Capítulo 5

El principio de proporcionalidad como límite de los ciberataques en los conflictos armados internacionales

DOI: https://doi.org/10.21830/9786289544671.05

Yonni Albeiro Bermúdez Bermúdez
Escuela Militar de Cadetes "General José María Córdova"

Resumen: surgido de la indeterminación acerca de cómo se aplica el principio de proporcionalidad en los ciberataques en medio de un conflicto armado internacional, este capítulo examina si dicho principio es pertinente en estos nuevos escenarios de guerra cuando se despliegan operaciones militares. Para esto, analiza documentos físicos y digitales, bases de datos, revistas indexadas y disposiciones legales. Debido a los avances tecnológicos, hoy es más probable que se produzca una guerra cibernética que una guerra tradicional, ya que cuando se trata de ciberataques es más difícil seguir su rastro e identificar a sus responsables, por lo cual, al presentarse en medio de un conflicto armado, deben estar sometidos a los principios del Derecho Internacional Humanitario y, entre estos, el de necesidad, distinción y proporcionalidad.

Palabras clave: ciberataque; ciberespacio; conflicto armado; Derecho Internacional Humanitario; guerra cibernética; proporcionalidad

Yonni Albeiro Bermúdez Bermúdez

Doctorando, Universidad de Lérida, España. Magíster en Procedimiento Penal, Universidad Militar Nueva Granada, Colombia, Especialista en Derecho Penal, Universidad del Rosario, Colombia. Abogado, Universidad La Gran Colombia, Colombia. Docente, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Orcid: https://orcid.org/0000-0001-8766-6953
Contacto: yonni.bermudez@esmic.edu.co

Citación APA: Bermúdez Bermúdez, Y. A. (2024). El principio de proporcionalidad como límite de los ciberataques en los conflictos armados internacionales. En P. A. Velásquez Cardona, & C. H. Prieto Fetiva (Eds.), *Problemas abiertos en torno del principio de proporcionalidad: análisis desde el DIDH y el DIH* (pp. 141-160). Sello Editorial Esmic.
https://doi.org/10.21830/97862895446 71.05

Problemas abiertos en torno del principio de proporcionalidad: análisis desde el DIDH y el DIH

ISBN impreso: 978-628-95446-8-8
ISBN digital: 978-628-95446-7-1

DOI: https://doi.org/10.21830/9786289544671

Colección Ciencias Jurídicas
Serie Miles Doctus (Investigación formal terminada)
Sello Editorial Esmic

Escuela Militar de Cadetes "General José María Córdova"
Bogotá, D.C., Colombia

2024

Introducción

Uno de los compromisos que incumbe a los adversarios que participan en un conflicto armado no internacional (CANI) o internacional (CAI) radica en adoptar todas las precauciones para proteger de las hostilidades a la población civil que no participa en las hostilidades, bienes y lugares protegidos, garantizando el menor número de víctimas y daños colaterales. A su vez, velar por la preservación de la vida de la población y las infraestructuras civiles. Los principales desafíos radican en garantizar en la fase de planificación y de ejecución la proporcionalidad de una operación cuando estamos en la presencia de nuevas tecnologías para direccionar un ataque cibernético en medio de un CAI.

El principio de proporcionalidad ha sido comprendido por la doctrina nacional como un principio general del derecho, que obliga a tratar de conseguir el justo equilibrio entre los intereses en conflicto (Bernal, 2014). En el escenario del conflicto armado, este principio dispone que los daños indirectos que se pueden llegar a causar a los civiles dentro del marco de un conflicto bélico no deben ser superiores en comparación con la ventaja que se pueda obtener como consecuencia de la operación militar, es decir, la ventaja obtenida debe ser superior a los daños incidentales (Valdés, 2021).

Sin embargo, debido a la imposibilidad de determinar la intensidad de un ataque cibernético y calcular los daños causados, se estaría vulnerando el principio de proporcionalidad, convirtiéndose en una grave violación del derecho internacional humanitario (DIH) y del derecho internacional de los derechos humanos (DIDH), toda vez que la población civil que no participa en las hostilidades puede llegar a resultar afectada por los daños colaterales. Sobre esta premisa, se plantea como pregunta de investigación: Ante las nuevas tecnologías para direccionar un ataque en medio de un conflicto armado internacional, ¿debe aplicarse el principio de proporcionalidad?

Cuando los Estados despliegan operaciones militares en el marco de un conflicto, el uso de la fuerza reconocido por la Constitución debe respetar los derechos y libertades de las personas dentro del acatamiento del principio de proporcionalidad, de ahí que las ciberoperaciones deben ser necesarias y proporcionadas, es decir, se debe limitar la escala, el alcance, la duración y la intensidad del ataque, lo cual implica que cuando se exceden estas propor-

ciones y se llegan afectar infraestructuras críticas y ámbitos industriales, como las centrales nucleares o plantas de energía, estamos ante una latente vulneración del principio de proporcionalidad.

Para llegar al objetivo propuesto en el presente capítulo se aplicará un enfoque cualitativo en el cual se realizará un análisis de fuentes de información como documentos físicos y digitales. Con la metodología propuesta, se hizo una selección y evaluación del conocimiento disponible sobre el objeto de estudio con la finalidad de evidenciar la importancia de respetar los límites definidos por el DIH en relación con los conflictos armados, especialmente, el principio de proporcionalidad en los ciberataques.

En un primer momento se abordan los antecedentes, tipologías y características de los ciberataques; en un segundo momento se estudian los principios clave del DIH aplicables a un CAI; en un tercer momento se realiza un recorrido de los ciberataques más importantes que han tenido lugar en las últimas décadas; en un cuarto momento, se analiza el principio de proporcionalidad como límite de límites de los ciberataques y, en un último momento, se identifican los riesgos, avances y vías en Latinoamérica para combatir los ataques cibernéticos .

Antecedentes, tipologías y características de los ciberataques

Las tecnologías modernas han puesto en peligro la seguridad de los Estados y de sus infraestructuras críticas por medio del ámbito cibernético, toda vez que con la evolución e implementación de las nuevas tecnologías se ha logrado redefinir el concepto tradicional de guerra, cuyas acciones se remontan a finales del siglo XX, lo cual ha generado la aparición de un nuevo concepto de guerra con los ciberataques, es decir, generalmente la implantación de virus o robo de información que responde a un nuevo concepto de conflicto armado. Si bien es cierto, su efecto no es de destrucción masiva, sí pueden llegar a tener un efecto demoledor cuando logran interrumpir la actividad cibernética y afectar la infraestructura critica de un Estado (Ferrero, 2013).

Las guerras se venían desarrollando en escenarios habituales como eran tierra, mar y aire, mirando a la cara al enemigo y luchando en el mismo tiempo y espacio. Sin embargo, en el siglo XXI aparece una nueva tipología de guerra:

los ciberataques, agresiones muy sofisticadas, llevados a cabo por civiles, grupos organizados o directamente por Estados en medio de un CANI o de un CAI. Según Sánchez & López (2017) el objetivo de este tipo de agresiones es robar información estratégica que sirva a los intereses del atacante; el bloqueo de servicios públicos; la toma de control de sistemas industriales, o el manejo de infraestructuras estratégicas que permiten el correcto funcionamiento del país.

Los ciberataques, también denominados por una parte de la doctrina como *ataques informáticos*, utilizan medios técnicos para combatir una guerra contra un enemigo determinado en el ciberespacio (Ambos, 2015). Es así, como estos pueden llegar a implantar un virus en los sistemas informáticos que causan pérdida de información y afectan el funcionamiento normal de las redes o sitios web (Izaguirre & León 2018). Estas acciones implican ingresos no autorizados a sistemas de información restringida, intromisión en sistemas de información o interceptación de datos, las cuales no son autorizadas por el titular de los derechos del sistema o de datos (Robles, 2020). Los casos más recurrentes de ataques en el ciberespacio están orientados a impedir el funcionamiento normal de entidades del Gobierno o empresas privadas, lo cual puede llegar a generar un escenario de desconcierto.

Las características de los ciberataques hacen de ellos el medio idóneo para generar incertidumbre. En primer lugar, se destaca su bajo costo de operatividad, ya que las herramientas necesarias pueden adquirirse a un precio muy reducido en cualquier comercio. En segundo lugar, su omnipresencia y fácil ejecución, pues no se requieren grandes conocimientos técnicos o especializados. En tercer lugar, su efectividad, porque si el ciberataque está bien trazado, es fácil que alcance los objetivos esperados. Asimismo, el reducido riesgo de descubrir al atacante complica la atribución de la comisión de un ciberataque a sus autores o partícipes, junto a un marco normativo precario de los Estados que dificulta la persecución de la conducta punible (Gorjón, 2021; Fernández & Rodríguez, 2017).

Los principales ataques cibernéticos son el *spam* o *adware*, que se caracterizan por producir molestias al sistema; el *spyware*, que puede supervisar hábitos de uso y de navegación, y el *phishing*, que tiene el potencial de emplear la información adquirida de manera no autorizada para realizar ciberata-

ques especializados y de mayor impacto. En el caso de los *troyanos, gusanos* y *ransomware* permiten el robo, la manipulación o la destrucción de datos. Sin embargo, entre los ciberataques de mayor gravedad nos podemos encontrar con los *RootKit* y *Advance Persistent Threats* que pueden llegar a causar una pérdida total e inconsciente del control del sistema y que pueden ser prácticamente indetectables, lo cual les permite permanecer en un sistema durante mucho tiempo antes de que sus efectos sean perceptibles (Ayerbe, 2018).

El acceso, robo, secuestro, transferencia o manipulación no autorizada de información de un sistema o centro de almacenamiento de información que se puede generar por medio de un ciberataque son un problema grave y cada vez más frecuente en entidades públicas y privadas, organizaciones y Estados, ya que los riesgos y amenazas derivados de un ciberataque han generado discusiones relacionadas con las pérdidas económicas, parálisis de las actividades de un país, desventajas en acciones militares, puesta en peligro de la existencia humana y puesta en peligro de infraestructuras críticas de los Estados.

En este contexto, los Estados se han visto en la necesidad de adelantar estrategias de ciberseguridad, entendido esto como maniobras centradas en estrategias defensivas (ciberdefensa) y ofensivas (ciberataques) empleadas para proteger el ciberespacio contra el uso indebido, defensa de su infraestructura, protección de los servicios que prestan y la información que almacenan. Sin embargo, una de las principales estrategias de los Estados frente a los ciberataques es emplear las capacidades del ciberespacio como instrumento de defensa o seguridad (Servitja, 2013).

Un ciberataque tiene como finalidad principal producir incertidumbre en el modelo de seguridad y control de una entidad, organización o Estado o, expresado de forma más práctica, busca revelar los puntos negros y ocultos en la implementación de seguridad que las empresas y los Estados adoptaron (Cano, 2020). Esto ha generado que los ciberataques cada día cobren mayor relevancia en el contexto de la seguridad de los Estados y, especialmente, abre la posibilidad de que futuros conflictos internacionales se desarrollen exclusivamente en estos nuevos escenarios bélicos.

Los ciberataques emplean las desventajas de seguridad presentes en las nuevas tecnologías de la información y comunicación (TIC) con la finalidad de

aprovecharse de las vulnerabilidades que presentan las estructuras cibernéticas (Machin, 2016). Estas estructuras pueden ser sanitarias, económicas, militares, gubernamentales y estructuras críticas. El siglo XXI ha sido reconocido como el siglo de la digitalización, debido a la constante evolución tecnológica que ha permitido hablar de la *cuarta revolución industrial*, la cual tiene numerosos pros, pero también contras, los cuales no son ajenos a las operaciones militares que pueden darse en medio de un CAI, especialmente lo relacionado con la aplicación de los principios del DIH.

Principios del DIH aplicables a un conflicto armado internacional

El Derecho Internacional Humanitario, como un cuerpo de normas que busca restringir las atrocidades humanitarias de los conflictos armados, prohibir los métodos y medios de guerra que utilizan las partes en medios de las hostilidades, garantizar la dignidad humana de las personas que no intervienen directamente o que han dejado de participar en las hostilidades (CICR, 2019), se orienta por unos principios básicos, pues incluso la guerra debe tener unos límites los cuales las partes deben respetar. Entre los más importantes están: equilibrio entre la necesidad militar y las consideraciones de humanidad, distinción, precaución, proporcionalidad, etc.

A la luz del principio de equilibrio entre la necesidad militar y las consideraciones de humanidad, el cual reconoce que una de las finalidades de un CANI o CAI es derrotar al adversario con diferentes maniobras operacionales, las cuales conllevan a causar la muerte, heridas en la humanidad, destrucción de objetivos militares o cualquier tipo de daño que puede hacer que el adversario deponga las armas o se rinda. Sin embargo, las consideraciones de humanidad imponen ciertos límites a los métodos y medios empleados en el desarrollo de la guerra, p. ej., armas que generen sufrimientos injustificados. Asimismo, quienes estén en poder de la contraparte reciban un trato digno en todo momento, no se generen tratos crueles e inhumanos en contra de los prisioneros de guerra y se respete en todo momento a la población civil (CICR, 2019).

La piedra angular del DIH es sin duda el principio de distinción, que parte del postulado de que "el único objetivo legítimo que los Estados deben propo-

nerse durante la guerra es la debilitación de las fuerzas militares del enemigo" (CICR, 2019, p.18). De ahí que la población que no participa en las hostilidades y los bienes que ostentan un carácter civil gozarán en todo momento de protección por los peligros originados en una operación militar; a su vez, el principio va aparejado de la prohibición de ataques indiscriminados (Benavides, 2015). Por lo tanto, las partes en combate tienen la obligación de hacer distinción en todo momento entre población civil y combatientes, no pudiendo, por ende, atacar a estos o bienes de carácter civil, y, en consecuencia, solo deben dirigir sus operaciones bélicas contra objetivos legítimos (Salmón, 2016).

El CICR, mediante la guía para interpretar la noción de participación directa en las hostilidades según el DIH, identificó tres elementos constitutivos de la noción de participación directa en las hostilidades, con la finalidad de diferenciar a quienes no hacen parte de las hostilidades y entre los cuales se encuentran: umbral de daño, causalidad directa y nexo beligerante. El primero de estos, debe afectar de forma ilegítima las operaciones o capacidad militar de una de las partes inmersas en las hostilidades. En el segundo elemento, debe existir un nexo causal directo entre el acto realizado y el daño infligido, el cual se deriva de una operación militar y, el último elemento, el acto debe haber sido diseñado específicamente para causar de modo directo el umbral del daño requerido con la operación militar (Salmón, 2016).

En cuanto al principio de precaución, íntimamente ligado con el principio de distinción, establece que las operaciones militares se deben desarrollar con cuidado constante de no afectar a la población civil y los bienes de carácter civil; por el contrario, siempre en medio de las hostilidades se debe buscar su preservación (CICR, 2019). Este principio debe ser objeto de respeto por ambas partes inmersas en el conflicto, de ahí que la parte que inicia una operación militar debe hacer todo lo posible para evitar causar daños innecesarios como resultado de sus operaciones, a su vez, la parte que es atacada deberá adoptar todas las medidas respectivas para proteger a la población civil y bienes de los contraataques que busquen repeler las agresiones.

De esta manera, quienes planifiquen o decidan llevar a cabo una operación militar en medio de un CANI o CAI deben tener en cuenta como límite de la guerra el principio de precaución, para lo cual están en la obligación en

todo momento de: 1) hacer lo posible para identificar que los objetivos que pretender atacar sean legítimos, es decir, de naturaleza militar y no civil; y 2) deben adoptarse todas las precauciones posibles en la elección de los medios y métodos que se van a emplear en el ataque, con el fin de evitar o reducir en lo más mínimo los daños a la población u objetos civiles (Farinella, 2021). Sobre los anteriores postulados, se busca dejar a un lado a la población civil que no participa en los conflictos bélicos, con la finalidad de no someternos a ningún tipo de agresión.

Las partes en conflicto durante las hostilidades deben aplicar el principio de proporcionalidad, el cual exige que quienes planeen o decidan un ataque deben abstenerse de iniciarlo o, en el desarrollo de este, suspenderlo cuando se esté en la capacidad de prever que causará daños en la población civil que no participa de manera directa en las hostilidades, perjuicios a bienes de carácter eminentemente civil, o ambas cosas, los cuales serían excesivos en relación con la ventaja militar prevista con en el ataque (CICR, 2019). A la luz de este principio orientador de la guerra se busca evitar una utilización desmedida de los medios y métodos empleados en la guerra, en los cuales resulta desproporcionalmente afectada la población civil.

En el contexto anterior, el principio de proporcionalidad se constituye en una herramienta idónea para la correcta planificación de las hostilidades, mediante su correcto uso y el empleo de los elementos compositivos del test de proporcionalidad, a saber: la idoneidad, la necesidad y la proporcionalidad *stricto sensu*. Se puede llegar a determinar cuándo se está en presencia de una operación militar desproporcionada. La idoneidad está ligada al fin que se desea, si resulta ser la medida más idónea para alcanzar el objetivo propuesto. La necesidad hace alusión al medio por el cual se debe conseguir el fin planteado. Y la proporcionalidad, en un sentido estricto, es el análisis de ponderación que se debe llevar a cabo para determinar las afectaciones a cada uno de los derechos en tensión (Ortiz, 2018).

De hecho, la doctrina especializada ha considerado el principio de proporcionalidad como el *límite de los límites* que protege los derechos fundamentales en medio de un CANI o CAN, pues supone una protección frente a posibles intromisiones ilegitimas en el escenario de protección de los derechos de las

personas y bienes (Carbonell, 2008). De ahí que el DIH ha cambiado la forma de gestionar un CANI O CAI, pues busca humanizar y limitar los efectos de las hostilidades con normas de origen convencional o consuetudinario logrando un equilibrio entre la necesidad militar y el principio de humanidad. Ahora bien, lo que no resulte necesario para lograr que el adversario deponga las armas debe ser considerado como un comportamiento de crueldad que va en contra de este conjunto de normas (Salmón, 2016).

La aplicación del DIH solo puede presentarse cuando se ha iniciado una situación de conflicto armado, bien sea de carácter nacional o internacional. No obstante esta marcada división, se han desarrollado varias posturas que buscan poner fin a esta discusión del carácter del conflicto y crear solo un régimen aplicable a todas las situaciones de conflicto armado, pues se ha evidenciado en la práctica que esta división resulta compleja, ya que el carácter real de los conflictos, la práctica y la jurisprudencia han ocasionado que esta distinción entre conflictos resulte menos precisa (ONU, 2011). Sin embargo, se debe promover la protección sobre el modo en que debe emplearse la fuerza en el marco de un conflicto armado.

Esta protección tiene como finalidad humanizar la guerra, pues si bien es cierto, resulta poco probable o casi imposible que no se presenten este tipo de confrontaciones donde resulte lesionada la población o bienes civiles. Se busca con la aplicación del DIH lograr limitar los efectos de las hostilidades por medio de una serie de reglas de obligatorio cumplimiento para las partes en conflicto, independientemente del carácter de este (Benavides, 2015). Ahora bien, como las guerras no se acabarán, sino que, por el contrario, con el transcurrir del tiempo se van evidenciando nuevos factores que las generan, resulta necesario que exista una regulación que sea aplicable a los conflictos armados, so pena de que se cometan arbitrariedades en el desarrollo de las hostilidades que afecten gravemente a los seres humanos.

En tal sentido, la creación y aplicación del DIH no busca acabar con los conflictos armados, pues esto no sería posible ya que con el transcurrir del tiempo se van a generar nuevos conflictos por variados motivos que culminen en el campo de batalla. Lo que realmente busca el DIH es regular las hostilidades con la finalidad de mitigar, apaciguar y restringir los sufrimientos que

estos conllevan para la humanidad (Contreras, 2006). Por tal razón, en este momento resulta oportuno revisar nuevos escenarios en los que en un tiempo no muy lejano se desarrollen las hostilidades; estos son los denominados *ciberataques*, de ahí que iniciaremos mencionando los principales ciberataques que se encuentran documentados, para evidenciar las consecuencias que estos han tenido para la población.

Ciberataques más importantes en las últimas décadas

Los principales ciberataques que se encuentran documentados hasta el momento son: los ciberataques cometidos contra Kosovo, con los cuales se logró penetrar la seguridad de la OTAN y de un portaviones de la marina de los EE. UU.; los ciberataques cometidos contra Estonia, conocidos por ser el primer caso documentado de ataques cibernéticos que afectan la seguridad de un país; los ciberataques cometidos contra Georgia, reconocidos por ser el primer caso registrado en el que las operaciones cibernéticas y militares se dan de manera conjunta; los ciberataques contra las instalaciones nucleares de Irak, que frenaron la creación de armas nucleares, y los ciberataques contra Ucrania, los cuales han generado pérdidas económicas.

El ataque cibernético de Kosovo se remonta a 1999, cuando más de 450 expertos informáticos de diferentes naciones consiguieron penetrar en los ordenadores estratégicos de la OTAN, de la Casa Blanca y del portaviones Nimitz de la marina de los EE. UU. (Ferrero, 2013). Esta operación tuvo como finalidad impedir las operaciones que la OTAN tenía planeadas contra Serbia, que, si bien se trató de una demostración de poder que no causó mayores daños, sí logro poner en peligro la seguridad de EE. UU.

Para 2007, Rusia consideró no grato la incorporación de Estonia a la OTAN (Ferrero, 2013). En concreto, para el 27 de abril de 2007 y hasta el 18 de mayo de aquel año se iniciaron los primeros ataques cibernéticos contra Estonia que afectaron sistemas de información de la infraestructura pública y privada (Martínez, 2015; Artiles, 2011). Estos ataques se dividieron en dos fases. La primera se caracteriza por ser ataques simples y rudimentarios contra sitios web de Estonia, especialmente del Gobierno, del Ministerio de Defensa y de los principales partidos políticos. En cambio, la segunda fase se caracte-

riza por ser ataques complejos y coordinados, de ahí que se contaba con listas de objetivos en los que se indicaba hora y lugar del ataque para conseguir un volumen de peticiones con el fin de dejarlos fuera de servicio, este tipo de ataques se realizó por DoS (por sus siglas en inglés *Denial of Service*) (Artiles, 2011; Ferrero, 2013).

Al año siguiente, las tensiones entre Georgia y Rusia se presentaron cuando la región de Osetia del Sur declaró su independencia unilateralmente de Georgia, tras vencerla en una guerra, por lo que se convirtió en una república independiente. Sin embargo, Georgia siempre la ha considerado como parte de su territorio, lo cual ocasionó innumerables conflictos como el del 7 de agosto de 2008, cuando Georgia, por un lado, y Osetia del Sur, Abjasia y Rusia, por el otro, atacaron por sorpresa a las fuerzas separatistas (Artiles, 2011).

La fase previa al conflicto armado se presentó entre junio y agosto de 2008. Los ataques cibernéticos en esta fase se caracterizaron por ser ataques a pequeña escala, como los ataques DdoS (por sus siglas en inglés, *Distributed Denial of Service*) contra sitios web oficiales. En relación con la fase durante el conflicto armado, es decir, desde el 08 hasta el 12 de agosto de 2008, se caracterizaron por ser ataques organizados y coordinados, de ahí que ocurrieron ciberataques contra sitios web del presidente de la República de Georgia, el Parlamento, Ministerios de Defensa y Asuntos Exteriores, el Banco Nacional y las principales agencias de noticias. Como resultado, la capacidad de toma de decisiones del entorno político y militar de Georgia durante el conflicto se vio afectada (Martínez, 2015; Artiles, 2011).

Para 2009 y fruto de las tensiones entre EE. UU. E Irán, el presidente Barack Obama decidió autorizar los ataques cibernéticos contra las instalaciones nucleares Nantanz, ubicadas en Irán. Los ataques consistían en la infiltración de un *cyberworm* llamado Stuxnet, el cual deshabilitó los centrífugos nucleares necesarios para la producción de armas. Así, EE. UU. Consiguió frenar el proceso de creación de armas nucleares de Irán. Más tarde, el Gobierno iraní confirmó que reivindicar los daños ocasionados demandaría meses o hasta años (Manotas & Burgaentzle, 2021).

A mediados de febrero de 2022, el presidente de Rusia, Vladimir Putin, anunció una operación militar contra ucrania, en la cual se llevó a cabo una

serie de ataques cibernéticos a varios sitios web gubernamentales y bancarios de este país, que generaron un colapso total del sistema. Este tipo de ofensiva empleada por Rusia se realizó por *bots*, herramienta digital que permite tareas repetitivas y automatizadas para inundar un servicio en línea, logrando su bloqueo e impidiendo su acceso. Otro tipo de ataque se presentó con la instalación de un *malware* llamado *wiper* que logró destruir datos de distintos sistemas. A su vez, algunos sitios web afectados fueron reemplazados por una advertencia que decía: ""Prepárense para lo peor" (Paúl, 2022).

Los anteriores ciberataques son un reflejo de la dinámica cambiante de la guerra, donde se ha dejado a un lado la guerra tradicional y se emplean nuevas tecnologías para direccionar operaciones militares. Sin embargo, los avances tecnológicos también conllevan nuevos riesgos y oportunidades de cambio que deben trazarse desde un primer momento para definir los escenarios futuros en que van a desarrollarse los CAI.

Riesgos, avances y vías en Latinoamérica contra los ciberataques

Aunque el desarrollo de nuevas TIC ha demostrado tener un sinnúmero de ventajas, también ha complicado la seguridad de los Estados y de sus infraestructuras, toda vez que con la implementación de estas nuevas tecnologías se ha logrado redefinir el concepto de guerra, cuyas acciones se remontan a finales del siglo XX, con lo cual se ha generado la aparición de las llamadas *armas cibernéticas*, es decir, los virus que responden a un nuevo concepto de arma que se emplea en los diferentes ciberataques en CANI o CAI (Ferrero, 2013). Si bien, su efecto no es de destrucción masiva como puede serlo el de las armas ordinarias, sí pueden llegar a tener un efecto devastador cuando logran interrumpir la actividad cibernética, económica, militar y afectar los servicios públicos, robar o destruir datos, entre otras cosas.

Otro de los riesgos latentes que se presentan con esta nueva modalidad, cuando se lleva a cabo un CANI o un CAI, es su difícil forma de demostrar quién fue el responsable de dicho ciberataque, pues su atribución suele ser difícil, ya que no necesariamente se lanzan desde servidores propios en determinado territorio y, por el contrario, estos pueden llevarse a cabo desde cualquier parte del mundo, lo que hace casi imposible su respectivo rastreo. Esta

situación dificulta la localización de los responsables y su posterior judicialización por parte de los Estados afectados por este tipo de ataques.

En los casos en que se logre identificar a los responsables de los ciberataques, tenemos otra barrera, la cual puede llegar a generar impunidad, esta es la falta de regulación dentro de los diferentes ordenamientos jurídicos internos de los países para la investigación y posterior sanción de esta clase de nuevas conductas punibles que merecen un reproche por parte del Estado afectado. Esto se debe al bajo desarrollo de política criminal que permita tener conciencia de los nuevos escenarios en los cuales se están adelantado los conflictos bélicos y que permitan tomar medidas oportunas para frenar las consecuencias de estos nuevos ataques.

Las vulnerabilidades en el *software* utilizado por las entidades públicas y privadas, aunado al mal manejo de las infraestructuras tecnológicas por parte de sus empleados ha permitido dañar, robar, destruir datos, comprometer sitios web o servidores. A su vez, la mala configuración de los sistemas de información por parte de las empresas los hace más vulnerables a ser objeto de un ciberataque. De hecho, cuando los ataques resultan ser exitosos se encuentran en la capacidad de acceder a información confidencial de seguridad del Estado, posicionamiento de armas, daños en sistemas informáticos y afectar la confianza y reputación.

El riesgo para empresas, entidades gubernamentales y Gobiernos de sufrir un ciberataque no se debe ignorar. En la actualidad, entidades, organismos públicos y privados optan por tomar diferentes posturas para combatir esta nueva modalidad de ataques, por eso se han adoptado medidas como análisis de vulnerabilidades, auditorías de seguridad, diseño e implementación de protocolos, aislar los sistemas comprometidos, mitigar los efectos del ataque, evitar su propagación y adoptar medidas para mantener la continuidad del servicio. Asimismo, en las entidades públicas, privadas y de Gobierno se han creado centros de operaciones de ciberseguridad conformados por ingenieros, abogados, gestores de crisis, etc. para responder rápidamente a un ciberataque.

A pesar de estas estrategias preventivas adoptadas por los diferentes países para combatir las secuelas de un ciberataque y reducir sus impactos, es nece-

sario que se adopten medidas conjuntas por los países latinoamericanos, entre ellos Colombia, para diseñar una estrategia de cooperación en la investigación y juzgamiento de estos ciberataques y, por supuesto, el fortalecimiento normativo ante estas nuevas dinámicas de la guerra, exige una reestructuración o modificación de los diferentes ordenamientos penales para que se contemplen sanciones contra estos ataques.

Asimismo, principios del DIH como el equilibrio entre la necesidad militar y las consideraciones de humanidad, distinción, precaución, proporcionalidad, etc., deben aplicarse a este nuevo escenario de la guerra, especialmente, el principio de proporcionalidad que busca el justo equilibrio entre los intereses en conflicto. En el caso de los ciberataques, deben ser objeto de análisis las implicaciones que tendría lanzar un ciberataque de manera indiscriminada, pues tiene el potencial de ser desproporcional y afectar derechos fundamentales de la población civil. A su vez, pueden llegar afectar objetivos que no son militares, sino de carácter civil.

En cuanto a la vulneración del DIH con los ciberataques en un CAI corresponde aquí a un órgano internacional decidir acerca de la violación y de la sanción de los responsables, en este caso pueden intervenir, la Corte Internacional de Justicia o el Consejo de Seguridad, con base en el procedimiento que regula a cada uno imponer las sanciones respectivas contra los Estados que por medio de los ciberataques vulneran los principios del DIH, cuyos límites de orientadores de la guerra deben ser respetados por las partes en conflicto en un escenario tradicional o nuevo de la guerra.

La proporcionalidad como límite de límites de los ciberataques

Los juicios de proporcionalidad que deben hacerse en medio de una operación militar se fundan en determinar el alcance de los daños colaterales o indirectos. Es así como es conocido que para conseguir un bien o una ventaja militar, puede conseguirse como efecto un mal significativo, razón por la cual surge un conflicto al momento de determinar, planificar, desarrollar y ejecutar una operación militar, ya que en últimas se ejecuta la acción o se abstiene de llevarla a cabo para evitar el daño colateral. Esto significa que para hablar de una operación que se rige por el principio de proporcionalidad "el bien que se

quiere conseguir mediante la acción debe al menos compensar al mal que se va a producir como efecto indirecto" (Miranda, 2021, p. 24).

Estos juicios de proporcionalidad, por lo tanto, son relevantes principalmente para evaluar acciones de las que se siguen efectos colaterales malos, por lo que son necesarios para resolver satisfactoriamente los casos de colisión entre dos principios jurídicos que consagran derechos fundamentales (Miranda, 2021). El principio de proporcionalidad en tal sentido establece que cuanto mayor sea el mal que un medio provoque, tanto mayor debe ser el bien que ese medio permita alcanzar, de lo contrario puede hablarse de una operación desproporcional ya que la ventaja obtenida en medio de las hostilidades no es proporcional a los daños causados con esta.

El problema entonces surge de la aplicación del principio de proporcionalidad en medio de un ciberataque, por cuanto este resulta importante para realizar la garantía efectiva de no ocasionar daños colaterales desproporcionados, pero ante la imposibilidad de calcular los daños que pueden llegarse a ocasionar con un ciberataque, este puede llegar a poner en peligro a la población civil y bienes protegidos por el DIH, pues pueden llegarse a afectar estructuras críticas del Estado que son vitales para la sobrevivencia de los seres humanos.

El criterio de proporcionalidad que debe emplearse al momento de llevar un ciberataque en medio de un CAI debe partir de efectuar un análisis riguroso y detallado de los bienes jurídicos que se disputan, es decir, ¿resulta proporcional poner en peligro la población civil para conseguir la ventaja militar que se busca con el ciberataque? Si esta ecuación falla, la operación militar es totalmente desproporcionada. Aunque es complicado facilitar una explicación fenomenológica de las consecuencias devastadoras de un ciberataque, sí tenemos referentes como los abordados en apartes anteriores, donde se evidencian los resultados catastróficos de no aplicar la proporcionalidad a los nuevos escenarios de la guerra.

El análisis desarrollado acerca del principio de proporcionalidad en abstracto confirma sin duda su preponderancia como uno de los límites de límites de un ciberataque. Sin embargo, este análisis no debe abarcar solo el nivel abstracto, ya que, para un mejor abordaje del principio de proporcionalidad, este análisis debe ir acompañado de un examen crítico de este desde

el punto de vista práctico. Es interesante señalar, respecto de los intereses en juego que pueden llegarse a ver inmersos en medio de un ciberataque que deben tenerse, como referentes, la escala, el alcance, la duración y la intensidad del ataque, factores que servirán para determinar con mayor precisión la proporcionalidad de un ciberataque.

En este contexto, cobran especial relevancia los juicios de proporcionalidad, toda vez que son un concepto e instrumento de control jurídico que aparece cada vez con mayor frecuencia en la motivación de las decisiones en el ámbito del derecho operacional, el cual resulta aplicable a los nuevos escenarios de adelantarse las hostilidades militares. Una adecuada concreción de los juicios de proporcionalidad por las partes en medio de un conflicto demanda una racionalidad lógico-operacional, por lo tanto, se convierte en un mecanismo de legitimidad de una operación militar, de ahí que, al no superar este juicio, la operación, como consecuencia, resulta ser desproporcionada e iría en contra de los límites que se han definido para adelantar las hostilidades en medio de un CAI.

La recepción del principio de proporcionalidad por parte del derecho operacional se vio impulsada por el perfeccionamiento de instrumentos normativos internacionales y el desarrollo jurisprudencial de los tribunales internacionales de derechos humanos. Por tal motivo, el principio de proporcionalidad ha ido extendiéndose progresivamente, como es natural, a distintos escenarios prácticos, ámbitos académicos y derechos fundamentales, de ahí que, este nuevo concepto de guerra moderna, es decir, los ciberataques que se han dado con la denominada cuarta revolución industrial no pueden ser ajenos a la aplicación del principio de proporcionalidad como un instrumento de control de los daños colaterales.

Conclusiones

Las amenazas de los ciberataques empezaron a suscitar el interés de la comunidad internacional décadas atrás. Desde el primer ciberataque que se tiene documentado, el de Kosovo, que se remonta a 1999, se han venido escuchando diferentes propuestas de la academia que buscan aplicar en el escenario de un CANI o un CAI, los principios del DIH que orientan los conflictos tradicio-

nales a los nuevos escenarios en que se adelantan las hostilidades militares, toda vez que las características de los ciberataques hacen de ellos el medio perfecto para crear el caos. Su bajo costo de operatividad, ubicuidad, efectividad e impacto y el reducido riesgo de descubrir al atacante complica la atribución de la comisión de un ciberataque a su verdadero autor, autores o partícipes.

El DIH como conjunto de normas que busca limitar las consecuencias humanitarias de los conflictos armados, restringir los métodos y medios que emplean las partes en conflicto en medio de una guerra, se orienta por unos principios básicos, pues incluso la guerra debe tener unos límites que las partes deben respetar, entre ellos, la distinción, la precaución y la proporcionalidad. A este último, se le ha reconocido la categoría de límite de límites de los principios que orientan la guerra, razón por la cual, en medio de las hostilidades militares de un CANI o un CAI debe reconocerse, aplicarse y respetarse, so pena de cometer graves infracciones al DIH.

Al asegurar que se respeten los límites fijados por el DIH, se logra minimizar el impacto negativo de los conflictos armados en la población civil y sus bienes. A su vez, se garantiza un trato humanitario a todas las personas afectadas por las hostilidades, lo cual convierte al DIH en un actor crucial en la prevención de abusos y violaciones de derechos humanos durante el desarrollo de los conflictos armados. Al establecer estos límites, el DIH busca que se evite la impunidad por los actos cometidos y que se logre sancionar a los responsables de violaciones graves en tiempos de guerra.

El análisis del principio de proporcionalidad no solo debe hacerse en abstracto, ya que, para una comprensión integral del principio, tal análisis debe ir acompañado de un examen crítico de este desde el punto de vista práctico. Por ejemplo, la escala, el alcance, la duración y la intensidad del ataque son factores que les van a servir a las partes que participan en las hostilidades para determinar con mayor precisión la proporcionalidad de una operación militar. Estos mismos factores resultan de obligatorio cumplimiento para las partes que llevan a cabo ciberataques en sus operaciones militares, pues estos ataques están en la capacidad de poner en peligro la población civil y pueden llegar afectar estructuras críticas del Estado que son vitales para la sobrevivencia de los seres humanos.

Especialmente debe acatarse el principio de proporcionalidad ante las nuevas tendencias de adelantar las operaciones militares, sin desconocer que los límites fijados por el DIH son todos de obligatorio cumplimiento, pero, por su trascendencia en el desarrollo de una guerra, este adquiere mayor relevancia en las hostilidades, ya que su no cumplimiento puede acarrear una ventaja militar desproporcionada que iría en contra de los postulados del DIH.

Referencias

Angarita Piña, R. (2010). El derecho internacional humanitario, sus reglas, su interpretación y la Corte Penal Internacional. *Reflexión Política, 1*(2). https://n9.cl/pa1uf

Arauz Cantón, J.B. (2013). *Guerra asimétrica y proporcionalidad: retos para el derecho internacional humanitario*. Universidad Complutense de Madrid. https://n9.cl/8qlvr3

Artiles, N. (2011). La situación de la ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia,* (149), 165-214. https://n9.cl/1p473

Ayerbe F. (2018). La ciberseguridad de la industria 4.0: Un medio para la continuidad del negocio. Economía industrial (EI) https://n9.cl/6heni

Benavides, L. (2015). *Derecho internacional humanitario*. CNDH. https://n9.cl/g5uka

Bernal Pulido. C. (2014). *El principio de proporcionalidad y los derechos fundamentales* (4.ª ed.) Universidad Externado de Colombia.

Cano, J. (2020). *Ciberataques. ¿Impuestos inevitables en la dinámica de una economía digital?* DOI: 10.29236/sistemas.n157a6

Carbonell. M. (2008). *El principio de proporcionalidad y la interpretación constitucional*. https://n9.cl/vg0ajr

Contreras Ortiz, J. F. (2009). El Derecho Internacional Humanitario: principio de una educación para la paz. *Educación y Educadores, 9*(1), 177-189. https://n9.cl/s1e5h

Farinella, F. (2021). Sistemas de armas autónomos y principios del derecho internacional humanitario. *Quaestio Iuris, 14*(2), 504-514. https://n9.cl/bjsbo

Fernández, V., & Rodríguez, C. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia* (185), 97-138. https://n9.cl/hm89f

Ferrero, A. (2013). La ciberguerra. Génesis y evolución. *Revista general de marina,* (264), 81-99. https://n9.cl/yx8nuj

Giraldo Restrepo, Y. (2008). Violación del derecho internacional humanitario por parte del Estado colombiano. *Anuario mexicano de derecho internacional, 8,* 223-253. https://n9.cl/567h

Gorjón Barranco, M. C. (2021). Sabotaje informático a infraestructuras críticas: análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista. *Revista De Derecho Penal Y Criminología*, (25). https://doi.org/10.5944/rdpc.25.2021.28405

Izaguirre Olmedo, J., & León Gavilánez, F. (2018). Análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal*, *3*(9), 172–181. https://doi.org/10.33890/innova.v3.n9.2018.837

Llorens, P. (2017). Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional* (17), 785-816. https://n9.cl/qcchj

Machin, M. (2016). La ciberseguridad como factor crítico en la seguridad de la unión europea. *Revista UNISCI, 42*, 47-68. https://n9.cl/za7x1

Maldonado, C. (2018). *Desarrollo de algoritmos eficientes para identificación de usuarios en accesos informáticos* (Tesis doctoral). Universidad Complutense de Madrid. https://dialnet.unirioja.es/servlet/tesis?codigo=123061

Manotas, C., & Burgaentzle, I. (2021). Las guerras cibernéticas en el Derecho Internacional Humanitario: aplicación de los principios rectores del DIH. *USFQ Law Review, 8*(1), 71–86. https://doi.org/10.18272/ulr.v8i1.2162

Martínez, C. (2015). *El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de EE. UU. y Rusia*. [Tesis de grado]. Universidad Pontificia. http://hdl.handle.net/11531/1222

Miranda Montecinos, A. (2021). Los juicios de proporcionalidad en la teoría moral y jurídica de la escolástica española aurisecular. *Bajo Palabra,* (26), 21–38. https://doi.org/10.15366/bp2021.26.001

Nils, M (2019). *Derecho internacional humanitario una introducción integral*. CICR. https://n9.cl/j91ec

ONU (2011). *Protección jurídica internacional de los derechos humanos durante los conflictos armados*. Publicación de las naciones unidas.

Ortiz Agudelo, M. O. (2018). La proporcionalidad como método interpretativo de la justicia transicional. *Revista de la Facultad de Derecho y Ciencias Políticas, 48*(129), 507–548. https://n9.cl/n70ow

Paúl, F. (2022, 26 de febrero). Rusia invade Ucrania: cómo los ciberataques se convirtieron en otra poderosa arma en el conflicto entre ambos países. *BBC News Mundo.* https://n9.cl/h1n6z

Robles Carrillo, M. (2020). Sanciones contra ciberataques: la acción de la Unión Europea. *bie3 Boletín IEEE,* (20), 492-513. https://n9.cl/mj6sk

Salmón, E. (2016). *Introducción al derecho internacional humanitario*. https://n9.cl/gl92e

Sánchez, F., & López, J. (2017). Cooperación público-privada en la protección de infraestructuras críticas. *Cuadernos de estrategia*. https://n9.cl/kljzn

Sapag, M. A. (2008). El principio de proporcionalidad y de razonabilidad como límite constitucional al poder del Estado: un estudio comparado. *Díkaion: revista de actualidad jurídica,* (17). https://n9.cl/rv90h

Servitja Roca, X. (2013). Ciberseguridad, contrainteligencia y operaciones encubiertas en el programa nuclear de irán: de la neutralización selectiva de objetivos al "cuerpo ciber" iraní. *Pre-bie3,* (3). https://n9.cl/sbe45

Urueña Centeno, F.J. (2015). Ciberataques, la mayor amenaza actual. *Pre-bie3,* (1). https://n9.cl/wmnxpj

Velásquez Ruiz, M. A. (2009). Los principios de distinción y proporcionalidad en el marco de la responsabilidad penal internacional individual –contenido y problemática–. *International Law: Revista Colombiana de Derecho Internacional, 7*(14). https://n9.cl/swry6