La necesidad de complementar la definición de acto de agresión, ¿forzados a una definición insuficiente ante ciberataques en la guerra moderna?

The Need to Complement the Definition of Act of Aggression: Forced into an Insufficient Definition in the Face of Cyberattacks in Modern Warfare?

A necessidade de complementar a definição de ato de agressão: forçados a uma definição insuficiente diante dos ciberataques na guerra moderna?

Daniela Velásquez Aponte*

Fecha de recepción: *28 de febrero de 2025*
Fecha de aprobación: *5 de mayo de 2025*
Doi: *https://doi.org/10.12804/revistas.urosario.edu.co/anidip/a.15860*

Para citar este artículo: Velásquez Aponte, D. (2025). La necesidad de complementar la definición de acto de agresión, ¿forzados a una definición insuficiente ante ciberataques en la guerra moderna? *Anuario Iberoamericano de Derecho Internacional Penal (ANIDIP), 13*, 1-24. https://doi.org/10.12804/revistas.urosario.edu.co/anidip/a.15860

Resumen

Este artículo examina cómo la definición de "acto de agresión" establecida en la Resolución 3314 de 1974 de la Asamblea General de la ONU resulta insuficiente frente a las nuevas formas de violencia interestatal impulsadas por tecnologías digitales. Parte de la idea de que ciertos ciberataques deberían considerarse actos de agresión según el derecho internacional, ya que impactan directamente la infraestructura crítica y la soberanía de los Estados. El análisis combina enfoques dogmáticos, normativos y doctrinales para proponer un literal hipotético de esta como enmienda de adición a la definición de agresión contenida en el artículo 3º de la Resolución

* Abogada y especialista en Derecho Internacional, Universidad del Rosario (Colombia). Correo electrónico: danielavelasquez9986@outlook.com. ORCID:

3314. Además, se discuten los retos teóricos relacionados con la atribución estatal y la forma en que se materializa el daño en el ámbito cibernético.

Palabras clave: ciberoperaciones; ciberataques; acto de agresión; Resolución 3314 de 1974; definición.

Abstract

This article examines how the definition of "act of aggression" established in UN General Assembly Resolution 3314 of 1974 is insufficient in the face of new forms of interstate violence driven by digital technologies. It starts with the idea that certain cyberattacks should be considered acts of aggression under international law, as they directly impact critical infrastructure and the sovereignty of States. The analysis combines dogmatic, normative, and doctrinal approaches to propose a hypothetical provision as an amendment to the definition of aggression contained in article 3 of Resolution. In addition, it discusses the theoretical challenges related to state attribution and the way in which damage materializes in the cyber realm.

Keywords: Cyberoperations; cyberattacks; act of aggression; Resolution 3314 of 1974; definition.

Resumo

Este artigo examina como a definição de "ato de agressão" estabelecida na Resolução 3314 de 1974 da Assembleia Geral das Nações Unidas é insuficiente diante das novas formas de violência interestatal impulsionadas pelas tecnologias digitais. Parte da ideia de que certos ciberataques devem ser considerados atos de agressão nos termos do direito internacional, uma vez que afetam diretamente infraestruturas críticas e a soberania dos Estados. A análise combina abordagens dogmáticas, normativas e doutrinárias para propor uma disposição hipotética como emenda à definição de agressão contida no artigo 3º da Resolução. Além disso, analisa os desafios teóricos relacionados à atribuição estatal e à forma como os danos se materializam no ciberespaço.

Palavras-chave: operações cibernéticas; ciberataques; ato de agressão; Resolução 3314 de 1974; definição.

Introducción

La definición de agresión dada en la Resolución 3314 de 1974 de la Asamblea General contiene todos los elementos necesarios para establecer qué operaciones militares constituyen un acto de agresión según el derecho internacional. Sobra decir que esta definición juega un rol importante para poder identificar y calificar la conducta de los Estados ante un conflicto internacional.

El artículo 3º de dicha resolución provee una lista de conductas que constituyen un acto de agresión que da lugar a responsabilidad internacional por hacer uso indebido de la fuerza. Esta lista, como menciona el artículo 4º, no es exhaustiva, y será potestad del Consejo de Seguridad determinar si hay otras conductas no incluidas en el artículo 3º que también se consideren actos de agresión.

A pesar de la gran utilidad que ha implicado la existencia de estas disposiciones, el Consejo de Seguridad no ha dado un mandato claro, derivado del artículo 4º, que busque incluir el uso de las nuevas tecnologías como nuevas formas de agresión, basándose en la comparabilidad o escala que puedan tener las ciberoperaciones con formas de agresión tradicionales.

La pertinencia de hacer este estudio radica en que los ciberataques pueden efectivamente afectar la soberanía estatal, la paz y la seguridad internacionales, sin contar aún con normatividad adecuada. Este vacío regulatorio ha sido señalado desde la doctrina; por ejemplo, Ávila García (2024) sostiene que "[e]l principal desafío futuro radica en la creación de un marco jurídico internacional más robusto que regule las actividades cibernéticas, tanto en tiempos de paz como de conflicto" (p. 119).

La hipótesis de este texto consiste en que resulta necesario avanzar en la redacción de alguna disposición en ese sentido, teniendo en cuenta que las ciberoperaciones han jugado un papel importante como métodos de ataque en los conflictos modernos, para así responder oportunamente a las nuevas amenazas a la paz y seguridad internacionales.

Así las cosas, a través de un análisis de fuentes primarias como tratados, resoluciones y pronunciamientos de órganos de la Organización de las Naciones Unidas (ONU), doctrina especializada y análisis comparado de ciberataques recientes, este texto expondrá, en primer lugar, las razones que respaldan la necesidad de dar la clasificación de acto de agresión a los ciberataques adelantados por Estados; enseguida, se identificarán las formas más comunes de llevar a cabo los ciberataques; y cerrará con la propuesta de enmienda hipotética, de tal modo que se abarquen de la mejor manera posible los hechos con la propuesta de definición.

1. La necesidad de la inclusión de ciberataque como forma de agresión

Los elementos que se pueden resaltar de los ataques cibernéticos llevados a cabo por Estados son: i) no son fácilmente atribuibles a un autor; ii) tienen la capacidad de generar un daño; iii) violan la soberanía estatal; iv) están desprovistos de consecuencias claras; y v) no cuentan con posibles rutas de acción proporcional que vaya acorde con la Carta de las Naciones Unidas, que es el recurso normativo más fácilmente aplicable a la mayoría de los Estados. Aunado a esto, se ha considerado aplicable la legítima defensa ante estos ataques, asunto importante porque denota que hay un acto que amerita recibir el trato que se le daría a un acto de agresión 'tradicional'.

Como complemento, Kai Ambos (Tsagourias *et al.,* 2017, pp. 120-121) indica otros elementos para tener en cuenta sobre estos ataques. El doctrinante sostiene que, a diferencia del ciberespionaje, con un ciberataque no se busca solo obtener información. A su vez, un ciberataque tampoco es un simple crimen cibernético, porque no busca ganancias económicas. A esto se puede agregar que tampoco se debe confundir con el ciberterrorismo, que tiene objetivos políticos o religiosos como móvil (Lazar & Costescu, 2018, p. 161). Kai Ambos se refiere a estas diferencias entre distintos ataques a redes informáticas (ARI) de la siguiente manera:

> La razón de este enfoque en las ARI es que sólo estas formas de ataques son normalmente lo suficientemente graves como para calificarse de crímenes internacionales y, por tanto, estar cubiertos por una jurisdicción penal internacional como la Corte Penal Internacional (CPI). Sin embargo, el significado exacto de una ARI sigue siendo objeto de debate. Según la opinión mayoritaria, pueden distinguirse tres elementos. En primer lugar, un ARI no se lleva a cabo con fines de lucro o beneficio financiero (directo) como los ciberdelitos económicos clásicos. En segundo lugar, el ataque no se lleva a cabo con el fin de obtener información ("ciberespionaje"). En tercer lugar, un ARI altera, interrumpe, degrada o destruye una red informática y puede provocar la interrupción de los dispositivos conectados a la red atacada. Este último elemento queda bien recogido en la definición que ofrece mi *Manual de Tallin* sobre ciberguerra: "Una operación cibernética, ofensiva o defensiva, de la que se espera razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos [...]" (Tsagourias *et al.,* 2017, pp. 120-121).

Para ilustrar el debate, podemos recurrir a Detlev Wolter, 1 de los 15 expertos del Grupo de Expertos Gubernamentales (GEG) de la ONU, entre 2012 y 2013, sobre información y telecomunicaciones en el contexto de la seguridad internacional, quien comenta que la cooperación para determinar normas aplicables es necesaria y que es aplicable la figura de legítima defensa frente a ciberataques, lo que da a estos la connotación de acto de agresión.

No obstante, como nota aparte, la legítima defensa, como siempre, encuentra límites al momento de ser invocada: si no hay atribución clara a otro Estado, no hay forma de defenderse de lo desconocido, por lo que la figura de la legítima defensa se desdibuja, pues pierde al menos el elemento de la inmediatez. Así mismo, puede que los efectos del ataque se manifiesten de forma diferida en el tiempo o de forma no inmediata, lo que dificulta seriamente el uso de la legítima defensa a la que podría acudir un Estado bajo un ataque de distinta naturaleza (Pérez, 2021).

El primer caso de alta cobertura considerado como un ciberataque fue Stuxnet, ocurrido en Irán en 2010, a través de un virus insertado con una USB y varias impresoras en los sistemas operativos de la planta nuclear de Natanz. Este virus atacó específicamente a las centrifugadoras de enriquecimiento de uranio y les daba la orden de autodestruirse. Dado que la planta no tenía las dimensiones ni condiciones para generar un derrame nuclear, no hubo daños en la computadora central, ni un derrame nuclear (*BBC News Mundo,* 2015), pero sí constituyó una clara violación a la soberanía estatal, a la seguridad nacional, un sabotaje al programa armamentístico o energético que Irán estaba desarrollando, daños a la infraestructura de la planta y un retraso de casi dos años al programa nuclear iraní. La responsabilidad de este ataque se le atribuyó sin confirmación formal a Estados Unidos y a Israel, los cuales, en junio de 2025, bombardearon tres complejos nucleares de Irán: Fordo, Isfahán y Natanz (BBC Verify & Equipo de Periodismo Visual, 2025).

Aunque en el texto de Lazar y Costescu de 2018 se habla de dos formas de interpretar el caso Stuxnet, hay un elemento que no se puede ignorar si se observa bajo la óptica del derecho internacional humanitario (DIH): el virus se instaló en una central nuclear para sabotear las centrífugas de enriquecimiento de uranio. Esto sugiere que no fue un mero acto de ciberterrorismo para intimidar al gobierno iraní, sino un acto que hubiera podido terminar en el escalamiento de la situación hasta generar un conflicto, de no ser porque era imposible identificar inmediatamente al atacante, cosa que sigue sin poderse hacer, lo que dificultó una respuesta inmediata.

En ese sentido, sí se han llevado a cabo estudios sobre la procedibilidad de la legítima defensa en escenarios en los que los ciberataques tengan la magnitud correspondiente, siempre teniendo en cuenta que, si se llegara a justificar el uso de la fuerza, tendría que ser proporcional y bajo lo dispuesto en el artículo 51 de la Carta de las Naciones Unidas (Gutiérrez Espada & Cervell Hortal, 2012, cap. 10).

Estas discusiones sobre la legítima defensa muestran que la comunidad internacional efectivamente reconoce los ataques cibernéticos como potenciales actos de agresión y potenciales amenaza a la paz internacional, aplicando los instrumentos internacionales tradicionales, como la Carta de las Naciones Unidas, el *Manual de Tallin 2.0,* la figura de la legítima defensa e, incluso, el Proyecto de Artículos sobre Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos.

A pesar de que el anonimato puede implicar un obstáculo para una posible defensa dentro de la proporcionalidad y la inmediatez, también se debe ver como un agravante a la conducta. Cuando un Estado adelanta un ataque armado, la evidencia de que las armas o las fuerzas militares pertenecen a ese Estado no demora en dilucidar; sin embargo, en el caso de los ciberataques, la proveniencia desconocida y clandestina genera mayor impunidad y aumenta la necesidad de regulación.

Como si lo anterior no demostrara que sí hay una suerte de consenso sobre identificar lo que sucede en el ciberespacio y la guerra con todo lo que eso implica. El *Manual de Tallin* puede ser el mejor ejemplo de esto. El *Manual de Tallin* fue creado por el Centro de Excelencia de Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN), publicado en 2013, surgió de ajustar la aplicación del *ius ad bellum* y del *ius in bello* de forma no vinculante.

El manual hace un trabajo muy importante al establecer esas relaciones para la forma de aplicar las normas existentes de la guerra a una nueva forma de guerra. Identifica como primer elemento por tratar dentro de sus reglas la soberanía de los Estados, y señala que, aunque ningún Estado puede reclamar la soberanía sobre el ciberespacio *per se,* los Estados pueden ejercer prerrogativas soberanas sobre cualquier infraestructura cibernética situada en su territorio, así como sobre las actividades asociadas a dicha infraestructura cibernética (Schmitt, 2012, p. 11).

Esta sección encapsula los elementos más importantes sobre por qué se puede hablar de afectación a la soberanía en el ciberespacio, que es el punto de partida para poder pensar en agresión entre Estados. Esta forma de determinar la soberanía de los Estados sobre el ciberespacio es la que abre la puerta a que se pueda hacer todo lo que sea necesario para estudiar un ataque como jurisdicción, responsabilidad estatal, uso de la fuerza, legítima defensa, metodología de los ataques y todo lo que se ha concebido en torno a los conflictos armados entre Estados.

La regla 30 del *Manual de Tallin* define "un ciberataque [como] una operación cibernética, ofensiva o defensiva, de la que cabe esperar razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos".

La mención de la expectativa de que esa operación, como acto que inicia una guerra, o como un instrumento empleado dentro del conflicto ya iniciado, afecte la integridad de la población o destruya objetos es una nueva puerta para hablar de derecho internacional humanitario. Ya condicionado por lo considerado sobre la soberanía, indica que sí se entiende que existe un ataque en el sentido estricto de la palabra, pero, además, que ese ataque debe respetar los Convenios de Ginebra de 1949 y sus protocolos, lo cual nos ubica directamente en un campo nuevo pero indiscutible de conflicto armado internacional entre Estados.

Entender de esta manera la soberanía en el ciberespacio es la piedra angular que da paso al resto de la discusión para así comprender que esa soberanía, si se ve afectada por un ataque cibernético organizado, dirigido o bajo el comando de otro Estado, ha sufrido efectivamente de un ataque.

> Para el CICR, durante un conflicto armado, una operación diseñada para desactivar una computadora o una red informática constituye un ataque según el DIH, ya sea por medios cinéticos o cibernéticos. Si se interpreta que la noción de ataque hace referencia únicamente a las operaciones que provocan muertes, heridas o daño físico, entonces una ciberoperación que tiene como objetivo interrumpir el funcionamiento de una red civil (como una red eléctrica, bancaria o de comunicación) o que se prevé que provocará ese efecto de manera incidental puede no estar contemplada por las normas esenciales del DIH que protegen a la población civil y a los bienes de carácter civil. Sería difícil conciliar una interpretación tan excesivamente restrictiva del concepto de ataque con el objeto y fin de las normas del DIH sobre la conducción de las hostilidades. Para lograr la protección adecuada de la población civil contra los efectos de las ciberoperaciones, es esencial que los Estados coincidan en su definición de ataque (CICR, 2019, p. 9).

Siendo el CICR el comité que tiene como función promover el respeto al derecho internacional humanitario y revisar de qué forma se están adelantando las hostilidades para aplicarlo, es esencial tener en cuenta que coincide en que los Estados deben revisar la definición de ataque, pues la visión actual es muy restrictiva.

En efecto, la escurridiza naturaleza de los perpetradores de ciberataques y de la ejecución misma de estos ha contribuido a la imposibilidad de reaccionar en debida forma a los ataques que ya han ocurrido. Desde que Wolter hizo ese comentario de su experiencia en el GEG no se ha elaborado un tratado ni se ha codificado qué normativa internacional es aplicable a estas potenciales agresiones (Lazar & Costescu, 2018); no obstante, los ciberataques se han seguido generando. La teoría de la gobernanza global de Zürn (Wibowo, 2022) sería el mecanismo ideal para diseñar normas que puedan aplicarse del modo más amplio posible a través de la cooperación internacional consensuada.

El 11 de julio de 2025 se dio una actualización relevante al respecto: el Grupo de Trabajo de Composición Abierta sobre la Seguridad y el Uso de las Tecnologías de la Información y las Comunicaciones presentó su borrador final para establecer un mecanismo global que establece parámetros de buen comportamiento de los Estados en cuanto a su uso de las tecnologías de la información y comunicación (TIC). En este documento se recalcó que el uso de la fuerza está proscrito (num. 41, lit. c) y que se debe seguir determinando cómo el derecho internacional es aplicable a las TIC, que

> [l]as conductas que utilizan las TIC y que no constituyen una violación de la prohibición del uso o la amenaza del uso de la fuerza pueden, dependiendo de las circunstancias, ser contrarias a otros principios del derecho internacional, como la soberanía de los Estados o la prohibición de intervenir en los asuntos internos o externos de los Estados (Grupo de Trabajo de Composición Abierta sobre la Seguridad y el Uso de las Tecnologías de la Información y las Comunicaciones 2021-2025, 2025) (traducción propia).

A pesar de este último reporte, no se llega aún al llamado mecanismo global que propone el grupo. Se dieron bases y llegaron a consensos, pero realmente no hay aproximaciones materiales a siquiera un código de conducta o un instrumento similar para este tipo de operaciones en el ciberespacio.

Todas estas aproximaciones dan una señal inequívoca de que los ciberataques sí son vistos como potenciales actos de agresión cuando tienen elementos en común con lo que se entiende como agresión dentro de la Resolución 3314, por lo que es pertinente tratarlos como tal, clara y oportunamente.

2. Tipos de manifestación de ciberataques

Como ya hemos visto y como bien reconoce el Comité Internacional de la Cruz Roja (CICR), los ataques cibernéticos pueden generar heridas y muertes, o daños tanto a objetivos militares como a bienes civiles. Ante esto, el CICR se ha enfocado en el estudio de la aplicación del DIH a los ciberataques bajo el entendido de que esas conductas sí pueden constituir un acto de agresión o como métodos o medios de guerra, también conocida como *cyberwarfare,* en el contexto de un conflicto armado.

El CICR se pronunció de la siguiente forma en 2019: "En los casos no previstos por las normas vigentes del DIH, las personas civiles y los combatientes están protegidos por la llamada cláusula Martens, que establece que estos quedan bajo la protección y el imperio de los principios del derecho internacional derivados de la costumbre, de los principios de humanidad y de los dictados de la conciencia pública" (p. 5).

Además de ello, especifica que el DIH es aplicable a los conflictos futuros y presentes, por lo que, si se dan los elementos de un acto de agresión a través de ciberoperaciones, es indistinto, pues el daño real o potencial es el mismo. La Corte Internacional de Justicia se pronunció mediante opinión consultiva en 1996 acerca de la aplicación del DIH con respecto a armas nucleares y afirmó que los principios de DIH son aplicables a "todas las formas de guerra y todos los tipos de armas", incluso "las del futuro".

A efectos de este trabajo, los ciberataques que pueden generar efectos similares al uso de la fuerza tradicional se clasifican en tres grandes categorías según su intensidad y el tipo de objetivo: i) operaciones de denegación de servicio, ii) intrusiones en sistemas de información y iii) manipulación de infraestructuras críticas. Estas tipologías son propuestas a partir de la doctrina especializada y de casos reportados en conflictos recientes, con el fin de distinguir lo que constituye un mero cibercrimen de un posible acto de agresión estatal en los términos del derecho internacional.

Así las cosas, se han identificado las siguientes posibles materializaciones de ataques cibernéticos:

2.1. Ataques de denegación de servicio (DDoS)

Los ataques de denegación de servicio o DDoS han sido usados al menos desde 2013 para sobrecargar el tráfico orgánico de un servidor o de una red para impedir su funcionamiento normal. IBM los ha detectado cuando han afectado diferentes servidores. Por ejemplo, para hacer fallar micrositios de ventas; para interrumpir las funciones de servidores, como fue el caso de Amazon Web Services en 2020; o

para generar crisis financieras sobrecargando y desconectando servicios bancarios, impidiendo el acceso a cuentas o afectando las especulaciones en las bolsas de valores.

Estos ataques se lanzan al emitir solicitudes falsas que requieren de todo el ancho de la banda para ser atendidos, impidiendo el acceso de usuarios reales.

Este tipo de operaciones corresponde por lo general a un cibercrimen o a un acto de ciberterrorismo, que usualmente tiene motivos políticos o intereses económicos, lo que los dejaría por fuera del enfoque de este artículo (Lazar & Costescu, 2018, pp. 160-163). Sin embargo, dado que pueden adelantarse dentro de un conflicto armado, bajo órdenes de un Estado y dirigidos contra otro, pueden generar daños que tomen relevancia ante el DIH y a la luz de la responsabilidad de los Estados, ya que según su escala y alcance pueden constituir un acto de agresión.

2.2. Intrusiones en sistemas de información

Estas operaciones incluyen, pero no se limitan a, acceder sin autorización a bases de datos y redes de información con el fin de robar, alterar o destruir información. Las intrusiones se relacionan de una forma más clara con una configuración de ataque dentro de un conflicto armado por la intención que acarrea.

Durante el desarrollo de un conflicto armado la confidencialidad y reserva de la información estatal o militar es especialmente importante. Dado que los sistemas de almacenamiento de bases de datos y de elaboración de documentos se han trasladado definitiva y masivamente a sistemas virtuales, estos se encuentran vulnerables a las intrusiones y con mayor razón serán objetivo de intrusión durante un conflicto.

En el conflicto aún vigente entre Rusia y Ucrania, la BBC reportó: "[En] redes sociales ucranianas y rusas se pueden ver pruebas de aparentes ataques con drones a civiles, seis de los cuales fueron examinados por BBC Verify". Aunque es verdad que estos actos de civiles no son adelantados con violencia, sí contribuyen al esfuerzo general de guerra de Ucrania si esa información llega y alerta a las fuerzas armadas ucranianas y aporta a exponer las violaciones al DIH por parte de Rusia. De acuerdo con Schmitt (2012), la tecnología y la asimetría de la guerra hacen más complicada la identificación de participaciones directas e indirectas en conflictos contemporáneos. La tecnología en este conflicto también se ha usado para detectar celulares de civiles y confiscarlos para que no tengan ningún celular activo (HRW, 2022).

Más allá de lo violatorio de la medida de confiscar los celulares de civiles ucranianos, es fundamental poner nuestra atención en la tecnología usada de forma indiscriminada para localizar celulares de civiles a fin de confiscarlos, pues estaban siendo usados para grabar los crímenes que la milicia rusa cometía contra civiles.

Desde el punto de vista de inteligencia militar, es comprensible tomar medidas para que, por ejemplo, no se dé la denuncia de los crímenes que se cometen o que la posición de tanques o el movimiento de tropas no sea revelada, pero estos actos de confiscación de bienes de civiles no son permitidos bajo el DIH.

Adicionalmente, estos celulares pudieron ser objeto de intrusiones indebidas para poderlos localizar, o se interceptaron las redes de telefonía para identificar los lugares en la región de Kiev, fuera del territorio ruso, que emiten señales de uso de celulares. Esta es una información que se tomó por medio de la tecnología. Si se tuvo acceso a las bases de los prestadores de tecnología para acceder y así tomar represalias, se configura una intrusión como *cyberwarfare* dentro del conflicto. Si se tuvo acceso a los sistemas de GPS de los celulares, también hubo un acto de intrusión contra los civiles para ubicar y confiscar sus celulares.

Actos como estos de tomar información de la población de uno de los Estados beligerantes es una de las maneras en que la información puede robarse para usarse en el conflicto a favor de la parte que la robó, violando la soberanía estatal por haber accedido a bienes y datos generados dentro del Estado, en este caso, de Ucrania.

Es relevante señalar el caso mencionado por el representante de la Misión Permanente de Georgia ante las Naciones Unidas en la carta del 1º de julio de 2021 dirigida al secretario general y a los representantes permanentes de los miembros del Consejo de Seguridad por la presidencia del Consejo de Seguridad, en la cual relató que en agosto de 2008 Georgia fue víctima de "un ciberataque masivo realizado en paralelo a la agresión" de Rusia sobre Georgia, y que la modalidad de guerra híbrida la había estado usando Rusia en su contra desde los años noventa.

Igualmente, expresa que en 2019 recibieron un nuevo ataque a gran escala que afectó servidores y sitios web, entre otros "sistemas operativos de la administración del presidente de Georgia, los tribunales, asambleas municipales, órganos estatales, organizaciones del sector privado y medios de comunicación". Tras investigaciones profundas, concluyeron que este último ataque había sido planeado y ejecutado por la División Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia.

Este tipo de operación es especialmente significativa, porque, si se infiltran las redes de seguridad nacional, se obtendrá toda la información reservada, lo que podría ser legítimo como parte de la estrategia, pues también se puede llevar a cabo con métodos análogos, pero ello implica irrumpir en el ciberespacio de una forma en que se viola la soberanía nacional por tratarse de páginas creadas y controladas por el Estado. Esto siempre y cuando la escala e impacto genere un daño o perjuicio asemejable al del uso de la fuerza armada.

2.3. Manipulación de infraestructuras críticas

Las infraestructuras críticas son las instalaciones físicas o tecnológicas que cimentan el funcionamiento de los servicios esenciales de la sociedad.

Conforme con el Centro de Ciberseguridad Industrial (CCI, 2022), el primer ciberataque a una infraestructura crítica fue el que se emitió desde un servidor ruso hacia una planta de servicio de agua en Illinois (Estados Unidos) el 8 de noviembre de 2011. Adquirieron los permisos para ingresar al servicio de distribución de agua y lograron desactivar una bomba de distribución remotamente.

El CICR (2019) identifica que estas estructuras pueden estar en riesgo desde otro ángulo al indicar que las redes civiles y las redes militares pueden estar interconectadas en el ciberespacio, y que exponen a ataques sin discriminación ni proporcionalidad a los civiles y a los combatientes (p. 8).

Si pensamos en lo sucedido en Illinois, se abre un abanico infinito de riesgos. Dentro de los dolorosos conflictos vigentes, uno de los Estados beligerantes podría decidir entrar a la red de los hospitales que atienden heridos de guerra, civiles y militares, para apagar todo el sistema de acueducto, eléctrico o servicios tecnológicos con el fin de que no puedan atender a los heridos, incumpliendo así el principio de distinción y el mandato del artículo 3º común de los Convenios de Ginebra de no atacar a quienes están fuera de combate.

Las terminales de transporte, estaciones de tren y tranvía que funcionan y se coordinan por medio de datos también estarían en riesgo. En el desarrollo de la guerra entre Rusia y Ucrania, Rusia atacó una estación de tren que estaba ocupada por civiles que iban a ser evacuados. Esto resultó en 50 muertos y 300 heridos (*BBC News Mundo,* 2022). Si la metodología no fuera un explosivo sino una infiltración al sistema de trenes de tal forma que se genere un choque, un corte eléctrico o un cambio en la orientación de los rieles móviles o del GPS para sacarlos de la ruta de evacuación, se trataría nuevamente de una infiltración a una infraestructura crítica por medio de un ciberataque, que reúne nuevamente los elementos de violación a la soberanía y acto hostil contra la población civil que no participa de las hostilidades.

Estas posibilidades existen y, si se materializan, se configurarían en crímenes de guerra, probablemente de lesa humanidad, y se incumpliría con el DIH, lo que reitera la necesidad de atender los ataques por operaciones cibernéticas entre Estados como lo que son: actos que, aplicando el artículo 1º de la Resolución 3314 de 1974, constituyen un ataque o un acto de agresión, solo que, en lugar de hacerlo a través de fuerzas armadas de forma tradicional, se hace por medio de una operación cibernética.

A los tipos de ataques cibernéticos mencionados ya se les ha dado la interpretación de que pueden ser emitidos con objetivos militares y hacia bienes o redes de información y funcionamiento que podrían ser objetivos militares. Cada uno de estos modos de generar afectaciones a militares y civiles a través de las ciberoperaciones demuestra lo que puede quedar sin atribución de responsabilidad de forma específica si no se hace una debida codificación de la existencia de estos nuevos métodos de guerra.

Sin tener que especular demasiado, el incidente de la explosión de *beepers* en el Líbano materializa el riesgo que puede existir de no solamente irrumpir en estructuras críticas de servicios públicos, sino en una nueva estructura crítica: los celulares y métodos portables de comunicación. Este caso es interesante, pues, según se reporta, "desde el comienzo del conflicto en Gaza el año pasado, Hezbolá había advertido a sus miembros de que no utilizaran teléfonos celulares por temor a que pudieran ser manipulados o rastreados por agentes de inteligencia israelíes, por lo que estaban usando aparatos buscapersonas —conocidos también como mensáfonos o *beepers*— para comunicarse".

Si estos dispositivos fueron interceptados después de ser entregados a los miembros de Hezbolá, ¿cómo y qué se activó dentro de ellos para generar explosiones que dejaron al menos 2800 heridos y 12 muertos? (*BBC News Mundo,* 2024). ¿En qué momento se dio la intercepción o la instalación de un elemento susceptible de ser activado como explosivo? ¿Desde su fabricación?

Debido a que este no es un texto sobre ingeniería de las tecnologías, se deben hacer las preguntas desde el derecho. En este caso, cabría invitar a los Estados partes de la Organización Mundial del Comercio a que incluyan dentro del Acuerdo sobre Obstáculos Técnicos al Comercio que no se puedan instalar elementos explosivos en dispositivos de comunicación individual como *pagers, beepers,* celulares o computadores, que puedan ser activados remota y voluntariamente.

Ha habido eventos en los que celulares y computadores explotan, pero no habían sido explosiones coordinadas hacia dispositivos en posesión de un grupo específico de personas hasta ahora. Si la explosión fue generada por manipulación de un elemento explosivo (la batería u otro elemento desconocido) contenido dentro de los *beepers* desde su fabricación o a través de una infiltración al sistema físico operativo de los dispositivos, estamos frente a un ciberataque de infiltración a una infraestructura crítica de forma muy preocupante. Los celulares y dispositivos electrónicos pueden verse como infraestructura crítica de comunicaciones en tanto que son un objeto producido, comprado y usado masivamente por toda la población, civiles o no, para recibir un bien físico y un servicio de comunicación.

¿Qué otros dispositivos electrónicos, domésticos o de uso personal pueden ser manipulados para explotar a voluntad de quien decida que el dueño de ellos merece ser un objetivo de ataque explosivo, o eventualmente de otra índole, como químico o tóxico? Si se generan efectos comparables al uso de la fuerza armada, deben ser analizados a la luz del artículo 2(4) de la Carta de la ONU, de los principios de distinción y proporcionalidad del DIH, y de la teoría de la aplicación de la legítima defensa.

Aún no se ha dado un ciberataque que inicie una guerra por sí mismo, pero no es ideal tener que esperar a que ello suceda para actuar sobre la marcha y mientras tanto recurrir a los elementos existentes, puesto que, si bien son muy útiles y abarcan muchas necesidades, ir a la fuente del asunto puede ser una mejor medida. Y aunque no toda irrupción alcanza el umbral de agresión, cuando se generen daños sustantivos, por ejemplo, a la seguridad nacional o a sus operaciones militares, puede evaluarse su semblanza al uso de la fuerza definiendo elementos contextuales. Es por ello por lo que una definición que determine claramente qué sí es un acto de agresión a través de ciberoperaciones es ideal, porque no todo es un acto de agresión, pero sí lo puede llegar a ser, en especial con el rápido avance de la tecnología y la dependencia de los sistemas de tecnología de la información y las comunicaciones.

3. Literal *h* como enmienda hipotética de adición a la definición de agresión contenida en el artículo 3º de la Resolución 3314 de 1974

La propuesta de hacer una enmienda, aunque hipotética, a esta resolución no vinculante pero que constituye costumbre internacional parte justamente de la base de que genera menos rechazo definir sin obligar para poder actuar a través de la costumbre que proponer la negociación de un tratado completo o pretender que el Consejo de Seguridad haga una definición vinculante, o, más difícil aún, que se reformen los Estatutos de la Corte Internacional de Justicia o de la Corte Penal Internacional directamente. La costumbre ya reconocida sobre la resolución haría práctica la aplicación de ese nuevo literal sin tener que ajustar todos los textos, ya que se convirtió en una fuente no solo por tener la calidad de costumbre internacional, sino porque es el referente y la fuente de la cual se extrae la definición de acto de agresión.

Es prudente comentar que la propuesta que aquí se presenta nace en un tiempo en el que todavía no se ha hecho un mandato ni un acercamiento real por parte

de los Estados firmantes de la Carta de las Naciones Unidas para atender por medio de codificación el asunto de la *cyberwarfare,* de los ciberataques y, mucho menos, de los ciberataques como constituyentes de un acto de agresión. El amplio paso del tiempo ha sido una constante a la hora de identificar riesgos y tomar medidas por escrito.

Este comentario sobre el paso del tiempo es pertinente, pues el mandato de definir los actos de agresión se dio a través de la Resolución 2330 de 1967, como bien consta en la primera cláusula preambulatoria de la Resolución 3314 de 1974. En 1967 y 1974 ya había suficiente consciencia y conocimiento de que existían actos de agresión y las formas en que se llevaban a cabo, y que estos actos iniciaban o hacían parte de las conductas dentro de conflictos armados internacionales.

No obstante, tomó siete años llegar a un acuerdo de cómo definir estos actos de agresión por medio de una resolución de la Asamblea General, que, como bien es sabido, implica que no es vinculante. De todas formas, fue un gran esfuerzo y logro, dado que esta resolución es costumbre internacional, pero sí que demuestra que existe una dificultad alta para atender asuntos importantes y evidentes.

Como se propuso al inicio, los ciberataques: i) no son fácilmente atribuibles a un autor; ii) tienen la capacidad de generar un daño; iii) violan la soberanía estatal; iv) están desprovistos de consecuencias claras; y v) no cuentan con posibles rutas de acción proporcional que vaya acorde con la Carta de las Naciones Unidas.

Sin embargo, hay otro elemento que se puede agregar, el del umbral de gravedad, para llegar a constituir efectivamente un acto de agresión. El Proyecto de Artículos sobre Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos no exige que se constituya un daño dentro de la acción u omisión ilícita atribuible a un Estado. Para que el cuerpo del Proyecto de Artículos sea aplicable, debemos apartarnos de la no exigencia de daño y concentrarnos en las ciberoperaciones que sí generen un daño equiparable al generado por un ataque por medios convencionales; si no se exigiera ese umbral de daño de equiparación, se abriría la puerta a escalar conflictos a través de dar calidad de acto de agresión a ciberoperaciones que no poseen esa envergadura.

Si bien el artículo 1º de la Resolución 3314 de 1974 establece que "la agresión es el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas, tal como se enuncia en la presente definición", ya vemos que estas violaciones a la soberanía, a la integridad territorial y a la independencia política no se dan solamente a través de fuerza armada en el sentido tradicional de la palabra.

Entre abril y mayo del año 2007 Estonia fue objeto de múltiples y reiterados ataques después de quitar un monumento a los soldados soviéticos que murieron durante la Segunda Guerra Mundial. Uno de ellos dejó fuera de servicio páginas oficiales del Estado, sistemas de varios colegios y de bancos; el más grave fue el ataque del 10 de mayo cuando "el sitio web www.hanza.net (el banco más grande de Estonia) fue blanco de un fuerte ataque de DDoS; más del 97 % de todas las transacciones de banco en Estonia son realizadas en internet" (Díaz del Río Durán, 2011, p. 238). Las páginas del gobierno sufrieron cambios de apariencia y filtración de su contenido en medios de comunicación y foros de discusión rusos. Se ignora si el Estado ruso orquestó o no esta ráfaga de ataques.

El asunto de Estonia, aunque produjo muchos daños, igual que los demás casos comentados, no tuvo el calibre de escalar a un enfrentamiento que culminara en hostilidades entre Estados. No obstante, vale la pena discutir cuándo sí podría originar un daño suficiente para que un ciberataque inicie un conflicto por sí mismo.

Para adentrarse en los criterios que se deben tener en cuenta para la propuesta de enmienda hipotética, se toman como referencia i) la interpretación y aplicación de diferentes aspectos de los literales existentes, así como su formato de redacción; ii) ejemplos de posibles ciberataques; y iii) criterios de proporcionalidad y atribución contenidos en el DIH y en el Proyecto de Artículos sobre Responsabilidad de los Estados.

Para ello se proponen los siguientes criterios:

- *La intención del agresor:* que se pueda determinar que la operación fue deliberada y emitida contra un Estado soberano con la intención de generar un daño.
- *La gravedad del ataque:* evaluar el daño causado, incluyendo pérdidas humanas, económicas y sociales.
- *El contexto:* tener en cuenta si el ataque se produjo en un contexto de tensiones o conflictos preexistentes o dentro de hostilidades vigentes.
- *La atribución:* que se pueda relacionar el origen de la operación con un Estado. (Para esto se puede usar el Proyecto de Artículos sobre Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos).
- *La proporcionalidad:* analizar si el ataque puede considerarse equivalente a un acto de agresión armado tradicional.

De estos elementos, el más importante es el de la proporcionalidad. Si dentro de la operación se producen daños a bases militares o se interfiere en la red de armas controladas informáticamente para hacerlas explotar, podrían ser ataques que alcanzan ese umbral de violencia que permita aplicar el concepto de agresión con claridad.

Si examinamos los actos que el artículo 3º de la Resolución 3314 de 1974 identifica como actos de agresión, podemos acercarnos a traducir estos ataques tradicionales a las operaciones cibernéticas que pueden equipararse con ellos y a otros que no son aplicables.

El artículo 3º se remite al artículo 2º, y, al hacer esto, se somete a la diferenciación entre un quebrantamiento de la paz y una amenaza a la paz internacional, que será lo que decidirá el Consejo de Seguridad al momento de caracterizar un acto como acto de agresión o no.

El literal *a* de la resolución queda parcialmente excluido de semejanzas, pues no se pueden anexar territorios por medio de un ciberataque, pero sí que se pueden hacer infiltraciones totales a los sistemas de seguridad de un Estado, y dado que los Estados tienen control sobre su espectro electromagnético, y más claramente aún, sobre las páginas y bases de datos bajo su dominio, si se da un acto lo suficientemente agresivo, podría interpretarse que hay una invasión por afectar la soberanía estatal.

Por su parte, el literal *b* sí tiene más elementos que pueden ser aplicables a los ciberataques. Si un Estado se infiltrara en el sistema de control de misiles y los lanzara hacia el propio territorio, se daría una agresión armada generada por una ciberoperación.

El bloqueo de los puertos o costas recogido en el literal *c* no es tan susceptible de ser efectuado por una ciberoperación; lo que sí podría suceder es que se saboteen las comunicaciones que permiten la organización y comunicación para el tránsito de buques, lo que puede causar accidentes, pérdidas de mercancías, imposibilidad de llegar a puerto o demás daños logísticos. Sin embargo, esto no configuraría necesariamente un acto de agresión por ciberoperaciones.

Tomando en consideración que hay armas autónomas y que las operaciones cibernéticas pueden emitirse con la intención de generar un daño como medio de adelantar hostilidades, y recordando los escenarios hipotéticos que se presentaron en la sección anterior, las fuerzas armadas terrestres, navales y aéreas mencionadas en el literal *d* pueden ser susceptibles de un ciberataque que sí podría ser clasificado como acto de agresión.

El literal *e* puede aplicarse en una situación similar al caso de Nicaragua (2010), pero no es semejante a una operación cibernética, al menos no lo es al revisar casos empíricos con la tecnología existente.

La forma de agresión codificada en el literal *f* no podría darse a través de ciberataques, ya que nuevamente se trata de un tema geográfico físico. Quizá si la cercanía territorial aporta facilidad para irrumpir en los sistemas informáticos de un Estado,

podría originarse un acto de agresión a través del uso indebido del territorio del otro Estado, pero ya hemos visto que no es nada necesaria la cercanía para adelantar una ciberoperación.

El literal *g* podría haberse concretado en el caso Stuxnet, dado que el virus se instaló a través de una USB portadora del programa maligno que dio la orden de autodestrucción a las centrífugas de enriquecimiento de uranio. Si la persona que instaló el virus fue enviada por Estados Unidos o Israel, a los cuales se les atribuye informalmente el acto, habría el elemento estatal, pero no de daño o de alcance para ser considerado un acto de agresión.

Las relaciones establecidas en estos breves comentarios sobre el artículo 3º se hicieron con tres propósitos. El primero, identificar cómo se pueden configurar esas formas de agresión mediante ciberoperaciones hipotéticas o reales; el segundo, para reconocer que las operaciones que se han dado no llegan al umbral de agresividad al que se refieren los literales del artículo; y el tercero, para evidenciar que hay elementos de los ciberataques que quedan por fuera de estas disposiciones, pues son un método nuevo, un arma nueva, que no permite la misma claridad pero que sí puede generar un daño semejante.

Así las cosas, se confirma que los ciberataques no siempre encajan dentro de las manifestaciones previstas de los actos de agresión.

No obstante, lo más importante que se debe resaltar de este documento es que el hecho de que por ahora no se haya iniciado una guerra por medios cibernéticos no quiere decir que nunca vaya a suceder y estar preparados con antelación sería positivo para no sentir que tenemos las manos amarradas al tratar de atender un asunto nuevo.

Con base en las consideraciones anteriores, se propone la siguiente definición de los ciberataques como actos de agresión en el ámbito de la ONU, en sintonía con los artículos 1º y 2º de la Resolución 3314 de 1974.

Un ciberataque constituirá un acto de agresión cuando, llevado a cabo por un Estado o por actores no estatales respaldados por un Estado, tenga la intención y el efecto de comprometer la soberanía, integridad territorial, seguridad nacional o estabilidad política de otro Estado. Esto incluye, pero no se limita a, acciones que resulten en pérdidas humanas, interrupción de infraestructuras críticas o daños económicos y sociales significativos, y que bajo el concepto del Consejo de Seguridad sean comparables en alcance y gravedad a los actos de agresión armada definidos en el artículo 1º de la Resolución 3314 de 1974 de la Asamblea General de las Naciones Unidas.

Bajo tal concepto, la definición propuesta de enmienda hipotética por adición de un literal *h* al artículo 3º de la Resolución 3314 sería la siguiente: "La emisión por un Estado, o en su nombre, bajo su control y mandato, de operaciones cibernéticas que lleven a cabo actos que resulten en daños significativos a infraestructuras críticas, sistemas de defensa armada o bienes esenciales para la vida y subsistencia de la población civil de otro Estado con el fin de generar daños con gravedad equiparable a los actos antes enumerados, o su sustancial participación en dichos actos".

Esta definición hipotética está basada fuertemente en el contenido y la estructura del literal *g* del artículo 3º, compartiendo elementos como que el acto de agresión por medio de ciberoperaciones puede llevarse a cabo directamente por un Estado, en su nombre, o con sustancial participación de un Estado, pero agregando que también es importante que el Estado implicado tenga determinación sobre la forma en que se lleva la operación, por lo que se incluye la aclaración de que se actúe bajo su control y mandato.

Como se expuso en la sección anterior, varios de los objetivos más frecuentes han sido las infraestructuras críticas o bienes esenciales para la vida y subsistencia de la población civil, por lo que es pertinente incluirlas como posibles objetivos de un acto de agresión, pero siempre con el salvamento de que se debe alcanzar una gravedad semejante a la de un ataque armado para evitar que se escale automáticamente el conflicto por abrir una posibilidad de respuesta ante cualquier intrusión.

Así mismo, se incluye el sistema de defensa armada de otro Estado como objetivo de ciberoperaciones, que, de ser atacado, podría constituir un acto de agresión, acudiendo al contenido del literal *c,* pues, al hacer la aclaración de que se configura sobre sistemas de defensa armada, se limita el ámbito del ataque a bases militares y establecimientos de almacenamiento de arsenal militar, lo cual, como en el literal *c,* implicaría un ataque a fuerzas armadas terrestres, aéreas o navales del Estado atacado.

Por último, se indica que esa operación debe organizarse "con el fin de generar daños con gravedad equiparable a los actos antes enumerados", para ajustar a estas operaciones lo dispuesto en el literal *g,* haciendo las agresiones más claramente identificables y poniendo un umbral de daño que no permita escalar cualquier operación al nivel de un ataque que amerite una respuesta armada de forma prematura.

En otras palabras, el acto de agresión del literal *h* hipotético se configuraría únicamente cuando los daños generados alcancen un nivel equiparable al del uso de la fuerza tradicional. Adicionalmente, se recalca que sí debe haber daño, para que no todas las ciberoperaciones contra un Estado se entiendan como acto de agresión, pues no es el objetivo de la definición propuesta.

Esta definición busca la suficiente amplitud para abarcar las diversas formas de ciberataques, pero al tiempo establece criterios claros para determinar su gravedad e intención con el propósito de no escalar conflictos después de la ejecución de ciberoperaciones. Además, subraya la importancia de la atribución y el contexto, aspectos fundamentales para evaluar la responsabilidad en el ciberespacio.

Conclusiones

Sin atribuir juicios de valor demasiado definitivos, los Estados que tienen la capacidad, los medios y los motivos para usar las operaciones cibernéticas como un arma dentro de un conflicto (lo que se conoce como *cyberwarfare*) o de iniciar hostilidades con otro Estado o en el territorio de otro Estado son quienes eventualmente podrían promover con determinación la codificación de normas internacionales que califiquen un acto como internacionalmente ilícito y es posible que no quieran cerrar la puerta de forma tan definitiva. A su vez, los Estados que tengan menos capacidad militar pueden recurrir a enfrentarse a un Goliat por medios cibernéticos, en lugar de usar medios tradicionales, lo cual debe ser anticipado, puesto que es un potencial medio de guerra que nivelaría las asimetrías militares a través de la perpetración de hostilidades en el ciberespacio.

El CICR empezó a estudiar los impactos de los ciberataques desde 2011. En 2013 se expresó de la siguiente manera: "El término se utiliza aquí para referirse a los medios y métodos de guerra que consisten en ciberoperaciones que constituyen un conflicto armado o se adelantan en el contexto de un conflicto armado, bajo la definición del derecho internacional humanitario". El *Manual de Tallin* (2013) manifestó, y el CICR coincidió, que el DIH es aplicable a ciberataques que se den dentro de un conflicto armado, lo cual nos encamina a concluir que un ciberataque sí puede tener el tenor y el umbral de violencia que tienen las formas tradicionales de agresión, en especial con respecto de los daños.

A través de las referencias y del análisis de las operaciones ya llevadas a cabo y de proyectar las que se pueden lanzar, se refuerza la necesidad de la inclusión de ciberataques como forma posible, plausible y probable de agresión. Esto debe exhortar a todas las áreas del derecho internacional a tomar precauciones y prever lo que puede suceder en un futuro no muy lejano.

Ya se ha estudiado desde el derecho internacional humanitario, desde los estudios de responsabilidad de los Estados e, incluso, desde el derecho penal internacional. Christine Carpenter (2025) en su texto "Whose [Crime] is it Anyway" expone las diferentes formas en que el derecho internacional penal podría atender asuntos relacionados con los ciberataques y cómo la Corte Penal Internacional

debería interpretar los elementos de la conducta penal, la sistematicidad, la cadena de mando y demás desde la responsabilidad penal, que es individual. Esta apreciación señala otro vacío que la codificación de los ciberataques como actos de agresión podría llenar.

Sin embargo, a pesar de que en este momento la Corte tendría competencia sobre los ciberataques, sería bajo la forma de instrumentos a través de los cuales se cometen crímenes de guerra o de lesa humanidad, mas no de agresión. Siendo que la Corte Penal Internacional también tiene competencia sobre los actos de agresión, no se deberían dejar fuera de esta competencia los actos de agresión que eventualmente se cometan por medio de ciberoperaciones y que ameriten ser investigados por la Corte.

Si los ciberataques se codifican, se logrará un importante desarrollo del derecho internacional que atenderá necesidades prácticas actuales y futuras para determinar responsabilidad por incumplir obligaciones que ya sean claras, sin tener que hacer aplicaciones interpretativas de normas creadas para conflictos desarrollados con otros medios.

La cláusula Martens es una herramienta maravillosa, pero ayudar a que haya menos dudas al momento de aplicar el derecho internacional es importante para evitar que haya falta de justicia internacional, como bien puede suceder. Los avances en la tecnología de punta con la ayuda de la inteligencia artificial y la dependencia de sistemas informáticos para almacenar toda la información sensible de los Estados exponen ya no un riesgo, sino una certeza de que el campo de batalla inicial será el ciberespacio en un mediano plazo. Adelantarse a las necesidades desde todas las áreas del derecho internacional no es solo deseable, sino una responsabilidad que se debe asumir con tiempo suficiente para disminuir el tiempo promedio de acción jurídica internacional

Aunque la idea de tener una nueva definición real está plagada de optimismo por enfrentarse a obstáculos políticos, no hace daño dejar constancia, al menos desde el debate académico, de proponer un literal *h* a la resolución existente, de que hay necesidades nuevas que deben ser atendidas y de explorar posibles formas de hacerlo.

Referencias

"Un ataque sin precedentes": cómo ocurrieron las explosiones de *beepers* y *walkie-talkies* que han dejado decenas de muertos y miles de heridos en Líbano. (2024, 18 de septiembre). *BBC News Mundo*. https://www.bbc.com/mundo/articles/cx20l70yrn2o

Ávila García, I. L. (2024). Ciberseguridad y derecho internacional: el conflicto en el ciberespacio. *Revista Derechos Humanos, Conflicto y Justicia, 3*(6), 115-127. https://doi.org/10.25062/2955-0262.4946

BBC Verify, & Equipo de Periodismo Visual. (2025, 22 de junio). Cómo es Fordo, la instalación nuclear secreta de Irán bombardeada por EE. UU. *BBC News Mundo*.

Carpenter, C. (2025). Whose [crime] is it anyway? Adapting the crime of aggression to grapple with AI and the future of international crimes. *Journal of International Criminal Justice,* 1-18. https://doi.org/10.1093/jicj/mqae055

Comité Internacional de la Cruz Roja (CRIC). (2011). *ICRC, international humanitarian law and the challenges of contemporary armed conflicts in 2011.* https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflicts-2011

Comité Internacional de la Cruz Roja (CRIC). (2019). *Derecho internacional humanitario y ciberoperaciones durante conflictos armados: documento de posición del CICR*. https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_armed_conflict_sp.pdf

Consejo de Seguridad de las Naciones Unidas. (2021, 1º de julio). *Carta del presidente del Consejo de Seguridad dirigida al secretario general y a los representantes permanentes de los miembros del Consejo de Seguridad (Documento S/2021/621).* Naciones Unidas. https://docs.un.org/es/s/2021/621

Convenios de Ginebra del 12 de agosto de 1949.

Corte Internacional de Justicia. (1996, 8 de julio). *Legalidad de la amenaza o el empleo de armas nucleares*. Opinión consultiva.

Díaz del Río Durán, J. (2011). La ciberseguridad en el ámbito militar. *Cuadernos de Estrategia,* (149), 215-256.

El virus que tomó control de mil máquinas y les ordenó autodestruirse. (2015, 11 de octubre). *BBC News Mundo*. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Grupo de Trabajo de Composición Abierta sobre la Seguridad y el Uso de las Tecnologías de la Información y las Comunicaciones 2021-2025. (2025). *Draft final report, eleventh substantive session, New York A/AC.292/2025/CRP.1*. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf

Gutiérrez Espada, C., & Cervell Hortal, M. J. (2012). El régimen jurídico de los espacios (conclusión). En *El derecho internacional en la encrucijada: curso general de derecho internacional público* (3ª ed.) (pp. 311-330). Trotta.

Human Rights Watch (HRW). (2022, 18 de mayo). *Ukraine: executions, torture during Russian occupation. Apparent war crimes in Kyiv, Chernihiv regions, section Kyiv Region, Andriivka*. https://www.hrw.org/news/2022/05/18/ukraine-executions-torture-during-russian-occupation

IBM. (s. f.). *Ataques de denegación de servicio (DDoS)*. https://www.ibm.com/es-es/topics/ddos

International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn manual on the international law applicable to cyber warfare*. https://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

Lazar, E., & Costescu, D. N. (2018). Los ciberataques: una noción sin tipificación, pero con un futuro. *Anuario da Facultade de Dereito da Universidade da Coruña, 22,* 157-175. https://doi.org/10.17979/afdudc.2018.22.0.5180

Organización de las Naciones Unidas (ONU), Asamblea General. (1974). *Definición de la agresión* [Resolución 3314 (XXIX)]. https://www.acnur.org/fileadmin/Documentos/BDL/2007/5517.pdf

Organización de las Naciones Unidas (ONU), Asamblea General. (1974). *Definición de la agresión* [Resolución 3314 (XXIX)]. https://legal.un.org/avl/pdf/ha/da/da_ph_s.pdf

Pérez Sierra, I. (2021). *La legítima defensa del Estado frente a ataques cibernéticos según el derecho internacional.* Global Strategy. https://global-strategy.org/la-legitima-defensa-del-estado-frente-a-ataques-ciberneticos-segun-el-derecho-internacional

Rusia y Ucrania: decenas de muertos y más de 300 heridos en ataque a una estación de tren que se usaba para evacuar civiles. (2022, 8 de abril). *BBC News Mundo*. https://www.bbc.com/mundo/noticias-internacional-61038085

Schmitt, M. N. (2014). Wired warfare: computer network attack and *jus in bello. International Review of the Red Cross, 96 (893), 189-206*. https://doi.org/10.1017/S1816383114000381

Tsagourias, N., Buchan, R., & Ambos, K. (2017). *International law and cyberspace*. Elgar Publishing.

Wibowo, A. R. R. (2022). The importance of global effort to secure space sector from cyberattack. *Intermestic: Journal of International Studies, 7*(1), 298-315.

Wolter, D. (2013). *The UN takes a big step forward on cybersecurity.* Arms Control Association. https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity

ANIDIP, Bogotá, ISSNe: 2346-3120, Vol13, pp. 1-24, 2025