

El desarrollo de la prohibición del uso de la fuerza: los ciberataques y el límite mínimo de intensidad

Manuel Marín Gastón

Universidad Nebrija

Fecha de presentación: julio 2025

Fecha de aceptación: abril 2026

Fecha de publicación: junio 2026

Resumen

La prohibición del uso de la fuerza es el pilar del orden internacional contemporáneo. Sin embargo, su alcance se ha definido a la par que surgían diferentes desafíos para la paz y la seguridad internacionales. Tras repasar el desarrollo de la norma, queda demostrado que hay preceptos bien afianzados y otros que son objeto de debate. En concreto, tanto la práctica y la jurisprudencia internacionales como la doctrina ofrecen argumentos a favor y en contra de la existencia de un límite mínimo de intensidad por encima del cual un hecho contravenga dicha prohibición. Frente a esta ambigüedad, el ámbito de los ciberataques emerge como escenario decisivo. A partir del análisis, la *opinio iuris* internacional sostiene que un número muy significativo de Estados identifica la gravedad (especialmente cuando existen efectos físicos o daños a infraestructuras críticas) como criterio determinante para calificar un ciberataque como uso ilícito de la fuerza.

Palabras clave

uso de la fuerza; agresiones híbridas; límite mínimo de intensidad

The development of the ban on the use of force: cyberattacks and the minimum intensity limit

Abstract

*The prohibition on the use of force is the cornerstone of contemporary international order. However, its scope has been defined as different challenges for international peace and security arose. After reviewing the development of the standard, it is demonstrated that there are well-established precepts and others that are the subject of debate. In particular, both international practice and jurisprudence and doctrine offer arguments for and against the existence of a minimum limit of intensity above which a fact contravenes such prohibition. Against this ambiguity, the cyberattack landscape emerges as a decisive scenario. Based on the analysis, the international *opinio iuris* holds that a very significant number of States identify severity (especially when there are physical effects or damage to critical infrastructure) as a determining criterion for classifying a cyberattack as an unlawful use of force.*

Keywords

use of force; hybrid aggressions; minimum intensity limit

Introducción

El desarrollo de la guerra está irremediablemente ligado al avance de la potencia de fuego de los Estados. Su capacidad destructiva fue evidente ya en las grandes batallas del siglo XIX; como la de Solferino en 1859, que sacudió los espíritus de la sociedad internacional. El sufrimiento humano de esta batalla marcó especialmente la conciencia de Henry Dunant, precursor de la *Convención de Ginebra de 1864* (Dunant, s.f.). Este tratado, considerado el germen del derecho internacional humanitario, constituyó el primer límite jurídico a la conducción de la guerra. A partir de entonces, la regulación de la fuerza durante el fulgor del conflicto (*ius in bello*) fue expandiéndose hasta finalmente excluir el derecho a utilizarla en las relaciones internacionales (*ius ad bellum*).

Este proceso estuvo influido por diferentes acontecimientos históricos, siendo las dos guerras mundiales las que tuvieron mayor impacto. Casi cuatro años antes de que finalizase la Segunda Guerra Mundial, los líderes de EE. UU. y Reino Unido expresaron su convicción de que «all of the nations of the world, for realistic as well as spiritual reasons must come to the abandonment of the use of force» (The Atlantic Charter, 1941). Ese compromiso se materializó en San Francisco (1945) con la firma de la Carta de las Naciones Unidas (CNU). Este tratado consagró los principios fundamentales que regirían las relaciones internacionales. De entre ellos, el objeto de este estudio es la prohibición del uso de la fuerza, consagrada en el artículo 2, párrafo 4 (art. 2.4), que reza:

«Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas».

Durante ochenta años, esta disposición ha constituido el pilar del orden internacional y ha permanecido formalmente inalterada. Sin embargo, es razonable afirmar que los desafíos contemporáneos a la paz y la seguridad tienen poco que ver con los que dieron origen al orden internacional. Es más, podría argüirse que el art. 2.4 nació desfasado respecto del contexto en el que debía aplicarse. Entre su firma y su entrada en vigor, las bombas sobre Hiroshima y Nagasaki transformaron el panorama de la seguridad internacional: la prohibición del uso de la fuerza fue concebida en un mundo prenuclear, pero debía

aplicarse en una era, para siempre, condicionada por la amenaza atómica.

Así, como veremos más adelante, la práctica y jurisprudencia internacionales han tenido que adaptar e interpretar la norma a la vez que surgían nuevos desafíos a la paz. Tanto es así que el primer caso de la Corte Internacional de Justicia (CIJ), *Corfu Channel*, asentó el amplio alcance de la prohibición, lo que excluye cualquier consideración que legitime el uso de la fuerza (salvo las excepciones previstas en la CNU).

Como queda detallado en el apartado 1 de este artículo, hay preceptos de la norma que todavía quedan por esclarecer. Uno de ellos es si existe un umbral mínimo de gravedad a partir del cual un hecho constituye un uso ilícito de la fuerza. Se trata de un requisito cuya existencia ha sido objeto de debate durante décadas. Esto se debe a que tanto la práctica como la jurisprudencia internacionales son tan heterogéneas que impiden afirmar con rotundidad su vigencia. Sin embargo, en el intento de los Estados por adaptar la prohibición del uso de la fuerza a los ciberataques, se está resolviendo este problema jurídico.

Este concepto de «ciberataque» carece de una definición consensuada. La Estrategia de Seguridad Nacional española de 2021 lo define como acciones disruptivas contra sistemas y elementos tecnológicos producidas tanto por actores estatales como no estatales (BOE, 2021). En el marco de la Unión Europea (UE), la decisión PESC 2019/797 entiende que los ciberataques atañen a una amplia categoría de acciones, pero enumera los siguientes como amenazas a los Estados: el acceso o intromisión a sistemas de información y a datos que afecten a las funciones vitales del Estado como son, principalmente, la defensa, el funcionamiento de las instituciones, las elecciones electorales, la seguridad interior y las misiones diplomáticas. Asimismo, también se considerará como ciberataque la acción contra las infraestructuras críticas y los servicios necesarios para el ámbito de la salud, la seguridad, el bienestar social, la energía, el transporte, el sector bancario y financiero, el suministro de agua potable, entre otros. En cuanto a lo aportado por la doctrina, un ciberataque es la acción que deliberadamente altera, interrumpe, engaña, degrada o destruye sistemas informáticos adversarios, así como la información o los programas que contienen (Lin, 2010; Gervais, 2012; véase también la definición publicada en la página web del gobierno australiano). En resumen, el concepto de «ciberataque» abarca una variedad de conductas

con distinta intensidad: desde el robo de información o el espionaje, hasta la paralización, la disfunción o la eliminación de infraestructuras y servicios críticos del Estado.

Como destaca Francisco Javier Roldán Barbero (2018), «la exégesis [de la prohibición del uso de la fuerza] debe ser adaptada al mundo de hoy», y el ámbito de los ciberataques ofrece el campo de pruebas adecuado para comprobar si efectivamente existe un límite mínimo de intensidad. En este contexto, en julio de 2025 concluyó el trabajo del Open-ended Working Group on security of and in the use of information and communications technologies. Se trata de un órgano cuyo fin ha sido elaborar «las reglas, normas y principios de comportamiento responsable de los Estados» en lo concerniente a la aplicación de las nuevas tecnologías de la información y la comunicación (A/RES/75/240, 2020). Su informe de julio de 2025 recoge la voz de los Miembros de la ONU y sus conclusiones plantean el fin del debate doctrinal.

En definitiva, este artículo sostiene que: es en el esfuerzo por adaptar el *ius ad bellum* a los ciberataques donde se comprueba que la mayor parte de la comunidad internacional acude a la gravedad de los hechos para discernir cuáles quebranta el principio de no uso de la fuerza. Para demostrarlo, el artículo aborda los siguientes apartados: tras la metodología, el apartado 2 establece la base material del análisis, es decir, define el alcance de la prohibición del uso de la fuerza y el problema jurídico que debe abordarse, a saber, el límite mínimo de gravedad. En el apartado 3 se descarta que el supuesto límite de intensidad se encuentre en hechos considerados de baja intensidad para finalmente llegar al ámbito de los ciberataques. En el apartado 4 se recoge toda la evidencia de la *opinio iuris* internacional con la que finalmente se elaboran las conclusiones.

1. Metodología

Para poder analizar la adaptación del principio de no uso de la fuerza a los ciberataques, este artículo adopta un enfoque normativo. En primer lugar, debe advertirse que esta norma tiene naturaleza convencional y consuetudinaria. Como estableció la CIJ en el caso *Military and Paramilitary Activities in and against Nicaragua* (*Actividades Militares en Nicaragua*), la CNU «by no means covers the whole area of regulation of the use of force», y añadió que el principio de no uso de la fuerza recogido en la Reso-

lución 2625 reflejaba su contenido consuetudinario (CIJ, 1986). En consecuencia, su alcance varía en función del ámbito en que se consagra.

La enmienda del art. 2.4 de la CNU está condicionada al proceso agravado previsto en los arts. 108 y 109 de la CNU. Por ello, la evolución convencional de la norma no resulta relevante para este trabajo. Sin embargo, el alcance de la costumbre depende de cómo muten sus elementos constitutivos, a saber, una práctica constante y uniforme, acompañada de *opinio iuris* (CIJ, 1950). La práctica estatal no debe entenderse solo como una conducta física. Dentro de este concepto también caben los actos verbales (Green, 2022). En cuanto a los requisitos de constancia y uniformidad, la CIJ desarrolló su contenido en los casos *North Continental Shelf* y *Actividades militares*. En el primero, señaló que cuando una nueva costumbre deriva de una norma convencional previa, el transcurso de un breve período de tiempo no impide su consolidación; circunstancia que resulta relevante para este estudio. En el segundo, excluyó la necesidad de que la práctica sea totalmente uniforme: basta con que sea general y rigurosa respecto de la norma.

Ahora bien, para esta investigación no sirve cualquier suerte de práctica estatal. Únicamente deben considerarse aquellas que reflejen la *opinio iuris* internacional. De acuerdo con el criterio de la Comisión de Derecho Internacional (CDI), el convencimiento jurídico de los Estados puede obtenerse de las declaraciones y publicaciones oficiales, la jurisprudencia o la correspondencia diplomática, entre otras (CDI, 2018). En consecuencia, la investigación se basará principalmente en fuentes primarias.

Debe matizarse, aun así, que no todas las declaraciones públicas sirven para averiguar la *opinio iuris* de los Estados. Algunas de ellas pueden tener naturaleza política sin implicaciones jurídicas directas, lo que condiciona un análisis individualizado del lenguaje. A este respecto, la doctrina coincide en que cuanto más preciso sea el mensaje, mayores implicaciones jurídicas se le podrán atribuir. Asimismo, es necesario tener en cuenta también el contexto. Por ejemplo: una protesta diplomática, cuya redacción suele someterse a sucesivas revisiones, posee un mayor valor jurídico que una declaración espontánea o en caliente (Green, 2022). Por último, la titulación de los comunicados también es relevante. Por ejemplo, cuando un documento oficial se titula «declaración», lo expuesto en él tendrá normalmente un carácter político (Dörr, 2019).

Por otro lado, la interdicción de la fuerza es una norma de *ius cogens*. Como indica el art. 53 de la Convención de Viena sobre Derecho de los Tratados, una norma imperativa es aquella reconocida como tal por la comunidad internacional y únicamente modificable por otra subsecuente del mismo carácter. Esto conlleva demostrar que la comunidad internacional respalda cualquier modificación de la norma. Según la CDI, esto no debe interpretarse *strictu sensu*, ya que si un exiguo número de Estados no reconoce su carácter imperativo, no supondrá un impedimento para considerarla como tal (CDI, 2019). Determinar la *opinio iuris* de 193 Estados es, sin duda, técnicamente complejo. Por ello, además de recopilar el mayor número posible de declaraciones unilaterales, resulta esencial atender a la práctica de las organizaciones internacionales, a los debates en sus órganos y a las resoluciones y decisiones adoptadas (Corten, 2021).

Como última consideración metodológica, es preciso exponer cómo se plantea determinar la existencia del umbral mínimo de intensidad. Una vez expuesto el punto de partida, esto es, lo que se entiende incontestablemente por uso ilícito de la fuerza, se procederá a un análisis de los hechos siguiendo una escala descendente de gravedad. Es decir, primero abarcaremos aquellos casos en los que la gravedad de la fuerza ha sido mayor. Si en estos no hay referencia alguna al límite mínimo, se seguirá buscando allí donde los hechos tengan una menor intensidad. Así sucesivamente hasta que se localice el momento en que los Estados apelan explícitamente a la gravedad como criterio para discernir si se ha usado o no la fuerza.

2. El alcance actual de la prohibición del uso de la fuerza

El contenido del art. 2.4 ha tenido que ser precisado desde su consagración. Incluso durante su redacción, el concepto de «fuerza» resultaba ambiguo. Si se acude a los trabajos preparatorios de la CNU, Brasil propuso que la coerción económica quedara comprendida bajo su paraguas, pero fue rechazado (Documents of the United Nations Conference on International Organization, 1945). Para sostener que la norma se refiere a la fuerza armada, es necesario interpretarla en conexión con otras partes de la CNU. En el preámbulo, por ejemplo, se excluyó el uso de «la fuerza armada sino en servicio del interés común». En esta misma línea, el art. 42 hace referencia a las fuerzas aéreas,

marinas o terrestres de los Estados; y el art. 44 permite identificar claramente su sentido armado: «Cuando el Consejo de Seguridad [(CSNU)] haya decidido hacer uso de la fuerza, antes de requerir a un Miembro que no esté representado en él a que provea fuerzas armadas [...]».

La práctica internacional ha ido perfilando el contenido de la norma a medida que han sucedido nuevos acontecimientos. Es más, el primer caso de la CIJ, *Corfú Channel*, sirvió para determinar el alcance amplio de la prohibición: Reino Unido, para legitimar sus actos de fuerza, alegó que no había violado la integridad territorial de Albania (CIJ, 1950); sin embargo, la Corte rechazó este argumento (CIJ, 1949). Efectivamente, el art. 2.4 debe interpretarse junto con el art. 2.3, que obliga a la resolución pacífica de todas las disputas internacionales. Asimismo, mediante las Resoluciones 2625 y 42/22 de la Asamblea General, los Miembros de la ONU excluyeron la posibilidad de invocar consideración alguna que justificase el uso de la fuerza.

De igual modo, las Resoluciones 2625 y 3314 ayudaron a delimitar el ámbito personal y territorial de la norma. De la primera resolución surten principalmente dos efectos: en primer lugar, que todos los Estados, no solo las partes de la CNU, deben abstenerse de usar la fuerza. En segundo lugar, que la fuerza no solo se proscribió entre Estados, sino también entre los Estados y los pueblos coloniales. En cuanto a la Resolución 3314, el Sexto Comité de la AGNU acordó que lo dispuesto en ella no afecta la autoridad del Estado dentro de su jurisdicción (A/9890, 1974). En otros términos, los usos de la fuerza dentro de la soberanía territorial quedan fuera del alcance del art. 2.4. Dicho esto, la costumbre ha restringido la capacidad del Estado en este aspecto. Como puede apreciarse en el laudo arbitral, S. S. *"I'm Alone"*, y en el fallo del Tribunal Internacional para el Derecho del Mar en el caso *MIV "SAIGA"*, los Estados deben emplear la fuerza dentro de la jurisdicción razonable, necesaria e inevitablemente (United Nations, 2006; ITLOS, 1999).

Las citadas resoluciones también desarrollaron el concepto de «uso indirecto de la fuerza». En la resolución 2625 se proscribió la organización, fomento, instigación o ayuda a grupos armados irregulares en sus acciones contra otro Estado. Y en la Resolución 3314 se enumeró como «agresión»: «[e]l envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza» que sean similares a los expuestos en los literales anteriores del art. 3 de dicha

resolución. A la luz de este precepto, la CIJ consideró en el caso *Military and Paramilitary activities in and against Nicaragua* que el envío de grupos armados constituye un ataque armado si sus efectos se equiparan a los producidos por fuerzas regulares. En cambio, la CIJ juzgó que la provisión de armas o la ayuda logística podían considerarse como usos de la fuerza o injerencias en los asuntos internos (CIJ, 1986).

La resolución 3314 incorpora, por tanto, un criterio de intensidad para diferenciar la agresión de otras formas de uso de la fuerza. Este mismo criterio se refleja en la propia definición de la agresión, descrita como «la forma más grave y peligrosa del uso ilegítimo de la fuerza» (A/RES/3314, 1974), así como en la definición del «crimen de agresión» contenida en el Estatuto de Roma (2010), que exige la preparación o el inicio de un «acto de agresión» con una «gravedad y escala» que «constituya una violación manifiesta» de la CNU. Según el juez Robinson (2015), la intensidad determina tanto la calificación de un hecho como uso de la fuerza o como acto de agresión. Por ello, sostiene que el criterio de gravedad previsto en la Resolución 3314 sirve como parámetro para determinar qué conductas constituyen usos ilícitos de la fuerza. A su juicio, cuanto más se comprometan los principios de la CNU y los elementos del Estado, más grave será la violación de la norma.

En la doctrina, Olivier Corten (2021) sostiene, apoyándose tanto en diversos episodios de la práctica internacional¹ como en la jurisprudencia de la CIJ,² que los Estados toman en consideración la gravedad al denunciar el quebrantamiento de la norma. En 2009, el *Independent International Fact-Finding Mission on the Conflict in Georgia* afirmó que «[t]he prohibition of the use of force covers all physical force which surpasses a minimum threshold of intensity». En una misma línea, Van Steenberghe (2011) arguye que, para identificar un uso ilícito de la fuerza, la gravedad es una variable más objetiva y segura que la intencionalidad de los hechos, que es subjetiva. Por último, Mary Ellen O'Connell (2022) sostiene que rebatir la existencia de un límite mínimo implicaría oponerse a la costumbre internacional. Critica así la postura de Tom Ruys (que se aborda en los párrafos siguientes). Según

la autora, Ruys se opone a las tesis defendidas por autores de referencia como Olivier Corten, Yoram Dinstein o Robert Kolb. Sin embargo, a continuación, se demuestra que la posición de estos dos últimos ha cambiado; lo que prueba que el debate sigue abierto.

Si bien es cierto que Kolb se alineaba con Corten en 2018, ahora toma una posición más mesurada. Reconoce que la parte de la doctrina que defiende la existencia del límite basa sus argumentos en una falta de práctica internacional. Es decir, en precedentes internacionales en los que no se invocó el art. 2.4 frente a actos de baja intensidad. Obtener conclusiones jurídicas a partir de una ausencia de práctica es metodológicamente complejo. Especialmente cuando el umbral que se pretende identificar es tan general que alberga diversas dimensiones: su existencia, dónde se encuentra, si puede aplicarse a todo tipo de fuerza, etc. Según él, la existencia de este umbral debe seguir debatiéndose (Kolb, 2024).

Tom Ruys (2014) también rechaza que se pueda extraer conclusiones jurídicas de la práctica internacional en la que se apoyan los anteriores autores. Por ejemplo, cuando Corten sostiene que la abducción de Adolf Eichmann no fue un uso ilícito de la fuerza por su levedad, Ruys lo rebate ofreciendo argumentos de peso. Que no fuese condenado como un uso ilícito de la fuerza pudo deberse, según él, a la obligación moral de juzgar a uno de los principales arquitectos de la solución final. Es contrario también a la interpretación en este sentido de la jurisprudencia. Para él, en el asunto *Corfú Channel* la CIJ no calificó las acciones británicas como actos de fuerza porque no era el objeto del litigio. Otro autor que rechaza la existencia de dicho límite es Yoram Dinstein (2018), quien directamente concluye: «no minimum degree of [violence] is postulated in article 2(4). [...] A *de minimis* threshold may indeed be read into the narrow term “armed attack”». Finalmente, Christine Grey (2018) sostiene que esta pluralidad de opiniones en la doctrina demuestra que la práctica internacional es heterogénea, por lo que no puede reconocerse una costumbre establecida.

También puede traerse a colación argumentos equidistantes entre ambas posturas. Claus Kress (2015), por ejem-

1. Como la abducción de Adolf Eichmann en 1960; el asesinato de Khalil Al-Wazir en 1988; el derribo de un avión comercial iraní en el mismo año o el de un avión militar pakistaní por misiles indios en 1999; entre otros.
2. *Corfú Channel*; *Military and paramilitary activities in Nicaragua*; entre otras.

plo, no afirma que la jurisprudencia haya identificado la existencia del límite, pero tampoco excluye tal posibilidad. En efecto, si se consulta la opinión de los jueces Owada y Robinson (2015), se comprueba que la CIJ no ha emitido un juicio definitivo: en el asunto *Certain Activities carried out by Nicaragua in the Border Area*, Costa Rica solicitó a la CIJ un pronunciamiento sobre los actos de fuerza cometidos por Nicaragua (CIJ, 2010). La Corte respondió señalando que ya había determinado que la presencia de militares nicaragüenses constituía una violación de la soberanía costarricense y, por tanto, decidió no examinar si dichos actos configuraban una ocupación militar contraria al art. 21 de la Carta de la OEA (CIJ, 2015). Ambos jueces criticaron la decisión del órgano sosteniendo que un análisis de la cuestión habría permitido delimitar con mayor precisión el eventual umbral mínimo de gravedad. Así las cosas, la Asociación de Derecho Internacional concluyó en 2018 que no hay evidencia suficiente para afirmar o negar la existencia de un umbral mínimo de intensidad (International Law Association, 2018). Desde entonces han transcurrido ocho años. Procede, por tanto, examinar el estado actual del debate.

3. El límite mínimo de intensidad

El objeto de este apartado es determinar en qué tipos de acciones se sitúa el umbral de intensidad, en caso de que exista. Para ello, se examinarán distintos escenarios, ordenados de mayor a menor gravedad. Un punto de partida adecuado sería el criterio de Finlandia:

«A minor use of force is not considered to violate the prohibition of the use of force [...]. Depending on the situation, this interpretation may apply for instance to cross-border 'police operations', [...]. The same is true for targeted killings in the territory of another state by means of drones or other targeted means» (Ministry for Foreign Affairs of Finland, 2015).

A propósito de los asesinatos selectivos, pueden citarse precedentes internacionales que contradigan lo anterior. En 1988, Túnez, el CSNU y otros Estados africanos condenaron como un acto de agresión el asesinato de Jalil al-Wazir, perpetrado por el Mosad (S/19789, 1988; S/PV.2809, 1988. S/RES/611, 1988). En 2018, el Reino Unido denunció que Rusia utilizó la fuerza al intentar asesinar a Sergei y Yulia Skripal en Salisbury (S/PV.8203. 2018). Del mismo modo, Irán condenó a EE.UU. por asesinar a Qasem Soleimani (S/2020/13. 2020).

Sin embargo, también hubo acontecimientos similares, la reacción ante las cuales fue más contenida. Por ejemplo, en 2008 Colombia eliminó a miembros de las FARC en Ecuador. Ecuador advirtió que, de repetirse, se quebrantaría el art. 21 de la Carta de la OEA (OEA: RC.25/doc. 7/08, 2008). Por su parte, la respuesta de la OEA fue ambigua. Aunque invocó los arts. 19, 21 y 28, se limitó a calificar los hechos como una violación de la soberanía ecuatoriana y a reafirmar el principio de inviolabilidad territorial frente a ocupaciones militares u otras medidas de fuerza (Ibíd).

Con menor intensidad que los asesinatos selectivos, cabe mencionar las abducciones transfronterizas. En este ámbito la práctica internacional también es poco clara. Por un lado, EE.UU. invocó el derecho a la legítima defensa cuando secuestró a Abu Khattalah (S/2014/417. 2014); lo que implica un reconocimiento implícito del recurso a la fuerza. Pero, por otro lado, en 2010 y 2014 el Líbano denunció que Israel vulneró su soberanía y otras normas básicas del derecho internacional al abducir a sus nacionales (A/64/656 - S/2010/74, 2010; A/64/853 - S/2010/351, 2010; A/68/876 - S/2014/326, 2014). Con una intensidad aún menor, las abducciones ejecutadas por órganos policiales tampoco permiten llegar a una conclusión definitiva. La abducción de Humberto Álvarez Machain por parte de la DEA en México no se calificó como uso de la fuerza (E/CN.4/1994/27, 1993; Mohit, 2006). En este ámbito, Olivier Corten expone dos episodios que, según él, serían usos de la fuerza. El primero aconteció en 1986, cuando agentes de la policía suiza penetraron en territorio francés en persecución de unos fugitivos y, en el transcurso de la operación, abrieron fuego. En respuesta, Francia se limitó a exigir explicaciones diplomáticas. El segundo caso se produjo en 1991, cuando la policía aduanera alemana procedió a la detención de un ciudadano neerlandés en territorio de los Países Bajos. Tampoco en esta ocasión se calificó la actuación como un uso ilícito de la fuerza (Corten, 2021). Ahora bien, si se sigue el criterio de Tom Ruys, cabría sostener que dichas calificaciones respondieron a otros factores distintos de la gravedad. El hecho de que estos episodios se produjeran entre Estados con relaciones amistosas (uno de ellos históricamente neutral) e involucraran a fuerzas policiales, y no militares, sugiere más bien la ausencia de *animus aggressionis*.

Sea como fuere, si se afirmara que las abducciones internacionales no alcanzan el umbral de uso de la fuerza, con mayor razón debería excluirse, por su menor gravedad, el mero cruce transfronterizo de unidades militares. En

este supuesto, la práctica internacional vuelve a ser notablemente diversa. En 2022, por ejemplo, la República de Corea invocó su derecho a la legítima defensa cuando diversas aeronaves norcoreanas cruzaron la línea de armisticio. (Arirang News, 2022). En 2005, en respuesta a Uganda, la República Democrática del Congo aseguró que amenazar con cruzar la frontera quebranta el art. 2.4 de la CNU (S/2005/620, 2005). Si finalmente se hubiese materializado, supondría *a fortiori* un uso ilícito de la fuerza.

Con todo, también pueden traerse a colación reacciones que apelaron a la violación de otras normas internacionales. Por ejemplo, cuando Bielorrusia utilizó la migración como arma contra Polonia, dos soldados bielorrusos se adentraron en territorio polaco. Polonia objetó que el traspaso violó su soberanía (Ministry of Foreign Affairs Republic of Poland, 2021). Durante el conflicto armado en el Cáucaso, Azerbaiyán denunció la contravención del acuerdo de alto al fuego cuando soldados armenios se adentraron en su territorio (A/75/791 - S/2021/212, 2021). La falta de referencia a la interdicción de la fuerza en estos acontecimientos pudo deberse, no obstante, al interés en evitar una escalada del conflicto. Polonia, en concreto, destacó la necesidad de invertir en diplomacia preventiva para abordar riesgos para la seguridad que están a punto de convertirse en un «conflicto militar abierto». Expuso, como ejemplo de lo anterior, la agresión híbrida perpetrada por Bielorrusia (S/PV.8906 (Resumption 1), 2021).

La práctica internacional es, como aseguran ciertos autores, variada. No puede afirmarse, por tanto, que en este ámbito se identifique con claridad un umbral mínimo de intensidad. Sin embargo, la necesidad de adaptar el derecho internacional a los nuevos desafíos está contribuyendo a disipar toda esta ambigüedad. Es en el contexto de los ciberataques donde un mayor número de Estados reconoce explícitamente la gravedad como variable que permite identificar un uso ilícito de la fuerza. Por ejemplo, Alemania ha señalado dos circunstancias en las que «[c]yber operations can cross the threshold into use of force»: primero, cuando se integra en un ataque cinético mayor; segundo, cuando por sí mismas causan daños graves o numerosas víctimas (The Federal Government, 2021). Esta opinión no es aislada, sino que la comparten últimamente múltiples Estados.

4. Los ciberataques y el límite mínimo de intensidad

La idea de que un ciberataque constituye uso de la fuerza cuando sus efectos son homologables a los de la fuerza cinética cuenta con el respaldo de un amplio conjunto de Estados: Finlandia (Finnish Government, 2015), Francia, Italia (United Nations Office for Disarmament Affairs [UNODA], 2021), Austria, Vietnam, Ecuador, Liechtenstein (S/2021/621, 2021), Singapur, Sudáfrica, Australia, Nueva Zelanda, (UNODA, 2023), Brasil, Bolivia, Estados Unidos, Canadá (CJI/doc. 671/22 rev.2 corr.1, 2022), Suecia (Government Office of Sweden, 2023), Israel (Mission of Israel to the UN in Geneva, 2021), Polonia (GOV.PL, 2022), Estonia (ERR NEWS, 2019), Noruega (Government.no, 2021), Reino Unido (United Kingdom Mission to the UN, 2021) y Sri Lanka (S/2023/412, 2023). De las posiciones de todos ellos se desprende, además, que un ataque contra infraestructuras críticas constituiría un indicador de gravedad suficiente. Sri Lanka, por ejemplo, apunta que en tal caso se puede responder en legítima defensa. Asimismo, la OTAN ha comunicado que, si un ciberataque alcanza una gravedad equivalente a la de un ataque armado convencional, podría activarse el art. 5 del Tratado de la Organización (NATO, 2016). Por su parte, Mozambique matiza que, si bien se registra con frecuencia una pluralidad de ciberataques, solo unos pocos han llegado a superar el umbral del uso de la fuerza (S/2023/412, 2023).

Otros como Chile (Diario Oficial De La República De Chile, 2018), Egipto (A/C.1/68/PV.20, 2013), China, Rusia, la UE, a cuya declaración se adhieren Túnez, Macedonia del Norte, Montenegro, Albania, Bosnia-Herzegovina, Ucrania, Moldavia, Irán, República Checa (S/2021/621, 2021), Cuba (Representaciones Diplomáticas De Cuba En El Exterior, 2023), Tailandia (Permanent Mission of Thailand to the United Nations, 2023), Pakistán (UNODA, 2023), Kazajistán, Kirguistán, Tayikistán, Uzbekistán (A/69/723, 2015), Suiza (Federal Department of Foreign Affairs FDFA, 2021), Japón (Ministry of Foreign Affairs of Japan, 2021), Tanzania (AALCO/59/HONG KONG/2021/SD/S17, 2021), Rumania, Siria (United Nations, 2023), Irán y el Movimiento de Países No Alineados (MPNA) (A/75/816, 2021) sostienen que los ciberataques pueden vulnerar la prohibición del uso de la fuerza. Pero a diferencia de los anteriores, no precisan que sea necesario superar un umbral de intensidad o que conlleven determinadas consecuencias. Ello no implica necesariamente que lo consideren irrelevante: China, Japón, Tanzania, la UE e Irán han alegado que

ciertos ciberataques pueden infringir varias normas internacionales. Esto sugiere que la intensidad opera como variable determinante para distinguir, por ejemplo, una violación del principio de no injerencia de una violación de la prohibición del uso de la fuerza. Una interpretación que no debe estar lejos de la verdad al comprobar que en 2024 el Consejo de la UE declaró:

«*Depending on the circumstances, the combined effects of several cyber operations could, taken together, be comparable to a kinetic use of force. Whenever the scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it constitutes a use of force within the meaning of Article 2 (4) of the UN Charter*» (énfasis añadido. Council of the European Union, 2024).

Una gran parte de todas estas opiniones han sido expresadas en el foro del *Open-ended Working Group on security of and in the use of information and communications technologies*. Como hemos indicado en la introducción, su mandato concluyó en julio de 2025. Durante cinco años ha aglutinado la voz de los Miembros de la ONU en relación con los ciberataques. En diciembre, la AGNU adoptó sin votación la resolución por la que hizo suyo el informe final del grupo (A/RES/80/16, 2025). En él se reafirma el art. 2.4 de la CNU, y se destaca que el uso de las «ICTs that does not amount to a violation of the prohibition on the threat or use of force may, depending on the circumstances, be contrary to other principles of international law» (énfasis añadido. A/80/257, 2025). Aunque menos explícito que la declaración de la UE, el informe refleja que la posición general de la ONU admite que ciertos ciberataques equivalen, según las circunstancias, a un uso de la fuerza, lo que presupone la existencia de un umbral en el que la gravedad juega un papel relevante.

Conclusión

El alcance del principio de no uso de la fuerza ha evolucionado a la par que lo hacían los desafíos internacionales. Hay preceptos de la norma que gozan de consolidación y otros, por el contrario, siguen siendo controvertidos. Entre ellos, la posibilidad de que exista un límite mínimo de intensidad como requisito para que un hecho quebrante la prohibición.

El debate doctrinal en torno a la cuestión ofrece argumentos a favor y en contra igualmente valiosos. De esta di-

cotomía es complejo sacar conclusiones definitivas; pero se obtienen dos ideas principales: primero, la práctica internacional ha sido, hasta el momento, heterogénea, lo que impide afirmar el reconocimiento universal del límite de intensidad. Segundo, se trata de un criterio jurídico cuya existencia, empero, no puede descartarse. Toda esta ambigüedad parece estar cambiando en el ámbito de los ciberataques y de la necesidad de hacerles frente.

La aportación principal de este artículo es el compendio de fuentes que permiten diagnosticar el estado de la *opinio iuris* internacional respecto del límite mínimo de intensidad. Se ha observado que el número de Estados que reconocen los ciberataques como uso ilícito de la fuerza es significativo: al menos 152 de 193 Estados miembros de la ONU (120 Estados pertenecientes al MPNA, los miembros de la OTAN, más China, Rusia, Australia y Nueva Zelanda). De entre estos, solo 39 (los 27 miembros de la UE más Vietnam, Ecuador, Singapur, Sudáfrica, Australia, Nueva Zelanda, Brasil, Bolivia, EE. UU., Canadá, Israel, Reino Unido y Mozambique) identifican expresamente la gravedad como criterio para calificar determinados ciberataques como uso de la fuerza. En efecto, se trata de una cifra reducida que no permite afirmar que el criterio esté consolidado en el derecho internacional. No obstante, no debe descartarse que otros Estados compartan implícitamente esta posición. Por ejemplo, sin emplear expresamente el término «umbral», algunos sostienen que un ciberataque constituirá uso de la fuerza cuando sus efectos se equiparen a los de la fuerza convencional. Asimismo, una gran variedad destaca que, si las infraestructuras críticas del Estado quedan comprometidas, el ciberataque contravendría el art. 2.4 de la CNU. Este tipo de declaraciones debe tenerse en cuenta como prueba de la progresiva consolidación del umbral en la costumbre internacional. Por último, es realmente significativo que los miembros de la AGNU hayan hecho suyo el informe final del *Open-ended Working Group on security of and in the use of information and communications technologies*. Su aprobación por consenso demuestra el convencimiento internacional al respecto.

En síntesis, es en el ámbito de los ciberataques donde se está resolviendo el problema jurídico del umbral de gravedad. No puede afirmarse con rotundidad que se trate de una costumbre ya establecida, pero la evidencia demuestra que el convencimiento general apunta a este fin. Entre tanto, quedan muchas otras cuestiones por definir. Como sostiene Robert Kolb, no basta con demostrar que

los Estados tienen en cuenta la gravedad, sino también dónde se encuentra específicamente. Aunque hay Estados que lo sitúan en el momento en que se comprometen sus infraestructuras o servicios críticos, este necesita perfilarse. Asimismo, todo esto implica nuevos retos para la gobernanza del ciberespacio, por ejemplo: la dificultad de atribuir un ciberataque; determinar cómo pueden contrarrestarse proporcionalmente; o reducir la incertidumbre en el ciberespacio.

Referencias bibliográficas

- AGNU (1970). «Declaración sobre los Principios de Derecho Internacional Referentes a las Relaciones de Amistad y a la Cooperación entre Estados de Conformidad con la Carta de las Naciones Unidas», A/RES/2625 (XXV).
- AGNU (1974). «Definición de la agresión», A/RES/3314(XXIX).
- AGNU (1974). «Report of the Special Committee on the Question of Defining Aggression», A/9890, párr. 10.
- AGNU (2010). «Cartas idénticas de fecha 2 de febrero de 2010 dirigidas al Secretario General y al Presidente del CSNU por el Representante Permanente del Líbano ante las Naciones Unidas», A/64/656 - S/2010/74.
- AGNU (2010). «Cartas idénticas de fecha 29 de junio de 2010 dirigidas al Secretario General y al Presidente del CSNU por el Representante Permanente del Líbano ante las Naciones Unidas», A/64/853 - S/2010/351.
- AGNU (2013). «AGNU Documentos oficiales, 68º período de sesiones: 1ª comisión, 20ª sesión plenaria», A/C.1/68/PV.20, pág. 29.
- AGNU (2014). «Cartas idénticas de fecha 8 de mayo de 2014 dirigidas al Secretario General y al Presidente del CSNU por el Representante Permanente del Líbano ante las Naciones Unidas», A/68/876 - S/2014/326.
- AGNU (2015). «Carta de fecha 9 de enero de 2015 dirigida al Secretario General por los Representantes Permanentes de China, la Federación de Rusia, Kazajistán, Kirguistán, Tayikistán y Uzbekistán ante las Naciones Unidas», A/69/723.
- AGNU (2020). «Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional», A/RES/75/240.
- AGNU (2021). «Carta de fecha 2 de marzo de 2021 dirigida al Secretario General por el Representante Permanente de Azerbaiyán ante las Naciones Unidas», A/75/791 - S/2021/212.
- AGNU (2025). «Developments in the field of information and telecommunications in the context of international security», A/80/257, pág. 13.
- AGNU (2025). «Grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), establecido en virtud de la resolución 75/240 de la Asamblea General», A/RES/80/16.
- Amendments to the Rome Statute of the International Criminal Court on the crime of aggression*. Kampala, 11 de junio de 2010, Serie de Tratados de las Naciones Unidas, núm. 38544.
- ARIRANG NEWS (2022). «Yoon calls N. Korean drone intrusion “utterly unacceptable”». *Youtube* [en línea]. Disponible en: <https://www.youtube.com/watch?v=rzACXWbJm14>. [Fecha de consulta: 4 de julio de 2025].
- ASIAN-AFRICAN LEGAL CONSULTATIVE ORGANIZATION (2021). «International Law in Cyberspace», AALCO/59/HONG KONG/2021/SD/S17, pág. 5.
- AUSTRALIAN GOVERNMENT (s.f.). «Cyber attack». ASD [en línea]. Disponible en: <https://www.cyber.gov.au/glossary/cyber-attack>. [Fecha de consulta: 13 de febrero de 2026].
- BARBERO, F. J. (2018). «El principio de prohibición del uso de la fuerza armada y la posverdad». En: *Principio y Justicia en el Derecho Internacional*, págs. 90-91. Madrid: Dykinson S. L. DOI: <https://doi.org/10.2307/j.ctv9hvtkb.10>
- Carta de las Naciones Unidas, San Francisco, 26 de junio de 1945.
- Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Application instituting proceedings, 2010, párr. 41.
- Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports, 2015, párr. 99.
- Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Separate Opinion of Judge Owada, I.C.J. Reports 2015, párr. 11.

- Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Separate Opinion of Judge Robinson, I.C.J. Reports 2015, párr. 47.
- Colombian-Peruvian asylum case. Judgment of November 20th 1950: I.C.J. Reports 1950. pág. 266, pág. 15.
- COMITÉ JURÍDICO INTERAMERICANO (2022). «Informe del Comité Jurídico Interamericano. Segundo informe: el derecho internacional aplicable al ciberespacio», CJI/doc. 671/22 rev.2 corr.1, pág. 18.
- CONSEJO ECONÓMICO Y SOCIAL (1993). «Informe del Grupo de Trabajo sobre la detención arbitraria», E/CN.4/1994/27, pág. 154.
- Convención de Viena sobre Derecho de los Tratados, de 23 de mayo de 1969, Serie de Tratados de las Naciones Unidas, vol. 1155, núm, 18232, pág. 331.
- Corfu Channel case, Judgement of April 9th, 1949: I.C.J. Reports 1949, pág. 4, pág. 6. DOI: <https://doi.org/10.18356/9789211544947c001>
- Corfu Channel Case, pleadings, oral arguments, documents, vol. III, 1950, pág. 296.
- CORTEN, O. (2021). *The Law Against War: the prohibition on the use on the use of force in contemporary law*, págs. 65, 76-90, 90. 2.ª ed. Oxford: Hart Publishing. DOI: <https://doi.org/10.5040/9781509949021>
- COUNCIL OF THE EUROPEAN UNION (2024). «Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace», 15833/24, pág. 6.
- CSNU (1988). «Acta taquigráfica provisional de la 2809ª sesión celebrada en la Sede, Nueva York», S/PV.2809.
- CSNU (1988). «Carta de fecha 16 de abril de 1988 dirigida al secretario general por el representante permanente del Irak ante las Naciones Unidas», S/19789.
- CSNU (1988). «Resolution 611 (1988) / adopted by the Security Council at its 2810th meeting», S/RES/611.
- CSNU (2005). «Carta de fecha, 3 de octubre de 2005, dirigida al Presidente del CSNU por el Representante Permanente de la República Democrática del Congo ante las Naciones Unidas», S/2005/620.
- CSNU (2014). «Carta de fecha 17 de junio de 2014 dirigida al Presidente del CSNU por la Representante Permanente de los Estados Unidos de América ante las Naciones Unidas», S/2014/417.
- CSNU (2018). «CSNU, 73º año: 8203ª sesión», S/PV.8203, pág. 2.
- CSNU (2020). «Carta de fecha 3 de enero de 2020 dirigida al Secretario General y a la Presidencia del CSNU por el Representante Permanente de la República Islámica del Irán ante las Naciones Unidas», S/2020/13.
- CSNU (2021). «Carta de fecha 1 de julio de 2021 dirigida al Secretario General y a los Representantes Permanentes de los miembros del CSNU por la Presidencia del CSNU», S/2021/621, págs. 15, 32, 38, 41, 48, 68.
- CSNU (2021). «Consejo de Seguridad, 76º año: 8906ª sesión», S/PV.8906 (Resumption 1), pág. 21.
- CSNU (2023). «Carta de fecha 6 de junio de 2023 dirigida a la Presidencia del Consejo de Seguridad por el Representante Permanente de Albania ante las Naciones Unidas», S/2023/412, págs. 33 y 72.
- Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros.
- Diario Oficial de la República de Chile*, núm. 42.003, de 9 de marzo de 2018.
- DINSTEIN, Y. (2018). *War, Aggression and Self-Defence*, págs. 90-91. 6.ª ed. Cambridge: Cambridge University Press. DOI: <https://doi.org/10.1017/9781108120555>
- Documents of the United Nations Conference on International Organization*, vol. VI, 1945, págs. 334-335, 459.
- DÖRR, O. (2019). «Declaration». *Max Planck Encyclopedias of International Law*, párr. 8 [en línea]. Disponible en: <https://www.mpil.de/de/pub/forschung/nach-rechtsgebieten/voelkerrecht/max-planck-encyclopedia.cfm>
- DUNANT, H. (s.f.). *A Memory of Solferino*, págs. 105-146. Ginebra: American Red Cross.

- ERR NEWS (2019). «President Kaljulaid at CyCon 2019: Cyber attacks should not be easy weapon». *ERR* [en línea]. Disponible en: <https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon>. [Fecha de consulta: 3 de julio de 2025].
- FEDERAL DEPARTMENT OF FOREIGN AFFAIRS FDFA (2021). *Switzerland's position paper on the application of international law in cyberspace*, pág. 4.
- FINNISH GOVERNMENT (2020). *International Law and cyberspace: Finland's nations positions*, pág. 6 [en línea]. Disponible en: <https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf>. [Fecha de consulta: 3 de julio de 2025].
- GERVAIS, M. (2012). «Cyber Attacks and the Laws of War». *Journal of Law & Cyber Warfare*, Vol. 1, pág. 63. DOI: <https://doi.org/10.2139/ssrn.1939615>
- GOVERNMENT OFFICE OF SWEDEN (2023). *Position Paper on the Application of International Law in Cyberspace*, pág. 4.
- GOVERNMENT.NO (2021). «Norwegian Positions on Selected Questions of International Law relating to Cyberspace». *Norway*, pág. 5 [en línea]. Disponible en: https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf. [Fecha de consulta: 3 de julio de 2025].
- GRAY, C. (2018). *International Law and the Use of Force*, pág. 37. 4.ª ed. Oxford: Oxford University Press.
- GREEN, J. A. (2022). «The Rise of Twiplomacy and the Making of Customary International Law on Social Media». *Chinese Journal of International Law*, Vol. 21, págs. 14 y 34. DOI: <https://doi.org/10.1093/chinesejil/jmac007>
- Independent International Fact-Finding Mission on the Conflict in Georgia*, 2009, Vol. II, pág. 242.
- INTERNATIONAL LAW ASSOCIATION (2018). *Final Report on Aggression and Use of Force*.
- KOLB, R. (2018). *International Law on the Maintenance of Peace*, págs. 336-337. 1.ª ed. Cheltenham: Edward Elgar Publishing.
- KOLB, R. (2024). «Article 2(4)». En: *The Charter of the United Nations: A Commentary*, págs. 324-326. 4.ª ed. Oxford: Oxford University Press.
- KRESS, C. (2015). «The International Court of Justice and the “principle of non-use of force”». En: WELLER, M. (ed.). *The Oxford Handbook of the Use of Force in International Law*, págs. 574-577. 4.ª ed. Oxford: Oxford University Press.
- LIN, H. S. (2010). «Offensive Cyber Operations and the Use of Force». *Journal of National Security Law & Policy*, Vol. 12, pág. 63.
- Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, pág. 14, párrs. 176, 188-191. DOI: <https://doi.org/10.18356/9789211543469c002>
- MINISTRY FOR FOREIGN AFFAIRS OF FINLAND (2015). *Legal grounds for the use of force in international relations*, pág. 53. Government Administration Unit.
- MINISTRY OF FOREIGN AFFAIRS OF JAPAN (2021). *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, pág. 3.
- MINISTRY OF FOREIGN AFFAIRS REPUBLIC OF POLAND (2022). «The Republic of Poland's position on the application of international law in cyberspace». *gov.pl*, pág. 4 [en línea]. Disponible en: <https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace>. [Fecha de consulta: 3 de julio de 2025].
- MIV «SAIGA» (No. 2) (Saint Vincent and the Grenadines v. Guinea), Judgment, ITLOS Reports 1999, pág. 10, párrs. 155 y 156.
- MOHIT, A. (2006). «The Customary Law of International Abductions: Limits and Boundaries». *Asian Yearbook of International Law*, Vol. 11, pág. 131. DOI: https://doi.org/10.1163/9789047418306_006
- NATO (2016). «Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016». *NATO-OTAN*, párr. 72 [en línea]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htm. [Fecha de consulta: 4 de julio de 2025].

- NOTA DEL SECRETARIO GENERAL (2021). «Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional», A/75/816, págs. 22, 40 y 42.
- O'CONNELL, M. E. (2022). *International Law and the Use of Force*, págs. 236-237. 3.ª ed. San Paul: Foundation Press.
- OEA (2008). «Informe de la Comisión de la OEA que visitó Ecuador y Colombia», RC.25/doc. 7/08, pág. 17.
- PERMANENT MISSION OF ISRAEL TO THE UN. & INTERNATIONAL ORGANIZATIONS (2021). «Application of International Law to Cyberspace. Summary of Israel's Approach». *Israel* [en línea]. GENEVA. Disponible en: <https://embassies.gov.il/UnGeneva/priorities-statements/ScienceTechnologyDevelopment/Pages/Israel-approach-on-the-Application-of-International-Law-to-Cyberspace.aspx>. [Fecha de consulta: 3 de julio de 2025].
- PERMANENT MISSION OF THAILAND TO THE UNITED NATIONS (2023). *Statement by Mr. Krirkrit Ponlakhetchaiboon, Legal Officer, Department of Treaties and Legal Affairs, Ministry of Foreign Affairs of Thailand, Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 on how international law applies to the use of information and communications technologies by States at the fourth substantive session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025*, pág. 1.
- Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. *Boletín Oficial del Estado* (31 de diciembre de 2021), pág. 167812.
- REPRESENTACIONES DIPLOMÁTICAS DE CUBA EN EL EXTERIOR (2023). «Speech delivered by Ernesto Rodríguez Hernández, Deputy Minister of Communications of the Republic of Cuba, at the Fourth Substantive Session of the Open-Ended Working Group (OEWG) on Cybersecurity 2021-2025. Discussions on the existing and emerging threats». *Representaciones Diplomáticas de Cuba en el Exterior* [en línea]. Disponible en: <https://misiones.cubaminrex.cu/en/un/statements/speech-delivered-ernesto-rodriguez-hernandez-deputy-minister-communications-cuba>. [Fecha de consulta: 4 de julio de 2025].
- RUYS, T. (2014). «The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?». *American Journal of International Law*, Vol. 108, págs. 159, 168, 171-177. DOI: <https://doi.org/10.5305/amerjintellaw.108.2.0159>
- The Atlantic Charter, 14 de agosto de 1941.
- The Corfu Channel Case, pleadings, oral arguments, documents, vol. III, 1950, pág. 296.
- THE FEDERAL GOVERNMENT (2021). *In the Application of International Law in Cyberspace*, pág. 6.
- UNITED KINGDOM MISSION TO THE UNITED NATIONS (2021). «Application of International Law to States' Conduct in Cyberspace. United Kingdom Statement». *United Kingdom Mission to the United Nations*, pág. 3 [en línea]. Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990851/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf. [Fecha de consulta: 3 de julio de 2025].
- UNITED NATIONS (2006). «S.S. "I'm Alone" (Canada, United States)». *Reports of International Arbitral Awards*, Vol. 3, págs. 1609-1618.
- UNITED NATIONS (2023). «(6th meeting) Open-ended working group on Information and Communication Technology (ICT) - Fourth Substantive Session». *United Nations. UN Web TV* [en línea]. Disponible en: <https://webtv.un.org/en/asset/k1m/k1ma7b3tpl>. [Fecha de consulta: 4 de julio de 2025].
- UNODA (2021). *International Law Applied to Operations in Cyberspace*, pág. 3. [en línea]. Disponible en: <https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf>. [Fecha de consulta: 3 de julio de 2025].
- UNODA (2021). *Italy. Italian Position Paper on «International Law and Cyberspace»*, pág. 8. [en línea]. Disponible en: <https://documents.unoda.org/wp-content/uploads/2021/10/italian-position-paper-international-law-and-cyberspace.pdf>. [Fecha de consulta: 8 de julio de 2025].

- UNODA (2023). *OEWG: Fourth Substantive Session*, pág. 1. [en línea]. Disponible en: [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/New_Zealand_-_OEWG_Day_3_Agenda_Item_5_International_Law.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/New_Zealand_-_OEWG_Day_3_Agenda_Item_5_International_Law.pdf). [Fecha de consulta: 8 de julio de 2025].
- UNODA (2023). *Pakistan's Position on the Application of International Law in Cyberspace* [en línea]. Disponible en: [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/UNODA.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/UNODA.pdf). [Fecha de consulta: 4 de julio de 2025].
- UNODA (2023). *South African Statement Agenda Item 5 on the «applicability of international law to the use of information and communications technologies by States,» at the 4th Substantive Session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025*, pág. 1 [en línea]. Disponible en: [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/South_African_Statement_Agenda_Item_5_on_the_applicability_of_international_law_OEWG_ICT_IntSec.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/South_African_Statement_Agenda_Item_5_on_the_applicability_of_international_law_OEWG_ICT_IntSec.pdf). [Fecha de consulta: 8 de julio de 2025].
- UNODA (2023). *Statement by the Representative of Australia to the Fourth Substantive Session of the Open-ended Working Group on Security of and in the Use of ICTS*, pág. 2 [en línea]. Disponible en: [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/OEWG4_-_Australia_intervention_-_law_-_as_delivered_-_March_2023.pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/OEWG4_-_Australia_intervention_-_law_-_as_delivered_-_March_2023.pdf). [Fecha de consulta: 8 de julio de 2025].
- UNODA (2023). *Statement on applicability of international law by Singapore*, pág. 2 [en línea]. Disponible en: [https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ \(2021\)/2023-03-07_OEWG_4SS_IL_Intervention_\(SG\).pdf](https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_ (2021)/2023-03-07_OEWG_4SS_IL_Intervention_(SG).pdf). [Fecha de consulta: 8 de julio de 2025].
- VAN STEENBERGHE, R. (2011). «The Law Against War o Jus Contra Bellum: A new Terminology for a Conservative View of the Use of Force». *Leiden Journal of International Law*, Vol. 24, págs. 757-760. DOI: <https://doi.org/10.1017/S092215651100032X>

Cita recomendada

MARÍN GASTÓN, Manuel (2026). «El desarrollo de la prohibición del uso de la fuerza: los ciberataques y el límite mínimo de intensidad». *IDP. Revista de Internet, Derecho y Política*, núm. 45. UOC [Fecha de consulta: dd/mm/aa]. DOI: <http://dx.doi.org/10.7238/idp.v0i45.9800217>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Sobre el autor**Manuel Marín Gastón**

Universidad Nebrija

manuelmaringaston@gmail.com

Es doctor en Seguridad y Análisis de Riesgos y Conflictos (*cum laude*) por la Universidad Nebrija. Su tesis analiza la evolución del *ius ad bellum* y del sistema de seguridad de NNUU. Asimismo, es diplomado en Altos Estudios de la Defensa Nacional por el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y cuenta con un máster en Derecho Internacional por la Universidad Complutense de Madrid. En la actualidad ejerce como profesor de Relaciones Internacionales en la Universidad Nebrija, donde también es miembro del grupo de investigación en Seguridad, Gestión de Riesgos y Conflictos (SEGERICO). Su investigación se centra en el derecho internacional público, con especial atención a las normas de *ius ad bellum* y a su evolución ante los nuevos desafíos para la seguridad internacional.