarse a través del diálogo internacional y la cooperación que involucre los esfuerzos combinados de los Estados, las Organizaciones Internacionales, la sociedad civil y la academia.

***

NOTAS AL PIE

[1] En preparación de este documento de posición nacional, la República de Colombia analizó diversas Fuentes, incluyendo, entre otros, los trabajos del anterior y del actual Grupo de Trabajo de Composición Abierta sobre la Seguridad y en el Uso de las Tecnologías de la Información (GTCA) de las Naciones Unidas y del extinto Grupo de Expertos Gubernamentalespara el Avance del Comportamiento Responsable de los Estados en el Contexto del Ciberespacio, así como también el Manual de Tallin y el Toolkit de Derecho Cibernético.
[2] Para. 13 del Informe Periódico de 2024
[3] Normas de las Naciones Unidas para el Comportamiento Responsable de los Estados en el Ciberespacio.
[4] Caso "Isla de Palmas" (Países Bajos. vs. Estados Unidos), 2 RIAA 829, 838 (Corte Permanente de Arbitraje 1928).
[5] Artículo 9. Constitución Política de Colombia.
[6] Sentencia C-621/01 de la Corte Constitucional de Colombia del 13 de junio de 2001
[7] Informe Final del GIG. 2013.
[8] Asuntos internos o externos de los otros Estados
[9] Áreas en las que el Estado es libre de decidir, como las elecciones nacionales o la política exterior.
[10] La coerción puede entenderse de dos maneras: como un acto destinado a obligar a un Estado a cambiar su comportamiento o como un acto que priva a un Estado de su control sobre estas cuestiones. Mientras que las intervenciones militares son casos claros de coerción, la injerencia no forzosa, como la coerción económica o política, es más compleja y depende del contexto, y a menudo se citan como ejemplo las operaciones cibernéticas.
[11] Este principio fue esbozado por la Corte Internacional de Justicia en el caso Nicaragua vs. Estados Unidos de 1986.
[12] Sentencia de la Corte Internacional de Justicia. Gran Bretaña vs Albania. 1949.toridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales."

NOTAS AL PIE

[13] Artículo 33 de la Carta de las Naciones Unidas:
1.“Las partes en una controversia cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales tratarán de buscarle solución, ante todo, mediante la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección.
2.El Consejo de Seguridad, si lo estimare necesario, instará a las partes a que arreglen sus controversias por dichos medios.”
[14] Artículo 2(3) de la Carta de las Naciones Unidas:
“Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios:
(3) Los Miembros de la Organización arreglarán sus controversias internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia.”
[15] En inglés: SOGIESC es un acrónimo para: Sexual Orientation, Gender Identity and Expression, and Sex Characteristics.
[16] Opinión Consultiva sobre la Legalidad de la Amenaza o el Uso de las Armas Nucleares. Informes de la CIJ. 1996. Par. 86 “a todas las formas de guerra y a todo tipo de armas, las del pasado, las del presente y las del futuro”
[17] Artículo 49 (1) del Protocolo Adicional I a los Convenios de Ginebra:
“Artículo 49 - Definición de ataques y ámbito de aplicación:
(1) Se entiende por ataques los actos de violencia contra el adversario, sean ofensivos o defensivos”.
[18] De conformidad con el Artículo 57 del Protocolo Adicional I de los Convenios de Ginebra.

NOTAS AL PIE

[19] Artículo 2(4) de la Carta de las Naciones Unidas:
"Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios:
(4)Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas."
[20] (GGE 2021)
[21] Artículo 51. Carta de las Naciones Unidas:
"Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales."
[22] Artículo 21. Proyecto de Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos de la Comisión de Derecho Internacional de las Naciones Unidas:
"La ilicitud del hecho de un Estado queda excluida si ese hecho constituye una medida lícita de legítima defensa tomada de conformidad con la Carta de las Naciones Unidas."
[23] Colombia entiende las contramedidas como aquellas medidas que, de otra forma, serían contrarias a las obligaciones internacionales de los Estados, tomadas por un Estado afectado, en respuesta a un hecho internacionalmente ilícito, para procurar la cesación y la reparación por parte del Estado responsable. (Art. 22 ARSIWA)

Cancillería

BIBLIOGRAFÍA

- Acta de Constitución de la Unión Africana de Naciones.
- Carta de la Organización de los Estados Americanos
- Carta de la Organización de las Naciones Unidas
- Comisión de Derecho Internacional. Artículos de la sobre la Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos (2001).
- Constitución Política de Colombia. (1991).
- Corte Constitucional de Colombia. Sentencia número C-621/01. (2001).
- Corte Internacional de Justicia. Caso Canal de Corfú (Reino Unido vs. Albania). 1984
- Corte Internacional de Justicia. Sentencia del caso de Nicaragua vs. Estados Unidos. (1986).
- Corte Internacional de Justicia. Opinión Consultiva sobre la Legalidad de la Amenaza o Uso de Armas Nucleares (1996).
- Corte Permanente de Arbitraje. Sentencia de Isla de Palmas (Países Bajos vs. Estados Unidos) (1928).
- Cyber Law Toolkit https://cyberlaw.ccdcoe.org/wiki/Main_Page
- Grupo de Expertos Gubernamentales de las Naciones Unidas. Informe Final (2021).
- Grupo de Trabajo de Composición Abierta. Informe Final (2022)
- Instituto de Oxford para la Ética, el Derecho y los Conflictos Armados
- Manual de Tallin sobre el Derecho Internacional Aplicable a la Guerra Cibernética (2013)
- Organización de las Naciones Unidas. Asamblea General. Resoluciones 68/167, 69/166, 77/211, 7 5/176, 75-240
- Organización de las Naciones Unidas. Consejo de Derechos Humanos. Resoluciones 20/8, 26/13, 47/16
- Protocolo I Adicional a los Convenios de Ginebra

***

Cancillería