ARTÍCULOS DE DERECHO INTERNACIONAL PÚBLICO

BREVE ANÁLISIS SOBRE EL ENCUADRE DE LOS CIBERATAQUES EN EL ARTÍCULO 51 DE LA CARTA DE LAS NACIONES UNIDAS Y LA APLICABILIDAD DE LA LEGÍTIMA DEFENSA BAJO EL DERECHO INTERNACIONAL

Andrea Izaguirre Blanco (4º GDL)

Abstract

Este artículo tiene el objetivo de determinar si los ciberataques pueden calificarse jurídicamente como un ataque armado[69] en el sentido del artículo 51 de la Carta de las Naciones Unidas (CNU)[70]. Para ello, se analizarán los distintos tipos de ciberataques y, en función de su carácter jurídico y efectos materiales, se examinará si justifican la posibilidad de tomar represalias legítimas, centrándose particularmente en el derecho de la legítima defensa[71].

Por otra parte, en caso de que tal precepto no sea aplicable, se esclarecerá cuál sería el encuadre jurídico de dicho ciberataque dentro del Derecho internacional público (DIP). Tal cuestión se plantea por el impacto que la innovación tecnológica y el desarrollo de las capacidades cibernéticas han tenido en la naturaleza de los conflictos armados. Planteando así, este artículo pretende responder a la urgente necesidad de actualizar el marco jurídico para garantizar una respuesta efectiva a los retos que conlleva la Era Digital[72].

[69] Concepto tipificado expresamente en el artículo 51 de la CNU: "*en caso de ataque armado contra un Miembro de las Naciones Unidas*".
[70] Instrumento de derecho internacional y de naturaleza vinculante para los estados miembros de la Organización de las Naciones Unidas. Firmadas y ratificada en el año 1945 (Naciones Unidas, s. f.).
[71] Derecho a dar respuesta a una agresión mediante el "*uso de la fuerza"* (concepto regulado por el derecho consuetudinario y tratados internacionales) expresamente reconocido en el art. 51 de la CNU si se cumplen unos determinados requisitos. Principio fundamental del derecho internacional (González Cussac, 2020).
[72] Hace referencia al período del tiempo que abarca desde finales del siglo XX y principios del siglo XXI, el cual está regulado por un uso constante de la tecnología. También llamada "*Tercera Revolución Industrial"* (Economipedia, 2024; Costa, Cuzzocrea y Nuzzaci, 2014).

El análisis se limitará a ciberataques de naturaleza internacional, tomando como referencia el Manual de Tallin[73], obra especializada en la materia, y otras fuentes normativas relevantes del derecho internacional.

Palabras clave

Ciberataques – Derecho internacional – Ataque armado – Uso de la fuerza – Era digital – Derecho de legítima defensa – Carta de las Naciones Unidas

1. Introducción

La creciente integración de las nuevas tecnologías en los conflictos armados ha contribuido a la aparición de nuevas formas de agresión entre las cuales se encuentran los ciberataques. Estos destacan por su alcance transnacional, así como su capacidad de infligir daños tanto a actores estatales como no estatales sin necesidad de mediar el uso tradicional de la fuerza y, por consiguiente, por su cada vez mayor complejidad. En este nuevo contexto, la lógica de los conflictos armados se ha visto alterada permanentemente y con ello, el papel del Derecho como mediador y regulador. La velocidad con la que se desarrollan y evolucionan las tecnologías de la información y comunicación (TIC) supera con creces la capacidad de adaptación e innovación de los marcos normativos existentes[74], generando zonas grises que dificultan la efectiva protección de aquellos afectados por estas situaciones de conflicto.

Por consiguiente, este artículo analizará la siguiente pregunta: *¿Qué tipos de ciberataques pueden encuadrarse en el art. 51 de la Carta de las Naciones Unidas (CNU) y, por ende, ampararse en el derecho a la "legítima defensa"? En caso de responder en sentido negativo, este artículo también cuestionará lo siguiente: ¿Qué condición jurídica tendría dicho ciberataque y, por tanto, qué circunstancias excluyen la ilicitud podrían ser invocadas respecto de las medidas unilaterales para responder a un ciberataque dentro del marco normativo del derecho internacional público (DIP)?*

Desde un punto de vista académico y personal, surge una motivación clara para responder a esta cuestión. Pues, hoy en día, no existe un consenso internacional sobre la aplicación del ordenamiento jurídico a la cuestión de los ciberataques, a pesar de su carácter novedoso. Por este motivo, se cuestiona actualmente la capacidad del marco normativo

[73] Principal proyecto de investigación CCDCOE (*"NATO Cooperative Cyber Defence Centre of Excellence"*) sobre derecho internacional aplicado a operaciones del ciberespacio (NATO Cooperative Cyber Defence Centre of Excellence, s.f.).

[74] Se establece que los juristas y teóricos del derecho deben de adoptar una *"consciencia tecnológica"*, término utilizado por Vittorio Frosini (profesor catedrático de derecho público comparado) como mentalidad necesaria para hacer frente a los cambios que suscitan las nuevas tecnologías (Pérez Luño, 2012).

internacional existente para ofrecer soluciones adecuadas ante estas nuevas formas de agresión[75]. Sobre todo, cuando estas tienen como objetivo las infraestructuras esenciales o la sociedad civil, así como por su complejidad al ser llevadas a cabo por actores estatales y no estatales que, en ciertas ocasiones, actúan bajo el anonimato, lo que genera una asimetría de poder sin precedentes (Rueda Villegas, Garza Piña y Ulloa Zamorano, 2025). El debate sigue abierto entre los que consideran suficiente el marco jurídico actual haciendo uso de una interpretación extensiva[76] del mismo y quienes, por otra parte, abogan por la creación de un marco jurídico específico que regule de forma clara y detallada todas las nuevas formas de agresión que puedan ir surgiendo. Por todo, se genera una inquietud por reflexionar, de forma crítica, sobre la aplicabilidad del derecho internacional a los ciberataques.

Sin embargo, el espectro de este análisis se centrará en la aplicabilidad del art. 51 de la CNU, en particular, en determinar cuáles son los tipos de ciberataques que, por su naturaleza, intensidad y efectos, podrían alcanzar los requisitos necesarios para ser considerados ataques armados, de forma que sea invocable jurídicamente el derecho de legítima defensa. Es así como conviene considerar que tal clasificación no es estática ni inamovible, destacando así la importancia del contexto actual de innovación digital[77]. Pues en virtud de la mejora y desarrollo tecnológico, este contexto altera continuamente los efectos, alcance, impacto y forma de los ciberataques. Por lo que, al ser un factor variable, también afectará su calificación jurídica. Por tanto, el objetivo final de este estudio es identificar bajo qué circunstancias puede aplicarse el art. 51 de la CNU en caso de un ciberataque y, en caso de que no proceda su aplicación, cuál sería la condición jurídica que tendría dicho ciberataque bajo el DIP. Esto es relevante, para analizar si cabría invocar, de forma jurídicamente válida, alguna de las circunstancias que excluyen la ilicitud bajo la responsabilidad internacional de los Estados.

A los efectos del presente artículo se tendrá en cuenta, dada su relevancia y estudio focalizado en materia de ciberataques, el Manual de Tallin[78]. Se trata de un estudio doctrinal financiado por la *"NATO Cooperative Cyber Defence Centre of Excellence"* (CCDCOE), realizado por un conjunto de expertos en Derecho Internacional. Sin

[75] No hay consenso y hay dos posiciones, la de EE. UU. y los países occidentales y la de Rusia, China y otros países. Los primeros abogan por la aplicación analógica mientras que los segundos por la creación de nuevas leyes (Quispe Remón, 2024; Serrano Segura, 2020).

[76] Amplía más allá de cierto punto el alcance (supuesto de hecho) o la prescripción (consecuencia jurídica) del precepto tal como lo da a entender su lenguaje. Sin embargo, es un concepto ambiguo. Para unos, corrige el significado literal sin desconocerlo. Mientras que, para otros, amplía y corrige el significado literal o incluso rebasa cualquier significado (González Ortega, 2019).

[77] A efectos de este trabajo, se entenderá como el Desarrollo de nuevos sistemas, métodos y herramientas digitales. Tales cambios han transformado la naturaleza de los conflictos desafiando los marcos normativos creados para conflictos tradicionales (BeeDIGITAL, 2020).

[78] Del mismo, hay dos versiones y una tercera en proceso (NATO Cooperative Cyber Defence Centre of Excellence, s.f.).

embargo, conviene tener en cuenta que no refleja un consenso ni se trata de un instrumento vinculante, sino que es un medio subsidiario para determinar las reglas existentes del Derecho Internacional en el marco de un ciberataque. En particular, porque analiza la práctica estatal en línea con estas nuevas realidades tecnológicas.

Para realizar tal estudio, conviene fijar unas definiciones para delimitar y entender adecuadamente el objeto de estudio.

En el presente artículo, por ciberataque se entenderá *"una operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause lesiones o muerte a personas o daños o destrucción a objetos"* de acuerdo con la regla 92 del Manual de Tallin 2.0 (Schmitt, 2017). Ello permitirá distinguir entre actos de agresión y meros incidentes cibernéticos. En esta línea, el término ataque armado ha sido definido por la jurisprudencia del Tribunal Internacional de Justicia (TIJ)[79] como *"(...) el envío por o en nombre de un estado de fuerzas armadas contra otro Estado ...de tal gravedad que equivaldrá (entre otras cosas) a un ataque armado real llevado a cabo por las fuerzas regulares, o su participación sustancial en él"*.

Finalmente, este artículo se divide en cuatro cuestiones centrales. Para ello, se examinará, en primer lugar, si un ciberataque puede justificar la válida invocación del derecho de legítima defensa. A continuación, se analizará si es necesario que concurra la atribución del ciberataque al Estado agresor como una condición necesaria para invocar este derecho. Con ello, se expondrán las consecuencias jurídicas que derivan de la no aplicación del artículo 51 de la CNU a un ciberataque. Así, por último, se reflexionará críticamente sobre la necesidad de adaptar o reformar el marco normativo internacional vigente.

2. Relación entre un ciberataque y el derecho de la legítima defensa del artículo 51 de la CNU

a. Breve introducción a la Legítima Defensa

Existen ciberataques que, efectivamente, constituyen un ataque armado en caso de alcanzar la intensidad requerida y mediante los cuales se hace uso de la fuerza, lo que a priori está prohibido por el artículo 2.4 de la CNU.

Una norma considerada ius cogens, es decir, que tiene carácter imperativo sobre cualquier otra norma del Derecho Internacional, tal y como establece el artículo 53 de la

[79] Sentencia del 26 de noviembre de 1984, Nicaragua c. Estados Unidos de América (Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua), párrafos del 187 al 201.

Convención de Viena sobre el Derecho de los Tratados, así como por la jurisprudencia del TIJ80 (Martín Escobar, 2023). Si bien la prohibición del uso de la fuerza prevista en el artículo 2.4 de la CNU constituye un pilar del orden jurídico internacional contemporáneo, los redactores de la Carta reconocieron la necesidad de prever una excepción limitada y controlada que permitiera a los Estados responder ante un ataque armado ilegítimo. Con ese fin se incluyó el artículo 51, que reconoce el derecho inherente de legítima defensa individual o colectiva en caso de que un Estado sufra un ataque armado, hasta tanto el Consejo de Seguridad adopte las medidas necesarias para mantener la paz y la seguridad internacionales.

A la vista de ese precepto se debe entender, de acuerdo con Alam-Pérez (2020), que la prohibición del uso de la fuerza y el derecho a la legítima defensa son dos caras de la misma moneda. En la que existe una relación indirectamente proporcional de ambos conceptos pues entre menor sea el alcance de la legítima defensa, mayor será el efecto de la prohibición del uso de la fuerza y viceversa.

b. Análisis del umbral de intensidad requerido

De acuerdo con el artículo 39 de la CNU el Consejo de Seguridad está encargado de determinar cuándo, entre otros aspectos, se han producido actos de agresión (Consejo de Seguridad de las Naciones Unidas – Oficina en México, s. f.). En este supuesto está previsto que los Estados puedan hacer uso de la legítima defensa. Incluso parte de la doctrina, a través de una interpretación extensiva de ese derecho, defiende también la aplicación de este derecho en aquellos supuestos donde la amenaza/ataque sea inminente (Martín Escobar, 2023). Sin embargo, tal y como se explicará, son los propios Estados los que valorarán si han sido víctimas de un acto de agresión de forma que, en su caso, evalúen cómo responder con el uso de la fuerza. Todo ello, como establece la Carta, es sin perjuicio del mandato conferido al Consejo de Seguridad para adoptar las medidas necesarias (incluyendo la de determinar si se trata de un uso legítimo de la fuerza). Para ello, cabe cuestionar lo siguiente: ¿se requiere un tipo de intensidad específica? Ello es relevante pues no todas las amenazas, ataques o agresiones activan la legítima defensa.

Para comenzar, el uso de la fuerza debe alcanzar un umbral de intensidad mínimo para ser considerado un ataque armado y, por ende, justificar la invocación del derecho de legítima defensa. El artículo 3(g) del anexo de la Resolución 3314 (XXIX) de la Asamblea General de la ONU de 1974 establece un listado de conductas que se considerarán como actos de agresión, salvo que el Consejo de Seguridad determine lo contrario. Esta caracterización como actos de agresión se funda en la "presunción prima facie del primer

[80] Sentencia del 26 de noviembre de 1984, Nicaragua c. Estados Unidos de América (Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua), párrafo 73.

uso de la fuerza", que prevé el artículo 2 in fine del mismo anexo, para calificar una conducta como un acto de agresión. Conforme con el TIJ[81], el cual ha reconocido el carácter consuetudinario del artículo 3(g) del anexo, es razonable entender que esta presunción (y la caracterización como actos de agresión) atrae también este valor jurídico. Esta presunción no depende únicamente del orden cronológico de los hechos, sino de la gravedad objetiva del acto. A modo de ejemplo, el primer disparo puede presumirse iuris tantum como acto de agresión, pero esta presunción puede ser desvirtuada por otras circunstancias relevantes.

Por consiguiente, el umbral mínimo de intensidad que activa el derecho de la legítima defensa exige que el acto supere las meras amenazas o usos limitados de la fuerza. Este umbral se define por la gravedad objetiva de la conducta y es sólo cuando un ciberataque o cualquier otra acción alcanza la magnitud y efectos equiparables a un ataque armado que se justifica invocar legítima defensa bajo el marco jurídico de la Carta.

Parte de la doctrina, establece que la acumulación de los efectos de varios ciberataques que, considerados individualmente no serían alegables para la ejecución de la legítima defensa, permitirían alcanzar el umbral requerido. Además, un ciberataque que cause una grave perturbación en sistemas e infraestructuras esenciales sí puede considerarse un ataque armado, pero, es casuístico. Pues habría que evaluar si se estaría produciendo un daño comparable al causado por medios convencionales, lo que eleva el ataque a uno en el que se hace uso de la fuerza y que constituye una violación del derecho internacional (Schmitt, 2017).

Definitivamente, el umbral mínimo para que un acto de agresión, incluido un ciberataque en caso de cumplir con los requisitos que se explicarán a continuación, active el derecho a la legítima defensa conforme al artículo 51 de la CNU es que constituyan un "ataque armado" en sentido estricto. Teniendo en cuenta la gravedad y efectos materiales dado que esta valoración depende de cada caso.

c. Criterios técnicos y jurídicos para determinar la aplicación del artículo 51 de la CNU

El artículo 51 de la CNU, que tipifica el derecho de los estados miembros a la legítima defensa, prevé lo siguiente:

[81] Página 14, párrafo 3 del caso Nicaragua (CIJ, Nicaragua c. Estados Unidos de América, Sentencia de 27 de junio de 1986) se encuentra en el contexto del artículo 3(g) de la Resolución 3314 (XXIX) de la Asamblea General de la ONU de 1974, que contiene la definición de "agresión". Además, a pesar de que no existe consenso que la totalidad de esta resolución se considere como reflejo de la costumbre internacional. Por ende, que tenga vocación de obligar. Aunque el TIJ ha reconocido que este carácter consuetudinario sí existe con respecto al artículo 3(g) del anexo, previamente mencionado.

> *"Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales"* (Naciones Unidas, s. f.).

En el citado precepto se tipifican los requisitos que debe cumplir un Estado para poder aplicar tal derecho una vez se ha constado que una ciberoperación tiene la consideración de ataque armado. De acuerdo con Domínguez Bascoy (2017), el citado precepto exige lo siguiente:

1) Constatar la existencia de un ciberataque, que a su vez constituya una violación del derecho internacional. De forma que la conducta sea atribuible al Estado, lo que le permitiría incurrir en responsabilidad (Schmitt, 2017).
2) Que la acción tenga carácter subsidiario a las medidas que, en su caso, pueda adoptar el Consejo de Seguridad de las Naciones Unidas y provisional (tiene que ser una respuesta temporal en función de la duración de la amenaza).
3) Deber de comunicación inmediata al Consejo de Seguridad sobre la ejecución de la legítima defensa, así como su forma y modo.

Por otra parte, el artículo 51 de la CNU no establece los requisitos o condiciones que debe reunir la acción consistente en la legítima defensa. Sin embargo, esta cuestión ha sido ampliamente abordada por el derecho consuetudinario y la jurisprudencia del TIJ. Se concretan en tres pilares fundamentales para analizar si las acciones del Estado defensor son legítimas:

1) Necesidad[82], que según el TIJ[83], consiste en que la acción del Estado defensor sea la última ratio. En otras palabras, la legítima defensa sólo es admisible cuando constituye la única vía disponible para repeler un ataque armado. En otras

[82] Se estableció junto al criterio de proporcionalidad cuando se aprobó la legítima defensa en los casos de armas nucleares (Corte Internacional de Justicia, 1996) y de esta doctrina junto a la expuesta en otros casos, como la disputa petrolífera entre Estados Unidos e Irán (Sentencia de 6 de noviembre de 2003 sobre el asunto de las Plataformas petrolíferas (República Islámica de Irán c. Estados Unidos de América)) (Corte Internacional de Justicia, 2003).

[83] Sentencia del 26 de noviembre de 1984, Nicaragua c. Estados Unidos de América (Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua), párrafo 102.

palabras, que no exista una alternativa menos gravosa o razonable. Esto implica que el uso de la fuerza únicamente estará justificado si otras vías jurídicas o diplomáticas han demostrado ser inviables o ineficaces.

2) Proporcionalidad, por lo que la intensidad del acto amparado por la legítima defensa debe ser acorde con la del ataque. No puede haber una respuesta desproporcionada, pues eso supondría la ilegitimidad de la acción. Por ende, la respuesta del estado defensor debe ser acorde, suficiente y razonable. Dado que el objetivo final de la legítima defensa es neutralizar la amenaza, no satisfacer un anhelo de revancha, el quantum entre la acción de ataque y la de defensa debe ser proporcional (Remiro Brotons et al, 2010).
3) Factor temporal[84], al que hace referencia parte de la doctrina (Martín Escobar, 2023): la inmediatez de la defensa. Pues si la acción no es inmediata al ataque podría considerarse una represalia más que un acto amparado en la legítima defensa. Sin embargo, en el contexto cibernético determinar el carácter proporcional y necesario de una contraofensiva es complejo. Cabe considerar que los efectos de los ciberataques no suelen ser inmediatos, sino que pueden manifestarse de forma diferida o acumulativa. En otras palabras, no sigue el modelo tradicional de "ataque–respuesta" propia del ius ad bellum. Por consiguiente, en este nuevo paradigma cibernético donde los conflictos ya no se limitan al espacio físico, se proyecta una necesidad de reinterpretar los criterios clásicos previamente explicados teniendo en cuenta las características técnicas de los ciberataques. También, hay otros requisitos que van más allá del ámbito material y pasan al formal:
4) La subsidiariedad del ataque –al que ya indirectamente se ha hecho mención–. En este caso, es porque se deberá comunicar al Consejo de Seguridad, sin perjuicio de las facultades de este órgano para actuar conforme a sus atribuciones. Aunque en la práctica, algunos Estados no cumplen con dicha obligación, esta omisión no afecta por si sola el derecho a la legítima defensa, si concurren los requisitos materiales exigibles por el derecho internacional. Sin embargo, tal incumplimiento sí puede constituir una violación del orden jurídico internacional y esta, en ningún caso, debe interpretarse como una exoneración de la supervisión del Consejo (Dinstein, 2017).
5) La provisionalidad, que consiste en que la legítima defensa debe llevarse a cabo mientras dure el ataque o amenaza inminente, no después. Por ende, aquella legítima defensa que se extienda más allá del ataque o amenaza inminente pasará a considerarse represalia y, por ende, ilegítima. Del mismo modo, podría haber casos de amenazas inminentes, aún sin disparos previos, que podrían ser

[84] Tal requisito tiene su origen en el "Caso Caroline", que fue una disputa diplomática entre los Estados Unidos de América y Reino Unido, ocasionada por el ataque de tropas británicas a un barco estadounidense —el Caroline—. A raíz de este caso se formuló que el principio la legítima defensa sólo es admisible si hay una necesidad instantánea, abrumadora y que no deje tiempo para deliberación (Academia Lab, s. f.).

suficientes para activar el derecho de la legítima defensa siempre que se cumplan con los requisitos previamente explicados (Vallarta Marrón, 2008).

Sin embargo, estos dos últimos requisitos sí se encuentran tipificados en el artículo 51 de la CNU.

d. Tipos de ciberataques

A los efectos de establecer el carácter jurídico de un ciberataque, conviene precisar su naturaleza y su diferencia respecto de una ciberoperación. Esta última consiste en actividades en las que se emplean capacidades cibernéticas para alcanzar unos determinados objetivos. De ahí viene que, es únicamente cuando estos objetivos consisten en la realización de un daño o en generar un perjuicio (económico, político o social), que nos encontraremos ante un ciberataque (Gutiérrez Espada, 2020).

Conviene avanzar que es necesario que los ciberataques sean llevados a cabo por un Estado, en su territorio o bajo la dirección del mismo, contra otro Estado para mantenernos en el objeto de estudio de este artículo. Pues si estos ataques son realizados por actores no estatales (y no es posible que tales ataques sean atribuibles a un Estado por no cumplirse los requisitos que después se analizarán) estaremos ante acciones calificadas como ciberterrorismo o ciberdelincuencia y la respuesta del Derecho frente a estos se encuentra fuera del ámbito del artículo 51 de la CNU (Cosgaya García, 2024).

A continuación, se explicarán los distintos tipos de ciberataques que se han identificado y si pueden constituir un ataque armado en virtud de los criterios previamente explicados:

1) *Denegación de actos de servicio (o Denial of Service (DoS)):* cuyo objetivo es impedir que un ordenador o dispositivo deje de estar disponible a través de la sobrecarga de solicitudes hasta que el tráfico normal no pueda ser procesado, por lo que este servicio dejará de estar disponible para los usuarios (Cloudflare, s.f.). En un principio, este tipo de ciberataques no alcanzaría el umbral de intensidad del art. 51 de la CNU, salvo que provoquen efectos en infraestructuras críticas como hospitales o centrales eléctricas. Por ejemplo, resulta relevante el caso de Estonia que sufrió este tipo de ciberataque repetidamente por parte del Gobierno ruso durante el 2007 que no resultó en daños físicos, pero sí una gran perturbación. Sin embargo, no se consideró que reuniera la intensidad necesaria para considerarse ataque armado, pues tan solo se consideró una interrupción corta periódica de servicios cibernéticos no esenciales (BBC News Mundo, 2017 y Kinast Werner, 2021). Aunque este suceso abrió el debate sobre si un ataque de esas características podría llegar a serlo en el futuro, sobre todo si sus efectos se

acumulan o afectan a infraestructuras críticas (aspectos que hoy en día sí se reconocen tal y como se explicó previamente) (Piernas López, 2024).

2) *Malware*: que consiste en todo tipo de software malicioso como, por ejemplo, los troyanos, gusanos o los virus (McAfee, s.f.). Este tipo de ciberataque podría, potencialmente, activar el artículo 51 de la CNU si produce una destrucción tangible y directa comparable a la de un ataque cinético (atacar desde el espacio una parte de la superficie). Un ejemplo clave es el caso Stuxnet contra el programa nuclear iraní (centrifugadoras nucleares) en el 2010, que también se relaciona con la actuación de actores no estatales (en este caso, un grupo terrorista). Este ciberataque en concreto consistió en la introducción de un malware muy sofisticado que logró sabotear las centrifugadoras nucleares iraníes ralentizando significativamente el programa de enriquecimiento de uranio del país. El Manual de Tallín 2.0 sí consideró que este ataque podía cumplir con el umbral requerido para ser considerado "ataque armado" y que, por consiguiente, permitiría activar el derecho de la legítima defensa, dado que se cumplen con los requisitos del TIJ (explicados previamente) (Obregón Fernández, 2023).
3) *Phishing*: método mediante el cual se engaña a la víctima para que, voluntariamente, realice una acción cibernética que, en principio, no haría libremente. Como, por ejemplo, compartir información confidencial (Universidad Pablo de Olavide, s.f.). Difícilmente se considerará un ataque armado, pues suele ser calificado como ciberdelincuencia o delitos de espionaje como, por ejemplo, el caso Cozy Bear (también conocido como "Caso de la campaña APT29") donde Rusia usó el Phishing para sabotear la campaña demócrata de los Estados Unidos durante las elecciones del 2016 (BBC Mundo, 2016). Pues este tipo de ataque no alcanza la intensidad requerida al no causar daños físicos o materiales. Por ende, este método, en términos prácticos, no puede llegar a ser un acto de agresión, sin perjuicio de que este tipo de operación sí pueda ser un paso previo a una operación cibernética que sí cumpla con los requisitos del TIJ.
4) *Inyección de código*: en los cuales un hacker inserta un código en la red para así quebrar las medidas de seguridad de un sistema informático o de un dispositivo conectado a la red con el objetivo de robar información del mismo (Ontek, s.f.). Dependiendo del efecto final puede o no considerarse "ataque armado". Aunque no se descarta que puedan ser la fase previa de una operación cibernética que sí pueda activar la legítima defensa, por ejemplo, si compromete datos e integridad de sistemas claves estatales, tal y como se explicó previamente. Un ejemplo, sería el ataque conocido como *SolarWinds* en el 2020 donde varias agencias estadounidenses se vieron afectadas. Sin embargo, se consideró un caso de ciber espionaje más no un ataque armado que activaba la legítima defensa, dado que no hubo daños materiales (por ende, sus efectos no son equiparables a los de un

ataque armado) y, además, Estados Unidos no invocó el artículo 51 de la CNU (El Confidencial, 2020).

5) *Fuerza bruta*: utilizado para descifrar claves o usuarios mediante un sistema de descarte probando distintas combinaciones (Keeper Security, s.f.). Difícilmente puede provocar efectos lo suficientemente intensos para considerarse un "ataque armado", pues es complicado que alcance la intensidad requerida y son considerados leves, pues se consideran preparatorios o una fase previa de una operación cibernética mayor. Por ende, no llegan a producir los efectos materiales necesarios para alcanzar el umbral requerido y, además, no cumplen con el principio de temporalidad (Schmitt, 2017).

Por ende, conviene tener en cuenta que la calificación jurídica de un ciberataque no depende únicamente del tipo de ataque, sino que hay que tener en cuenta la intensidad, efectos, y el contexto geopolítico en que se produce. Un mismo tipo de ciberataque puede no activar la legítima defensa si solo roba datos, pero sí ser considerado uso de la fuerza si causa destrucción material significante que sea comprable a los causados por un ataque armado tradicional. Por ello, resulta fundamental no analizar estos ataques en abstracto, sino en relación con sus consecuencias.

3. La atribución de responsabilidad por el ciberataque como condición para invocar la legítima defensa

a. Atribución directa vs. indirecta: el rol de actores no estatales

Conviene definir la diferencia entre la atribución directa e indirecta. Pues mientras la primera hace referencia a los casos en lo que un Estado utiliza la fuerza contra otro Estado; la segunda se refiere al supuesto en el que quien ejerce la fuerza es un actor no estatal, como, por ejemplo, grupos terroristas.

Según el TIJ[85], el derecho de legítima defensa reconocido en el artículo 51 de la Carta de las Naciones Unidas solo puede ejercerse frente a ataques armados imputables a un Estado, y no directamente frente a actores no estatales. Sin embargo, parte de la doctrina sostiene que también cabría invocar la legítima defensa cuando dichos actores no estatales cometen ataques armados desde el territorio de un Estado que los tolera o no actúa para impedirlos, postura de, por ejemplo, el jurista Yoram Dinstein[86]. Otra cosa, como se verá

[85] Opinión consultiva de 9 de julio de 2004 a solicitud de la Asamblea General de las Naciones Unidas: CONSECUENCIAS JURÍDICAS DE LA CONSTRUCCIÓN DE UN MURO EN EL TERRITORIO PALESTINO OCUPADO, párrafos 138 a 141.

[86] Fue un académico israelí y profesor emérito de la Universidad de Tel Aviv. Especialista en derecho internacional y una figura influyente y autoridad en la creación de leyes de guerra (Tel Aviv University, s. f.).

posteriormente, es si la acción de un actor no estatal puede ser atribuible al Estado a los efectos de justificar la legitimidad de la respuesta.

En cuanto al régimen de atribución, debe precisarse que al Estado se le imputan directamente las acciones llevadas a cabo por sus propios órganos o agentes, conforme a los artículos 4 y 5 de los Artículos de Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos (en inglés: *"Articles on Responsibility of States for Internationally Wrongful Acts"* (ARSIWA)). Por ende, es donde se tipifica la llamada atribución directa.

En el caso de actos cometidos por actores no estatales, también se aplican las normas de atribución establecidas en la ARSIWA para determinar una responsabilidad indirecta, por ejemplo, cuando el Estado no impide actividades ilícitas desde su territorio, tal y como se tipifica en los artículos 8 y 11. En tal supuesto, el Estado víctima podría reivindicar la legítima defensa u otras medidas de respuesta lícitas, de acuerdo con la jurisprudencia del TIJ[87], sin perjuicio de que la responsabilidad pueda variar en función de otros elementos (Vallarta Marrón, 2008).

b. Estándares de prueba en el derecho internacional: atribución razonable

Este apartado hace referencia a los criterios jurídicos que deben cumplirse para atribuirle a un Estado la responsabilidad por actos de fuerza –como los ciberataques– llevados a cabo por actores no estatales, como grupos terroristas o grupos armados desde el territorio de un Estado. Pero, el Estado no es el que ha disparado directamente. Por ende, se analizará qué condiciones se requieren para que sea legítimo y jurídicamente viable atribuir a un Estado la responsabilidad por actos de terceros a efectos de justificar una respuesta armada, como la legítima defensa.

La jurisprudencia mayoritaria ha establecido que el criterio para atribución de responsabilidad estatal por la conducta de actores no estatales es el control efectivo. Sin embargo, existen otros criterios jurisprudenciales o doctrinales, tales como, el control general ("*overall control*") y el estándar de atribución razonable.

El primero fue establecido por el TIJ en la sentencia del 26 de noviembre de 1984, *Nicaragua c. Estados Unidos de América*[88], donde se estipuló que para atribuir responsabilidad a un Estado por la conducta de actores no estatales se requería probar que

[87] Caso del Canal de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte v. Albania); fallo de 9 de abril de 1949, párrafo 121 y Caso de determinadas actividades realizadas por Nicaragua en la zona fronteriza (Costa Rica v. Nicaragua); fallo de 16 de diciembre de 2015, párrafo 97.
[88] Sentencia del 26 de noviembre de 1984, Nicaragua c. Estados Unidos de América (Caso relativo a las actividades militares y paramilitares en Nicaragua y contra Nicaragua), párrafo 99.

el Estado tenía un control directo sobre las operaciones de los citados actores. En este caso concreto, se consideró que Estados Unidos no tenía un control directo suficiente sobre los *contras* para atribuirle responsabilidad por sus actos. Este criterio está tipificado en el artículo 8 de los Artículos de Responsabilidad de los Estados por Hechos Internacionalmente Ilícitos (2001).

Por otra parte, el Tribunal Penal Internacional para la Antigua Yugoslavia (TPIY) estableció un régimen más flexible en el *"Caso Tadić"* (1999)[89], pues se estipuló que bastaba un control general sobre el actor no estatal –como, por ejemplo, apoyo financiero– para cumplir con el juicio de atribución, lo que se conoce en el ámbito del *ius ad bellum* como patrocinio plausible[90]. Por consiguiente, no se requiere probar un control directo sobre actos específicos, lo que reduce el estándar de prueba necesario.
Finalmente, hay parte de la doctrina y ciertos Estados, como Israel o Estados Unidos, que apoya el estándar de atribución razonable. Este, como se ha mencionado previamente, establece que, si un Estado tan solo tolera o consiente o incluso, si no impide manera activa las operaciones de actores no estatales contra otro Estado, se le puede atribuir responsabilidad por la agresión. No es un estándar reconocido universalmente, pero se ha utilizado para justificar acciones militares. Como, por ejemplo, la invasión de Afganistán del 2001, que, sin embargo, se consideró que no cumplía con los requisitos de necesidad, proporcionalidad e inmediatez para ser amparada por la legítima defensa (Novak Talavera, 2002).

Por ende, a pesar de cierto apoyo por parte de la doctrina al criterio del estándar de atribución razonable, el estándar de prueba se rige por el test de control efectivo, que es aceptado por el TIJ.

c. Obstáculos probatorios en el ciberespacio

Sin duda, uno de los desafíos para el Derecho internacional en relación con los ciberataques es la gran dificultad que supone conocer con certeza quién es el responsable de los mismos. Pues en lo que respecta a los conflictos tradicionales, resulta más sencillo identificar quienes son los agresores. Mientras que en el ciberespacio la identidad del autor de tales ataques puede permanecer oculta con ayuda de la tecnología y mediante técnicas como el *spoofing, proxy chaining o botnets*[91], que permiten esconder el

[89] Sentencia caso Dusko Tadic (Caso del Fiscal c. Duško Tadić). Fallo de la Sala de Apelación del Tribunal Internacional Penal para la Antigua Yugoslavia: 15 de julio de 1999, párrafo 70.
[90] Estrategia mediante la cual un Estado (u otro actor no Estatal) proporciona apoyo técnico, material o estratégico a una determinada operación sin dejar evidencia directa de su participación (Gaviria, C. y Jiménez-Leal, W., 2014).
[91] Spoofing: técnica mediante la cual se falsifica la identidad para ocultar al verdadero atacante. Proxy chaining: uso de varios servidores intermedios para enmascarar el origen real en el tráfico digital. Botnets:

verdadero origen del ataque y dificulta saber si se actuó en nombre o con apoyo de algún Estado (Tsagourias & Buchan, 2015). A esto, tal y como explica Schmitt (2013), se le conoce como: crisis de atribución en el uso de la fuerza. Por consiguiente, se dificulta aplicar el criterio de control efectivo establecido por el TIJ por la complejidad técnica y la falta de evidencia directa.

Finalmente, la recolección de evidencia técnica depende mayoritariamente de la colaboración de empresas privadas de ciberseguridad o de los equipos nacionales de inteligencia, a quienes no siempre les interesa compartir la información que poseen. Tal y como explica Schmitt (2013) esto puede deberse por motivos comerciales o asuntos de interés nacional. Otro obstáculo para tener en cuenta, serían las "falsas banderas" de las que hacen uso actores estatales y no estatales para dirigir la autoría a otro estado disminuyendo la fiabilidad de ciertas pruebas (Schmitt, 2017).

Esta falta de certeza ha llevado a algunos Estados a actuar de manera unilateral. Lo que ha derivado en atribuciones de responsabilidad politizadas o preventivas que, en la mayoría de las ocasiones, no respetan los principios de proporcionalidad, inmediatez o necesidad exigidos por la Carta de la ONU para ejercer la legítima defensa.

4. Implicaciones jurídicas de la no aplicabilidad del artículo 51 de la CNU

a. Alternativas normativas: contramedidas y actos de retorsión

Las contramedidas, reguladas en el capítulo II del texto *Responsibility of States for Internationally Wrongful Acts* (2001), se conocen en el *ius ad bellum* como aquellas acciones temporalmente ilícitas pero justificadas legalmente que un Estado puede adoptar en respuesta a una acción de otro Estado que viola alguna obligación internacional, con el objetivo de que cese dicha violación y que se repare el daño causado. En el caso de los ciberataques, existen las contramedidas cibernéticas que consisten en la interrupción temporal de servicios digitales o la imposición de sanciones tecnológicas, siempre que cumplan con los requisitos de proporcionalidad, necesidad y respetando la prohibición del uso de la fuerza (Piernas López, 2024).

Por otra parte, los actos de retorsión son actos lícitos que no violan el Derecho internacional, aunque hostiles, que un Estado realiza contra otro en represalia por sus acciones. Por ejemplo, la expulsión de diplomáticos, suspender cooperaciones económicas o limitar las acciones comerciales. Por ende, no consisten en conductas que

redes de dispositivos infectados que son controlados remotamente para ejecutar ataques coordinados entre sí (SecurityScorecard, 2025).

infringen el Derecho internacional en sí mismo, sino que se trata de una medida de presión (Brownlie, 2012).

Estamos ante dos alternativas a las que el Estado puede recurrir en caso de no cumplir con los requisitos de la legítima defensa.

También, cabe tener en cuenta que la OTAN advirtió en el 2021 que los ciberataques serían tratados de la misma manera que un ataque armado en lo relativo al artículo 5 del Tratado de la OTAN (Organización del Tratado del Atlántico Norte (OTAN), 2007), que tipifica la defensa colectiva[92]. Mediante el cual, cualquier ciberataque contra uno de los aliados, será considerado como ejecutado contra todos los demás y estos podrán tomar las medidas necesarias para defender al aliado víctima del ataque mediante el derecho de la legítima defensa reconocido en el artículo 51 de la CNU (ITUser. Centro de recursos, 2021).

b. El papel del Consejo de Seguridad de la ONU

Tal y como establece el artículo 51 de la CNU es el Consejo de Seguridad el encargado de supervisar la excepción de la prohibición del uso de la fuerza y, además, es quien se encarga de autorizar las acciones que constituyen la legítima defensa de los Estados. Esta circunstancia evidencia la importancia de este órgano, dado que su responsabilidad sobre materia de seguridad y paz internacional es primaria[93] (Martín Escobar, 2023). Todo ello sin perjuicio de que los Estados se reservaron la libertad de calificar qué actos consideran que deben responderse mediante el uso de la fuerza y cuáles no (Regueiro Dubra, 2012).

Por otra parte, su importancia radica en que, si por cualquier motivo alguno de los requisitos establecidos previamente sobre la aplicación del artículo 51 de la CNU no se cumple, los Estados miembros pueden acudir a la alternativa tipificada en el artículo 42 de la CNU. Este establece que el Consejo de Seguridad será el único órgano legitimado para invocar el uso de la fuerza de manera colectiva (con la excepción de la legítima defensa) cuando las medidas coercitivas (como sanciones) no diesen resultado. Por ejemplo, mediante operaciones para el mantenimiento de la paz o intervenciones militares bajo el mandato de la ONU (Vallarta Marrón, 2008).

[92] Conviene destacar que, aunque el artículo 5 del Tratado de la OTAN permite una respuesta colectiva ante un ataque armado contra uno de sus miembros, el ejercicio de la legítima defensa debe igualmente cumplir con los requisitos del artículo 51 de la CNU, incluyendo la notificación al Consejo de Seguridad y el cumplimiento de los umbrales de intensidad. Por consiguiente, la invocación automática del artículo 5 podría entrar en conflicto con otras previsiones del ordenamiento [si bien, tal análisis está fuera del objeto de estudio de este artículo].

[93] Opinión consultiva sobre "Ciertos gastos de las Naciones Unidas", emitida por el Tribunal Internacional de Justicia (TIJ) el 20 de julio de 1962. *Reports 962*, páginas 165 a 167.

Por último, el Consejo tiene la facultad de decidir si una declaración de agresión no se ha dado por considerar que no alcanza la intensidad necesaria, por ejemplo, por decidir durante la evaluación del hecho que las consecuencias no fueron los suficientemente graves[94]. Por ejemplo, en el caso de la operación israelí en Túnez en el año 1998[95], en el que se demostró que el Consejo puede abstenerse de calificar un acto como "agresión" si no cumple el umbral (Pezzano, 2024).

5. Reflexiones de lege ferenda. Modificación o innovación del marco jurídico actual

a. Efectos de lagunas normativas existentes

De acuerdo con Schmitt (2017), existen tres lagunas normativas relevantes: (i) la dificultad de aplicar los requisitos del conflicto armado a un ciberataque; (ii) la incertidumbre respecto al ámbito de aplicación territorial de un ciberataque y (iii) la inexistencia de instrumentos internacionales para codificar respuestas legítimas frente a ciberataques.

Se establece que la primera laguna se debe a la falta de claridad en cuanto a la definición de "conflicto armado" en el ordenamiento jurídico internacional. Por ello, aplicarlo a los ciberataques resulta sumamente complejo pues no se encuentran tipificados de manera expresa y estos por sí mismos difícilmente pueden alcanzar el umbral requerido para activar la legítima defensa. En estos casos, eso provoca que los Estados no cuenten con todas las alternativas legítimas de represalia que les ofrece el citado ordenamiento. Es una laguna importante, pues muchos ciberataques quedan excluidos del régimen jurídico aplicado a los conflictos armados a pesar de su gravedad y las consecuencias causadas.

La falta de regulación respecto a los ciberataques deja en evidencia una desconexión entre el desarrollo tecnológico y el marco jurídico actual.

Por ende, además de la falta de un ordenamiento específico, existe una incertidumbre geográfica. El ordenamiento reconoce una "zona de conflicto", pues el Derecho internacional se aplica a hostilidades delimitadas en un territorio específico. No obstante, esta delimitación espacial no es realista con el escenario de los conflictos actuales donde predomina el desarrollo tecnológico, incluidos los ciberataques. El clásico "principio de territorialidad" pierde efectividad. Pues las ciberoperaciones pueden ser ejecutadas desde terceros Estados, incluso desde Estados que no forman parte del conflicto. Por ende, se diluye la relación entre la clásica dicotomía entre territorio pacífico y aquel en conflicto generando lagunas normativas con respecto a la aplicabilidad espacial del Derecho

[94] Resolución de la Asamblea General de la ONU 3314 (XXIX) en el anexo "Definición de agresión".
[95] Resolución 611 de 25 de abril de 1988 del Consejo de Seguridad de las Naciones Unidas, en la cual no se utiliza el lenguaje del Art. 39 ni se invoca el Capítulo VII.

internacional la responsabilidad del Estado que podría alojar –incluso involuntariamente– a estos grupos o desde donde se realiza el ataque y el estatus jurídico de aquellos que actúan desde el extranjero –si bien, esta valoración trasciende el objeto de estudio de este artículo –.

Por otro lado, es relevante también la falta de mecanismos multilaterales confiables para establecer una represalia contra un ciberataque para responder colectivamente. Más allá de lo establecido por la OTAN (mencionado previamente) o la intervención del Consejo de Seguridad –que en muchas ocasiones está paralizado políticamente por el controversial poder de veto (Coalition for the International Criminal Court, 2015)– no hay un mecanismo especializado establecido para este tipo de ataques en específico. Siendo la principal consecuencia la creciente tendencia de los Estados afectados a ejercer acciones unilaterales al margen de la supervisión colectiva del sistema de seguridad internacional, poniendo en peligro el uso limitado y controlado del uso de la fuerza a través de ciberoperaciones. Todo lo que se suma a la inexistencia de un marco común que regule o legitime las reacciones estatales ante las mismas.

b. La evolución del debate: Hacia una futura convención de ciberconflictos

El incremento de las operaciones cibernéticas con implicaciones transfronterizas ha dejado en evidencia la insuficiencia del marco jurídico internacional actual. A pesar de que se han realizado esfuerzos notables, como es el Manual de Tallín –en sus distintas versiones– para consolidar las interpretaciones del Derecho existente con respecto al entorno digital actual. Pero, la comunidad internacional aún no ha adoptado un tratado vinculante que regule los conflictos armados en el ciberespacio. Por ende, el debate en la actualidad gira en torno a si hay necesidad de redactar una convención internacional que establezca normas vinculantes sobre qué conducta deben tener los Estados con respecto a los ciberataques. Incluyendo los umbrales de aplicación, especificar los principios de proporcionalidad y necesidad en el entorno digital, así como los mecanismos de atribución y responsabilidad estatal. Incluyendo el establecimiento de criterios funcionales y no únicamente formales para valorar la gravedad de los ciberataques atendiendo a su impacto real.

En los últimos años han surgido varias iniciativas sobre ciberseguridad en distintos foros internacionales, como la ONU, en particular el *"Group of Governmental Experts*"

(GGE)[96] y el *"Open-Ended Working Group"* (OEWG)[97]. No obstante, en la actualidad no se ha logrado un consenso sobre normas sustantivas, el proceso de codificación y la atribución de responsabilidad. Algunos autores, incluyendo Hollis (2011), sostienen que las divisiones geopolíticas y el temor a perder soberanía, autonomía y libertad operativa de determinados Estados son unos de los principales obstáculos para llegar a un consenso universal.

Casos como el de Estonia (2007) o el de *SolarWinds* (2020) demuestran la creciente necesidad de mecanismos internacionales efectivos de atribución de responsabilidad y que permitan ejecutar una respuesta colectiva que no deje a los Estados en una posición no solo vulnerable, sino reactiva que pueda hacer escalar el conflicto. Por consiguiente, una futura convención debe tener como objetivo garantizar la protección de los civiles y las infraestructuras, establecer criterios de atribución comunes y desarrollar procedimientos probatorios viables a través de la regularización del uso de la fuerza cibernética. Aún así, las dificultades no deben ser obviadas, por lo que los Estados deben primero tratar de encontrar un objetivo común que les incite a llegar a un consenso.

Como nota final, la CCDCOE se encuentra actualmente trabajando en el Manual de Tallin 3.0 que contendrá nuevas actualizaciones sobre la interpretación del marco jurídico aplicable a los ciberataques (NATO Cooperative Cyber Defence Centre of Excellence, s.f.).

6. Conclusiones

El presente artículo ha demostrado que, si bien el artículo 51 de la CNU puede ser aplicado a los ciberataques, esta posibilidad no es absoluta ni automática. La invocación del derecho a la legítima defensa solamente está justificada en aquellos casos en los que se alcance el umbral de intensidad necesario para ser equiparable al uso tradicional de la fuerza y cuya autoría pueda ser atribuida, directa o indirectamente, a un Estado. Por todo, la identificación de estos casos requiere un análisis casuístico que considere los efectos materiales, el contexto geopolítico y tecnológico en que se produce.

Asimismo, se ha evidenciado que el marco normativo actual contiene importantes lagunas relacionadas especialmente con la atribución de autoría, la ausencia de mecanismos

[96] Grupo de expertos que designados por los estados miembros que se reúnen bajo el mandato de la Asamblea General para discutir asuntos de ciberseguridad internacional y tratar de llegar a un consenso (United Nations Office for Disarmament Affairs (UNODA), s.f.).

[97] Foro establecido por la Asamblea General donde todos los estados tienen voz para discutir los principios, normas y reglas que regulan el comportamiento de estos en el ciberespacio. Su objetivo es prevenir los conflictos cibernéticos mediante el diálogo inclusive (United Nations Office for Disarmament Affairs (UNODA), s. f.).

multilaterales y la delimitación territorial de los conflictos en el ciberespacio. Esta insuficiencia normativa, en muchas ocasiones, obliga a los Estados a actuar unilateralmente, lo que debilita el marco jurídico que regula el uso de la fuerza.

Por ello, es una necesidad imperativa el repensar y adaptar los marcos jurídicos actuales a las particularidades de la Era Digital. Más específicamente, las futuras convenciones sobre ciberconflictos deberían establecer con claridad: (i) umbrales jurídicos, (ii) principios sustantivos comunes aplicables a los ciberataques y (iii) estándares probatorios. De esta manera, se podrán garantizar respuestas legítimas, proporcionadas y colectivas por parte de los Estados agredidos. Sin duda alguna, un esfuerzo en común será mucho más efectivo ante este tipo de ciberoperaciones y todas aquellas que emerjan en el futuro.

7. Referencias

Jurisprudencia

Opinión consultiva de 9 de julio de 2004 a solicitud de la Asamblea General de las Naciones Unidas: CONSECUENCIAS JURÍDICAS DE LA CONSTRUCCIÓN DE UN MURO EN EL TERRITORIO PALESTINO OCUPADO.
Opinión consultiva sobre "Ciertos gastos de las Naciones Unidas", emitida por el Tribunal Internacional de Justicia (TIJ) el 20 de julio de 1962.
Resolución 611 de 25 de abril de 1988 del Consejo de Seguridad de las Naciones Unidas.
Resolución de la Asamblea General de la ONU 3314 (XXIX).
Sentencia caso Dusko Tadic (Caso del Fiscal c. Duško Tadić). Fallo de la Sala de Apelación del Tribunal Internacional Penal para la Antigua Yugoslavia: 15 de julio de 1999.
Sentencia del TIJ de 6 de noviembre de 2003 sobre el asunto de las Plataformas petrolíferas (República Islámica de Irán v. Estados Unidos de América).
Sentencia del TIJ, fallo de 9 de abril de 1949. Caso del Canal de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte v. Albania).
Sentencia del TJI del 26 de noviembre de 1984 (Caso de Nicaragua v. Estados Unidos de América).
Sentencia del TJI, fallo de 16 de diciembre de 2015. Caso de determinadas actividades realizadas por Nicaragua en la zona fronteriza (Costa Rica v. Nicaragua).

Bibliografía

Alam-Pérez, B. (2020). "La Evolución de la legítima defensa de los Estados en el Derecho Internacional", en Transformaciones de los Conceptos Claves en Distintas Áreas del

Conocimiento Jurídico-Social, ed. Por María Teresa Montalvo Romero y Carlos Fernández Abad, 71-95, p. 76.

Brownlie, I. (2012). Principles of Public International Law (8th ed.). Oxford University Press. ISBN: 0199654174.

Corte Internacional de Justicia (1996). Legalidad de la amenaza o el empleo de armas nucleares, n.º 104, párr. 37 a 50.

Corte Internacional de Justicia (2003). Caso relativo a las plataformas petrolíferas (la República Islámica de Irán contra los Estados Unidos de América). N.º 106, párr. 37 a 52.

Costa, S., Cuzzocrea, F., & Nuzzaci, A. (2014). Use of the Internet in Educative Informal Contexts. Implication for Formal Education. Comunicar, 43, 163-171.

Dinstein, Y. (2017). War, Aggression and Self-Defence (6th ed.). Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781108120555. ISBN: 9781316641668.

Domínguez Bascoy, J. (2017). "Aplicación del derecho internacional humanitario a las operaciones en el ciberespaciol". p. 235. ISBN: 978-84-9119-870-3.

Gaviria, C. y Jiménez-Leal, W. (2014). Encuentros cercanos con argumentos del "tercer tipo": razonamiento plausible y probabilidad subjetiva como modelos de evaluación de argumentos. CRÍTICA. Revista Hispanoamericana de Filosofía, 46(137), 85–112. Disponible en: https://www.jstor.org/stable/24523119

González Ortega, M. (2019). La interpretación extensiva de la ley. Revista DERECHOS Y LIBERTADES, Núm. 40, Época II, pp. 67-108. ISSN: 1133-0937. DOI: 10.14679/1111.

Gutiérrez Espada, C. (2020). La responsabilidad internacional por el uso de la fuerza en el ciberespacio, Cizur Menor, Thomson-Reuters Aranzadi, p. 24.

Kreß, C., & Monsma, A. (2020). "Cyber Attacks, Attribution and the Use of Force in International Law." Journal of Conflict and Security Law, 25(2), 151–183.

Martín Escobar, R. (2023). El derecho a la legítima defensa de los Estados. Contexto histórico y requisitos del artículo 51 de la Carta de Naciones Unidas. DIGNITAS. REVISTA ON LINE DE DERECHOS HUMANOS Y RELACIONES INTERNACIONALES. Nº 6. p. 169. ISSN: 2605-2172.

Novak Talavera, F. (2002). La intervención de los Estados Unidos de América en Afganistán: ¿Hecho ilícito internacional? Agenda Internacional, 8(16), 21–39. DOI: https://doi.org/10.18800/agenda. Disponible en: https://www.google.com/url?sa=t&so

Obregón Fernández, A. (2023). Aplicabilidad del derecho a la legítima defensa contra el terrorismo internacional: el acto terrorista como ataque armado / Applicability of the right to self-defence against international terrorism: the terrorist act as an armed attack. Estudios de Deusto. Revista de Derecho Público, 71(2), julio-diciembre, pág. 6. DOI: https://doi.org/10.18543/ed.2929.

Piernas López, J. J. (2024). El Derecho internacional y las contramedidas cibernéticas (1.ª ed.). Tirant lo Blanch. Disponible en: https://editorial.tirant. ISBN: 978-84-1162-868-6.

Piernas López, J. J. (2024). Las medidas de autotutela frente a amenazas cibernéticas en derecho internacional: Especial referencia a la posible adopción de contramedidas colectivas / Self-help measures against cyber threats in international law: Special reference to the possible adoption of collective countermeasures. Cuadernos de Derecho Transaccional, 16(1), 798–828. DOI: 10.20318/cdt.2024.8412.

Quispe Remón, F. (2024). Los problemas ciber vistos desde el Derecho internacional. Un gran reto a enfrentar. Eunomía. Revista en Cultura de la Legalidad, 27, pp. 155-182.

Regueiro Dubra, R. (2012). La legítima defensa en derecho internacional, Madrid: Instituto Universitario General Gutiérrez Mellado – UNED, p. 92.

Remiro Brotons, A. et al. (2010). Derecho Internacional. Curso general. Tirant lo Blanch. p. 678-679. ISBN: 9788498769845.

Rueda Villegas, V., Garza Piña, E. and Ulloa Zamorano, R. (2025) "Pico- and nanosecond synchronized nonlinear magnetization dynamics of an isotropic nanomagnet under sinusoidal linear excitation," Academia Nano: Science, Materials, Technology. Academia.edu Journals, 2(1). DOI: 10.20935/AcadNano7610.

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press. ISBN: 9781139169288. DOI: https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. ISBN: 9781316822524. DOI: https://doi.org/10.1017/9781316822524

Serrano Segura, A. (2020). Ciberseguridad y normación en Derecho Interacional. Fundación Euroarabe, (5), p. 1-5.

Tsagourias, N., & Buchan, R. (2015). Cyber War and International Law. Edward Elgar Publishing. ISBN: 178254738X.

United Nations Office for Disarmament Affairs (UNODA). (s. f.). Open-Ended Working Group. Disponible en: https://disarmament.unoda.org/open-ended-working-group/

United Nations Office for Disarmament Affairs (UNODA). (s.f.). Group of Governmental Experts (GGE). Disponible en: https://disarmament.unoda.org/group-of-governmental-experts/

Webgrafía

Academia Lab. (s. f.). Asunto de Caroline. En Enciclopedia jurídica. Disponible en: https://academia

BBC Mundo. (2016). Qué se sabe sobre el ciberataque ruso contra las elecciones en Estados Unidos. BBC News Mundo. Disponible en: https://www.bbc.com/mundo/noticias-internacional-38350244

BBC News Mundo. (2017). Qué es el derecho a la legítima defensa que contempla la ONU y por qué es tan polémico. BBC. Disponible en: https://www.bbc.com/mundo/noticias-39800133

BeeDIGITAL. (2020). Innovación tecnológica: qué es, tipos y ejemplos. Disponible en: https://www.beedigital.es/tendencias-digitales/que-es-innovacion-tecnologica/

Cloudflare. (s.f.). Denegación de servicio (DoS). Cloudflare. Disponible en: https://www.cloudflare

Coalition for the International Criminal Court. (2015). La responsabilidad del derecho a veto en el Consejo de Seguridad de la ONU. Disponible en: https://www.coalitionfortheicc.org

Consejo de Seguridad de las Naciones Unidas – Oficina en México. (s. f.). Preguntas frecuentes. Disponible en: https://consejodeseguridad.onu.org.mx/el-consejo/preguntas-frecuentes/

Cosgaya García, E. (2024). Aplicación del Derecho Internacional a las operaciones en el ciberespacio [Trabajo Fin de Grado, Universidad de Valladolid]. UVaDOC. Disponible en: https://uvadoc.uva.es/bitstream/

Economipedia. (2024). Era digital: qué es y cómo ha transformado la economía y la sociedad. Disponible en: https://economipedia.com/definiciones/era-digital.html

El Confidencial. (2020). SolarWinds: el ciberataque que ha puesto en jaque a Estados Unidos, Microsoft o Cisco. Disponible en: https://www.elconfidencial.com/tecnologia/2020-12-22/

González Cussac, J. L. (2020). El ciberespacio como nuevo escenario del conflicto armado internacional: la necesidad de una respuesta jurídico-penal global. Universidad Complutense de Madrid. Disponible en: https://docta.ucm.es/rest/api/

Hollis, D. B. (2011). An e-SOS for Cyberspace. Harvard International Law Journal, 52(2), 373–430. Disponible en: https://journals.law.harvard.edu

ITUser. Centro de recursos. (2021). La OTAN advierte que considerará una respuesta militar a los ciberataques. Discover The New — Seguridad Inteligente. Disponible en: https://discoverthenew.

Keeper Security. (s.f.). Brute-force attack. Keeper Security Threats. Disponible en: https://www.keepersecurity.com/es_ES/threats/brute-force-attack.html

Kinast Werner, R. (2021). Disuasión y uso de la legítima defensa en el ciberespacio / Deterrence and use of self-defense in the cyberspace. Santiago de Chile: Instituto de Estudios Internacionales, Universidad de Chile. pp. 114–199. Disponible en: https://www.google.com/url?sa=t&source=

McAfee. (s.f.). ¿Qué es el malware y cómo puede protegerse? McAfee. Disponible en: https://www.mcafee.com/es-es/antivirus/malware.html

Naciones Unidas. (s. f.). Carta de las Naciones Unidas. Naciones Unidas. Disponible en: https://www.un.org/es/about-us/un-charter

NATO Cooperative Cyber Defence Centre of Excellence. (s.f.). CCDCOE to Host the Tallinn Manual 3.0 Process. Disponible en: https://ccdcoe.org/news/2020/

NATO Cooperative Cyber Defence Centre of Excellence. (s.f.). The Tallinn Manual. Disponible en: https://ccdcoe.org/research/tallinn-manual/

Ontek. (s.f.). ¿Qué es inyección de código? Disponible en: https://www.ontek.net/

Orellana, R. (2022). Qué es el Manual de Tallin y por qué es clave en una ciberguerra. Digital Trends Español. Disponible en: https://es.digitaltrends.com/computadoras

Organización del Tratado del Atlántico Norte (OTAN). (2007). Brussels Summit Declaration (2007). Disponible en: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Pérez Luño, A-E. (2012). "El derecho ante las nuevas tecnologías." El Notario del Siglo XXI, n.º 41. Disponible en: https://www.elnotario.es/revista

Pezzano, L (2024). La agresión en la práctica del Consejo de Seguridad. n.58. Disponible en: http://www.scielo.edu.uy/. ISSN: 0797-8316. DOI: https://doi.org/10.22187/rfd2024n58a5.

SecurityScorecard. (2025). What Are Proxy Browsers? How Cybercriminals Use Them In Attacks. SecurityScorecard. Disponible en: https://securityscorecard.com/

Tel Aviv University. (s. f.). Prof. Yoram Dinstein. Universidad de Tel Aviv. Disponible en: https://english.tau.ac.il/profile/dinstein

TEULP (2021). Dr. Cesáreo Gutiérrez Espada – Jean Monnet Chair. Universidad de Murcia. Disponible en: https://www.um.es/teulp/es/cesareo-gutierrez-espada-es/

Universidad Pablo de Olavide. (s.f.). ¿Qué es el phishing y cómo prevenirlo? Guías BibUpo. Disponible en: https://guiasbib.upo.es/ciberseguridad/phishing

Vallarta Marrón, J. L. (2008). La legítima defensa: ¿Es imprecisa la Carta de las Naciones Unidas o interpretaciones amañadas la deforman? ¿Es la defensa preventiva contra el terrorismo una norma in statu nascendi? Anuario Mexicano de Derecho Internacional, 8, 955–984. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542008000100040