Nullius
Revista de pensamiento crítico en el ámbito del Derecho
UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952
Portoviejo-Manabí-Ecuador

Cuando los Bits impactan en la Ciberguerra: Efectos cinéticos en el Ius Ad Bellum e Ius In Bello

When Bits strike in cyberwarfare: Kinetic effects on Ius ad Bellum and Ius in Bello

Juan Carlos Almache Barreiro [1], ORCID: 0000-0003-4502-7576

Nathali Berríos Marrero [2], ORCID: 0009-0007-0950-4714

[1] *Universidad Técnica de Manabí, Portoviejo, Ecuador, juan.almache@utm.edu.ec*

[2] *Universidad Militar Bolivariana de Venezuela, Caracas, Venezuela, nathivez2021@gmail.com*

Citación de este artículo: Almache. J. y Berríos, N. (2025). Cuando los Bits impactan en la Ciberguerra: Efectos cinéticos en el Ius Ad Bellum e Ius In Bello. *Nullius, 6*(1),100-117. https://doi.org/10.33936/nullius.v6i1.7619

Recepción: 20 de mayo del 2025 **Aceptación:** 26 junio del 2025 **Publicación:** 11 de julio de 2025

Resumen

La digitalización del conflicto armado ha desbordado los marcos tradicionales del derecho internacional, obligando a una relectura crítica de los fundamentos normativos que rigen el uso de la fuerza. Este artículo explora el impacto de los ciberataques con consecuencias cinéticas daños físicos provocados por operaciones digitales en la redefinición contemporánea del Ius Ad Bellum (Derecho a la Guerra) y del Derecho Internacional Humanitario. A partir de una metodología analítico-interpretativa y del estudio de casos paradigmáticos (Stuxnet, NotPetya, Colonial Pipeline), se examina cómo el ciberespacio, en tanto nuevo dominio bélico, erosiona las nociones de territorialidad, distinción y proporcionalidad. La investigación propone una reconstrucción jurídica del concepto de "zona de conflicto armado" en entornos transnacionales digitalizados, así como una problematización de la atribución y la legitimidad del contraataque estatal. Lejos de tratarse de una evolución meramente técnica, se sostiene que estamos ante una mutación estructural del conflicto moderno, cuyas implicaciones demandan una revisión normativa urgente bajo principios de humanidad, transparencia y responsabilidad internacional.

Palabras clave: Inteligencia Artificial; Ciberconflicto; Derecho Internacional Humanitario.

Abstract

The digitalization of armed conflict has overwhelmed the traditional frameworks of international law, requiring a critical reassessment of the normative foundations governing the use of force. This article investigates the impact of cyberattacks with kinetic consequences physical damage caused by digital operations on the contemporary redefinition of jus ad bellum and international humanitarian law. Using an analytical-interpretative methodology and a case study approach (Stuxnet, NotPetya, Colonial Pipeline), the paper explores how cyberspace, as an emerging domain of warfare, erodes the notions of territoriality, distinction, and proportionality. The research proposes a legal reconstruction of the concept of "armed conflict zone" within transnational digitalized environments and problematizes attribution and the legitimacy of state countermeasures. Far from being a merely technical evolution, the study contends that this represents a structural mutation of modern conflict, demanding an urgent normative revision grounded in principles of humanity, transparency, and international accountability.

Keywords: Artificial Intelligence; Cyberconflict, International Humanitarian Law.

Introducción

La guerra ya no se libra únicamente en campos de batalla físicos. La transformación del ciberespacio en un teatro de operaciones autónomo ha modificado radicalmente los contornos del conflicto armado moderno, desplazando los umbrales tradicionales de soberanía, territorialidad y uso legítimo de la fuerza. En este nuevo entorno, los ciberataques, especialmente aquellos potenciados por inteligencia artificial (IA), no solo comprometen datos o infraestructura digital: también tienen la capacidad de generar efectos cinéticos reales, provocando daños físicos sustantivos sin presencia militar convencional. Tal fenómeno exige un replanteamiento del Ius Ad Bellum y del Derecho Internacional Humanitario, cuyos marcos interpretativos actuales resultan insuficientes para contener la complejidad del conflicto digitalizado.

El presente artículo parte de una hipótesis disruptiva: la convergencia entre el dominio cibernético y las consecuencias físicas constituye una mutación ontológica del conflicto armado, una en la que el daño no se mide únicamente por explosiones o bajas humanas, sino por el colapso sistémico de infraestructuras críticas, la desestabilización socioeconómica transfronteriza y la erosión silenciosa del principio de distinción entre combatientes y civiles. A través del análisis de casos emblemáticos como *Stuxnet*, *NotPetya* o el ataque a Colonial Pipeline, se argumenta que nos encontramos ante una "tercera dimensión" de la guerra: una que opera en el umbral de lo invisible pero cuyas repercusiones son tan materiales como las de un misil.

Desde una perspectiva transdisciplinaria, que conjuga derecho internacional, estudios de seguridad y teoría crítica de la tecnología, este estudio propone una redefinición del concepto de "zona de conflicto", cuestionando no solo los criterios espaciales, sino también temporales y actorales del enfrentamiento. En ese marco, se plantea la urgencia de revisar las categorías jurídicas de ataque, proporcionalidad y responsabilidad estatal frente a operaciones cibernéticas con efectos equivalentes a los de una ofensiva convencional. Así, la investigación no solo se inscribe en el debate contemporáneo sobre la militarización del ciberespacio, sino que aspira a incidir en la formulación de un marco normativo actualizado, humanista y eficaz frente a una amenaza tan intangible como devastadora.

Así, el ciberespacio no solo redefine los escenarios de confrontación, sino que transforma radicalmente las nociones mismas de vulnerabilidad, poder y daño en los conflictos armados contemporáneos. La capacidad de infligir colapsos sistémicos sin despliegue físico de tropas diluye las fronteras tradicionales entre paz y conflicto, entre acto hostil y mera interferencia. Este fenómeno obliga a repensar los paradigmas clásicos de protección, defensa y responsabilidad estatal, incorporando la necesidad de blindar entornos digitales estratégicos como nueva condición de seguridad nacional e internacional. Frente a esta realidad, urge articular un nuevo consenso jurídico global que no solo se limite a la interpretación extensiva de normas existentes, sino que asuma la innovación conceptual necesaria para salvaguardar la dignidad humana en una era donde las armas más letales son invisibles y los escenarios de destrucción, son silenciosos y devastadores.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

1. La evolución del conflicto armado en el ciberespacio

1.1. Ciberataques con efectos cinéticos: redefiniendo el umbral del uso de la fuerza

La incorporación del ciberespacio como dominio autónomo de confrontación ha provocado una dislocación conceptual de los pilares sobre los que descansa el Derecho Internacional clásico. En particular, la noción de "uso de la fuerza" consagrada en el artículo 2(4) de la Carta de las Naciones Unidas (1945), concebida originalmente para regular ataques armados convencionales, ha sido desafiada por la aparición de ciberataques capaces de causar daños físicos tangibles. Este fenómeno nominado como efectos cinéticos derivados de operaciones digitales no es meramente una anomalía estratégica, sino la manifestación de una mutación estructural del conflicto moderno. Como lo afirma Schmitt, editor del *Tallinn Manual*, "la cibertecnología puede ser utilizada de tal forma que produzca consecuencias materiales equivalentes a las de un bombardeo tradicional" (Schmitt, 2013, p. 47), lo que exige aplicar criterios de Ius Ad Bellum (Derecho a la guerra) e Ius in Bello (Derecho en la guerra) incluso en escenarios digitalizados.

Uno de los casos paradigmáticos que evidencian esta transformación es el de *Stuxnet* (2010), un malware (software malicioso diseñado para dañar o infiltrarse en sistemas informáticos) creado con la finalidad de sabotear las centrifugadoras del programa nuclear iraní en Natanz. Aunque se trató de una operación silenciosa y sin despliegue de tropas, las consecuencias fueron físicas: cerca de mil centrifugadoras quedaron inoperativas, generando una disrupción material comparable a un ataque aéreo de precisión. La sofisticación técnica del código, que manipulaba variables físicas como la velocidad de rotación de los rotores, demostró que un algoritmo puede desencadenar un daño físico sin intervención humana directa. Para *Wired*, este evento marcó el nacimiento de la ciberarma cinética, un software que trasciende la frontera entre lo virtual y lo real (Aparicio, 2023).

Este tipo de ataque despliega interrogantes jurídicos de alta complejidad: ¿Puede considerarse *Stuxnet* un "uso de la fuerza"? ¿Constituye un "ataque armado" según el artículo 51 de la Carta de la ONU? La respuesta no es unívoca. El *Tallinn Manual, que es un estudio académico elaborado por un grupo internacional de expertos en Derecho Internacional, militares y técnicos en ciberseguridad publicado por el* Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN *en* Tallinn- Estonia**,** sostiene que los efectos materiales del ataque deben ser el parámetro principal para su clasificación legal. Si bien no existe consenso sobre si la operación alcanzó el umbral del "ataque armado", sí se reconoce que produjo un daño significativo que vulneró la soberanía iraní (Schmitt, 2013, p. 57). Esto indica que el Derecho Internacional debe desplazarse desde una visión centrada en los medios hacia una lógica basada en los efectos. En palabras de Duncan Hollis, "el ciberespacio ha roto la equivalencia entre causa y medio; ahora lo importante es el resultado tangible que se genera, sin importar si proviene de un misil o de una línea de código" (Hollis, 2020).

Adicionalmente, la problemática de la atribución complica la capacidad de los Estados para responder legalmente a ciberataques con efectos físicos. Según Finlay y Payne (2019), "la atribución es el talón de Aquiles del Derecho Internacional en el ciberespacio, pues sin evidencia concluyente, se erosiona el principio de responsabilidad estatal" (p. 204). A diferencia de los ataques convencionales, en los cuales el agresor suele ser identificable, los ciberataques pueden ocultar su origen mediante técnicas como el proxying, que el Instituto Nacional de Ciberseguridad de España (INCIBE, 2021,párr. 2) concibe como una tecnología que "añade una capa adicional de seguridad para evitar que determinados datos de conexión, generalmente información personal, se compartan y acaben en las manos equivocadas", así como la falsificación de rutas IP

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

y el empleo de infraestructura de terceros países. Esto diluye el marco de aplicación del Derecho Internacional Humanitario y bloquea, en la práctica, el ejercicio del derecho a la legítima defensa.

El principio de proporcionalidad del DIH también se ve afectado, pues en el ciberespacio los efectos de un ataque pueden amplificarse de manera exponencial e impredecible. El caso *NotPetya*, que identifica un ciberataque ocurrido en dicho año y atribuido a actores estatales vinculados a Rusia, utilizó un malware inicialmente disfrazado de ransomware (programa malicioso que bloquea o encripta archivos de un sistema informático y exige el pago de un rescate para su liberación) (Ávila, 2015). Sin embargo, NotPetya no buscaba lucro, sino la destrucción masiva de datos**,** afectando principalmente a infraestructuras críticas en Ucrania y, posteriormente, a empresas internacionales, con daños estimados en miles de millones de dólares, aunque inicialmente dirigido a Ucrania, causó pérdidas globales superiores a los diez mil millones de dólares **(**$10.000´000.000**),** afectando a multinacionales como Maersk y Merck (Greenberg, 2018). Aquí no hubo daños físicos directos, pero la disrupción logística global ocasionó pérdidas materiales equivalentes a un bloqueo económico a gran escala, lo que cuestiona si la proporcionalidad debe evaluarse únicamente con base en daños físicos o si debe incluir también los impactos económicos y sociales indirectos, excitando la urgencia de replantear los parámetros clásicos de la proporcionalidad en el Ius Ad Bellum y también en Ius Ad Bello.

Evaluar la licitud de una operación cibernética ya no puede circunscribirse únicamente al número de víctimas o al volumen de destrucción tangible producido, pues resulta imprescindible considerar también el daño funcional que una disrupción prolongada puede generar en la estabilidad de los Estados, en la salud pública, en el acceso a servicios básicos o en la seguridad económica internacional. De lo contrario, se corre el riesgo de invisibilizar formas de violencia estructural que, aunque menos espectaculares en términos de destrucción física inmediata, pueden resultar igual o más devastadoras a mediano y largo plazo para las sociedades afectadas. Esta ampliación conceptual exige una evolución jurídica que incorpore criterios de daño indirecto y sistémico en la evaluación de la proporcionalidad de los actos hostiles en el ciberespacio, atendiendo a las nuevas dinámicas de vulnerabilidad propias de la era digital.

Se debe considerar que la emergencia de actores no estatales con capacidades cibernéticas militares introduce -efectivamente- un elemento de desestructuración normativa. El mismo Instituto Nacional de Ciberseguridad de España (INCIBE, 2021), en el documento *Ciberamenazas a infraestructuras críticas: análisis y recomendaciones ha señalado que* grupos como Lazarus Group, APT28 o incluso asociaciones criminales como DarkSide han demostrado tener la capacidad de afectar sistemas de agua, hospitales y redes de transporte. En sentido consonante, el Comité Internacional de la Cruz Roja ha advertido que “la protección de la población civil está en riesgo en un entorno donde actores no estatales pueden operar desde cualquier jurisdicción sin responsabilidad clara” (ICRC, 2019, p. 5). Esto identifica un escenario donde el principio de Distinción —central en el derecho de los conflictos armados pierde aplicabilidad práctica.

En sumo, el paradigma del uso de la fuerza está siendo erosionado por la integración del ciberespacio como nuevo dominio operativo. La naturaleza transnacional, deslocalizada y técnicamente opaca de los ciberataques con efectos cinéticos exige una transformación del aparato jurídico internacional, pues bajo este nuevo pentagrama de guerra han quedado obsoletos no solamente el Principio de Distinción, sino a la par de éste y en su orden respecto al primero, los artículos 4 [art. 48 del Protocolo I del Convenio de y normas consuetudinarias 1 a 10 del DIH], el Principio de Proporcionalidad [(art. 51.4.c PI GC), en relación con la norma consuetudinaria 14 del DIH] y el de Precaución [(art. 57.2.a.1 PI CG), en consonancia con las normas consuetudinarias 15 a 24 del DIH] (Comité Internacional de la Cruz Roja, CICR, 1977). Además, no basta con

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

adaptar las normas existentes; es necesario construir un cuerpo normativo específico, con criterios funcionales de atribución, tipificación de actos hostiles, y mecanismos de respuesta proporcional ajustados al entorno digital, pues como concluye Koh, ex asesor legal del Departamento de Estado de los Estados Unidos de América: “el derecho internacional no debe ser un obstáculo para la defensa digital legítima, pero tampoco una coartada para la impunidad digital” (Koh, 2012, p. 10), identificándose así una necesidad apremiante de dicha reconfiguración normativa.

1.2. El reto de la atribución: evidencia técnica y responsabilidad estatal en ciberataque

La atribución de ciberataques representa uno de los desafíos más complejos en el ámbito del Derecho Internacional y la Ciberseguridad. La dificultad para identificar con certeza al autor de un ataque cibernético impide la aplicación efectiva de normas jurídicas y limita las posibilidades de respuesta por parte de los Estados afectados. Desde una perspectiva técnica, los atacantes pueden ocultar su identidad mediante técnicas como el uso de redes de bots (programas automatizados que ejecutan tareas repetitivas) y proxies (servidores que ocultan la IP real), que constituyen tácticas que dificultan la trazabilidad del ataque y complican la recolección de pruebas concluyentes sobre su origen. Como señala Schmitt (2013), "la atribución técnica rara vez es concluyente por sí sola; se requiere una combinación de evidencia técnica y análisis contextual para establecer la responsabilidad" (p. 59).

En el ámbito jurídico, la atribución es esencial para determinar la responsabilidad estatal en un ciberataque. El Derecho Internacional exige pruebas claras que vinculen el ataque con un Estado específico para que se puedan aplicar medidas como sanciones o represalias. Sin embargo, la falta de mecanismos internacionales estandarizados para la atribución complica este proceso. Según Valencia (2024), "la ausencia de un marco legal claro para la atribución de ciberataques socava la eficacia del derecho internacional humanitario en el ciberespacio" (p. 7), lo que sumado a la atribución errónea puede tener consecuencias diplomáticas y legales significativas. Una acusación infundada puede escalar tensiones internacionales y llevar a conflictos innecesarios, siendo crucial que los Estados desarrollen capacidades técnicas y legales robustas para llevar a cabo atribuciones precisas y responsables, pues como destaca Finlay y Payne (2019), "la atribución precisa es fundamental para la legitimidad de cualquier respuesta estatal a un ciberataque" (p. 205), por lo tanto, fortalecer los mecanismos de atribución, tanto en el ámbito técnico como en el legal es lo ideal en un entorno digital cada vez más complejo.

Ahora, la atribución en el ciberespacio no solo implica un reto técnico, sino también un delicado ejercicio político y estratégico que compromete la estabilidad internacional, resultando esencial para la preservación de la paz y la seguridad internacionales en un entorno digital cada vez más complicado. Frente a la dificultad de establecer vínculos irrefutables entre un ataque y un actor estatal, los Estados se ven obligados a actuar bajo condiciones de incertidumbre, lo que aumenta el riesgo de respuestas desproporcionadas o mal dirigidas, en concreto no ajustadas a Derecho. En este contexto, la atribución errónea no es simplemente un error procedimental: constituye una amenaza directa al principio de soberanía y puede desencadenar dinámicas de escalada conflictiva difíciles de contener. Por ello, resulta imperativo articular mecanismos de atribución que combinen la recolección forense digital rigurosa con procedimientos multilaterales de verificación y validación independientes, a fin de garantizar no solo la precisión técnica, sino también la legitimidad política de las imputaciones. De esta manera, se protegería la integridad del Derecho Internacional, se reduciría el margen de arbitrariedad en las respuestas estatales y se fortalecería la confianza internacional en un orden jurídico capaz de adaptarse a la complejidad del ciberespacio.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

En el contexto actual de creciente interconexión digital, la cooperación internacional y el intercambio de información se han convertido en elementos esenciales para fortalecer las capacidades de asignación en el ámbito de la ciberseguridad. La atribución precisa de ciberataques es fundamental para identificar a los responsables y aplicar las medidas legales correspondientes; sin embargo, la naturaleza transnacional y anónima de estos delitos complica su rastreo y enjuiciamiento. En este escenario, el Convenio de Budapest sobre la Ciberdelincuencia, promovido por el Consejo de Europa, emerge como un instrumento clave, por cuanto este tratado internacional busca armonizar las legislaciones nacionales y facilitar la colaboración entre Estados en la lucha contra los delitos cibernéticos, estableciendo un marco legal común que permite a los países cooperar eficazmente en la investigación y persecución de delitos informáticos, superando las barreras jurisdiccionales que a menudo impiden una respuesta rápida y coordinada (Consejo de Europa, 2024).

A pesar de estos avances, persisten desafíos significativos para establecer estándares globales en materia de imputación y responsabilidad en el ciberespacio. La falta de consenso internacional sobre las normas aplicables y la dificultad para obtener pruebas concluyentes complican la identificación de responsabilidades. Además, algunos Estados pueden carecer de los recursos técnicos o la voluntad política para participar plenamente en los mecanismos de cooperación existentes. Por ello, es imperativo fortalecer las capacidades nacionales y fomentar la confianza mutua entre los países. La implementación de estándares comunes y la promoción de la transparencia en las operaciones cibernéticas son pasos esenciales para avanzar hacia un ciberespacio más seguro y responsable. La comunidad internacional debe continuar trabajando conjuntamente para desarrollar marcos legales y técnicos que permitan una atribución efectiva y una respuesta coordinada a las amenazas cibernéticas (Naciones Unidas, 2021).

1.3. Ascensión del ciberdominio: soberanía digital y reconfiguración geoestratégica del teatro operacional

La incursión del ciberespacio como un dominio fundamental en la conducción de la guerra contemporánea trasciende la mera adición de un nuevo frente geográfico, pues implica una metamorfosis radical en la concepción ontológica misma del conflicto armado. La noción tradicional de la guerra, históricamente arraigada en enfrentamientos físicos y territorialmente delimitados entre fuerzas militares que operan dentro de confines geográficos reconocibles, se ve crecientemente desafiada y desmantelada por la naturaleza intrínseca de las operaciones cibernéticas. En la actualidad, los vectores de ataque cibernético, tales como el malware avanzado y las técnicas de intrusión de red, pueden franquear las fronteras nacionales con una facilidad y velocidad sin precedentes, permitiendo la manipulación y disrupción de infraestructuras críticas a distancias territoriales virtualmente ilimitadas, e incluso la generación de efectos cinéticos devastadores en el mundo físico sin la necesidad de un despliegue convencional de fuerzas militares en el terreno. Esta capacidad de las operaciones cibernéticas para trascender las limitaciones espaciales y temporales que históricamente han definido los conflictos armados genera incidencias epistemológicas y jurídicas de gran envergadura, exigiendo una valuación fundamental de los marcos teóricos y normativos que rigen la guerra en la era digital.

La transformación del teatro de operaciones hacia el dominio cibernético conlleva una desterritorialización del conflicto, donde las fronteras físicas y los límites geográficos tradicionales pierden relevancia estratégica (Martínez, 2011). Esta desterritorialización complica la aplicación del I*us ad Bellum* y el I*us in Bello*, que siendo los pilares del DIH, fueron diseñados para regular las hostilidades en un contexto predominantemente físico. La naturaleza extranacional y a menudo anónima de los ciberataques dificulta la atribución de responsabilidad, la determinación del umbral de un acto de guerra y la aplicación de los principios de distinción, proporcionalidad y precaución militar en un entorno donde los actores pueden operar desde

cualquier lugar del mundo y los efectos de sus acciones pueden manifestarse de manera indirecta y retardada. Además, la creciente interconexión de las infraestructuras críticas de los Estados, incluyendo redes de energía, sistemas financieros y sistemas de salud, las convierte en blancos potenciales de ciberataques, borrando aún más la distinción entre el ámbito civil y militar y planteando graves dilemas éticos y humanitarios.

El desplazamiento del conflicto hacia el ciberespacio también exige una reconsideración de los conceptos de soberanía y jurisdicción en el Derecho Internacional. La capacidad de los ciberataques para originarse en un Estado y causar daños en otro sin que haya una incursión física, expone las dificultades para precisar el alcance de la soberanía estatal en el ciberespacio y la aplicabilidad de las leyes nacionales en un entorno inherentemente transfronterizo. Tal como argumenta Deeks (2021), "el ciberespacio desafía la noción tradicional de soberanía basada en el control territorial exclusivo, exigiendo nuevos enfoques para la regulación de las actividades cibernéticas y la cooperación internacional en materia de ciberseguridad" (p. 112). De todo esto se colige que, la falta de consenso sobre las normas aplicables al ciberespacio y la ausencia de mecanismos internacionales efectivos para la atribución de ciberataques y la aplicación de sanciones contribuyen a un vacío normativo que aumenta el riesgo de conflictos y la impunidad de los ciberdelincuentes.

Así observamos que, la ascensión del ciberdominio dentro del teatro operacional contemporáneo detona una cascada de transformaciones que redefinen radicalmente la seguridad internacional y la estabilidad global. Lejos de ser una simple extensión del campo de batalla, esta evolución propulsa una metamorfosis en la propia naturaleza del conflicto, ya que la creciente sofisticación y el potencial inherentemente disruptivo de las armas cibernéticas, con su capacidad para trascender las limitaciones geográficas y desestabilizar tanto objetivos militares como bienes civiles, catalizan una profunda reestructuración del panorama de seguridad. Esta complejidad se ve exponencialmente amplificada por la proliferación de actores estatales y no estatales que empuñan capacidades cibernéticas ofensivas, borrando las distinciones entre las formas tradicionales de guerra y las operaciones que se desarrollan en el éter digital. Así tenemos que, la carencia de mecanismos internacionales robustos y eficaces para la prevención y resolución de conflictos en este nuevo dominio, enciende el riesgo de una escalada de tensiones abriendo paso a la sombría posibilidad de una "ciberguerra" a gran escala, cuyas consecuencias podrían tener un impacto sísmico en la paz y la seguridad internacionales.

En este contexto de creciente incertidumbre y fluidez tecnológica, la soberanía digital emerge no solo como un concepto legal, sino como un eje central en la convulsión geoestratégica que experimenta el teatro operacional. Rid (2020) arroja luz sobre el peligro que reside en los "umbrales difusos" que caracterizan intrínsecamente las operaciones cibernéticas, donde las acciones que se ejecutan por debajo del umbral convencional del conflicto armado pueden, sin embargo, desatar ramificaciones de gran alcance y provocar respuestas militares convencionales.

1.4. De la guerra física a la guerra de datos: La mutación estructural del conflicto armado

La evolución de los actos hostiles hacia el dominio cibernético representa no solo un cambio tecnológico, sino una *mutación estructural* del concepto de conflicto armado que reconfigura los cimientos históricos sobre los que se construyeron las categorías del DIH. A medida que el "campo de batalla" se desplaza del espacio físico al dominio virtual, la materia prima del conflicto ya no es necesariamente el territorio, la fuerza bruta o el dominio marítimo o aéreo, sino *los datos*: su control, su manipulación y su capacidad para desestabilizar infraestructuras críticas de los Estados. Como señala Nye (2010), en la era digital "el poder se mide cada vez más por el control de la información y de las redes de comunicación" (p. 3), y esta afirmación evidencia el

desplazamiento del centro de gravedad de la guerra contemporánea hacia escenarios donde el conocimiento, y no la superioridad material inmediata, marca la supremacía.

En este contexto, el ciberespacio no solo actúa como un nuevo entorno operativo, sino como un nuevo objeto de apropiación bélica. La información ya no es un mero recurso de apoyo logístico o estratégico, sino que deviene en sí misma un bien estratégico que puede ser destruido, alterado o exfiltrado como fin militar primario. Esto implica profundas tensiones con los principios tradicionales del DIH, como el principio de distinción, diseñado para proteger a la población civil de los efectos de las hostilidades. Como advierte Schmitt (2013), "la arquitectura técnica del ciberespacio hace extremadamente difícil diferenciar entre objetivos militares y bienes civiles, debido a la interconexión de sistemas" (p. 18), lo que socava uno de los pilares esenciales del Ius in Bello.

La mutación estructural del conflicto también afecta a la manera en que se conceptualiza la ocupación y la soberanía. A diferencia de la ocupación territorial tradicional, la ocupación digital no requiere la presencia física de tropas extranjeras; basta con que un actor hostil tome el control de redes críticas de un Estado soberano como sus sistemas eléctricos, de agua, salud o finanzas para producir efectos de dominación análogos a los de una ocupación militar convencional. Este tipo de control, aunque invisible y sin armas, debilita la capacidad de un Estado para proteger y gestionar su infraestructura esencial, poniendo en entredicho la noción clásica de invasión y obligándonos a replantear su significado en el contexto digital actual.

Esta nueva realidad de la guerra de datos también transforma la atribución de responsabilidad y la imputabilidad de actos ilícitos. Tradicionalmente, los actos de guerra requerían una clara cadena de mando y responsabilidad política. Sin embargo, en el ciberespacio, la posibilidad de operaciones encubiertas, de actores proxy, y de ataques anónimos realizados a través de redes distribuidas complica la atribución. Como explica Jensen (2015), "la dificultad de atribuir ataques cibernéticos plantea un reto fundamental para el cumplimiento del derecho internacional, al diluir la rendición de cuentas" (p. 547). Esto puede derivar en un debilitamiento sistémico del orden jurídico internacional si los Estados no logran adaptar los mecanismos probatorios y de verificación a las nuevas realidades técnicas.

Un elemento inédito que emerge en este contexto es lo que podríamos denominar **"**violencia algorítmica latente**"**, un estado de agresión continua, de baja intensidad, ejercido no mediante ejércitos o bombardeos visibles, sino mediante algoritmos autónomos que afectan la funcionalidad y resiliencia del tejido económico y social de los Estados adversarios. Esta forma de violencia no busca necesariamente destruir, sino erosionar la confianza pública, alterar procesos democráticos o socavar la estabilidad interna, generando condiciones de debilitamiento estratégico prolongado. Como advierte Rid (2020), "el ciberconflicto no se centra tanto en la destrucción como en la manipulación y la subversión" (p. 49), lo que trasciende a escenarios inéditos para la configuración jurídica del umbral de uso de la fuerza conforme al artículo 2.4 de la Carta de las Naciones Unidas.

Frente a este panorama, se hace imperativo repensar conceptos clave del DIH. ¿Puede considerarse un acto de guerra el sabotaje sistemático de servicios básicos de un Estado mediante ataques cibernéticos? ¿Debe clasificarse como "ocupación" la apropiación ilícita y control de sistemas bancarios o sanitarios por actores estatales hostiles? ¿Cómo delimitar la proporcionalidad de una respuesta armada cuando el ataque original no causa destrucción física sino degradación progresiva de la soberanía digital de un Estado? Estas preguntas no tienen precedentes claros y demandan una labor doctrinal profunda y urgente.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

La transformación del conflicto armado hacia una guerra de datos obliga, por tanto, a concebir un nuevo "Ius Ad Bellum Digital", basado en parámetros adecuados al entorno cibernético, que contemple la protección de bienes digitales esenciales, la regulación del uso de armas algorítmicas y la redefinición del principio de soberanía a la luz del control informacional. En palabras de Shackelford (2014), "el ciberespacio exige una soberanía responsable que garantice no solo la protección del propio entorno nacional, sino también el respeto a los derechos y la seguridad de otros Estados" (p. 105), pues la mutación estructural de la guerra a la era digital supone no una mera extensión del conflicto tradicional, sino un verdadero cambio paradigmático en la naturaleza, los objetivos y los medios de la guerra. Ante esta transformación radical, el derecho internacional enfrenta el desafío histórico de adaptarse o correr el riesgo de quedar obsoleto, incapaz de regular eficazmente los nuevos escenarios de confrontación donde los datos, los algoritmos y las redes son las nuevas armas de poder.

2. Ciberguerra y Derecho Internacional Humanitario: Reconfiguración y Nuevos Paradigmas

2.1. El Dolo Tecnológico en Ciberguerra: Una nueva categoría de imputabilidad internacional

La irrupción de la ciberguerra en el ámbito de las relaciones internacionales y, de cara al derecho humanitario ha forzado una relectura de los conceptos clásicos de responsabilidad y de dolo. En particular, emerge la necesidad de introducir una *nueva categoría de imputabilidad internacional: el dolo tecnológico***,** entendida como la programación o diseño intencional de vulnerabilidades, códigos maliciosos o algoritmos autónomos cuyo objetivo es producir daño en sistemas, infraestructuras críticas o derechos de otros Estados o sus ciudadanos. Esta noción desplaza la concepción tradicional del dolo, centrada en la voluntad consciente y directa del agente humano, hacia una nueva forma de responsabilidad basada en la *intencionalidad mediada tecnológicamente***.**

En el ámbito clásico del derecho internacional, el dolo ha sido interpretado como la consciencia y voluntad de violar normas jurídicas mediante actos ilícitos internacionalmente imputables (Cassese, 2005, p. 267). Sin embargo, cuando la acción nociva no se ejecuta de forma directa por un ser humano, sino mediante sistemas autónomos programados para actuar con independencia, la lógica de la imputación debe expandirse para capturar esta nueva forma de "agencia delegada". Como afirma Schmitt (2013), "la autonomía tecnológica plantea interrogantes fundamentales sobre cómo atribuir responsabilidad en situaciones en las que la acción humana directa está mediada o incluso reemplazada por sistemas algorítmicos" (p. 45).

El dolo tecnológico se manifiesta no solo en el despliegue directo de malware o ataques de denegación de servicio, sino también en la inserción deliberada de vulnerabilidades de diseño (backdoors) en sistemas de uso global, en la creación de algoritmos de manipulación de información o en la programación de inteligencias artificiales destinadas a identificar y explotar fallos de seguridad en infraestructuras críticas extranjeras. Estas conductas no suponen meros riesgos accidentales o negligencias, sino auténticas manifestaciones de voluntad dolosa orientadas a producir efectos dañinos a nivel internacional.

El reto jurídico es que, bajo los esquemas tradicionales, la imputación de responsabilidad internacional exige una conexión clara entre el autor y el acto ilícito. Pero, como advierte Lin (2010), "el carácter distribuido, anónimo y automatizado de las operaciones cibernéticas erosiona los mecanismos clásicos de imputación de responsabilidad en el derecho internacional" (p. 103). De allí la urgencia de conceptualizar el dolo tecnológico como una categoría autónoma que permita reconocer la responsabilidad internacional basada en la intención programada, aun en ausencia de intervención humana directa e inmediata en el daño.

Una dimensión particularmente problemática del dolo tecnológico reside en la creación de armas algorítmicas de efectos diferidos, es decir, sistemas que son diseñados para activarse en el futuro bajo determinadas condiciones o que escalan progresivamente su agresividad mediante procesos de autoaprendizaje. Tal programación premeditada implica una forma de voluntad adelantada en el tiempo, cuyo nexo de imputación no puede rastrearse únicamente a la acción final, sino al acto originario de programación maliciosa. La naturaleza predictiva y adaptativa de las tecnologías emergentes exige nuevos marcos de responsabilidad que reconozcan la intencionalidad incorporada en el diseño de sistemas autónomos.

Esta situación nos conduce a plantear que en el ámbito de la ciberguerra debe reconocerse un dolo programático, donde el foco de la responsabilidad jurídica se traslade del acto final al diseño inicial, evaluando la previsibilidad, la intencionalidad y la peligrosidad inherente de los sistemas creados. La omisión deliberada de medidas de control o de mecanismos de auto-limitación en armas cibernéticas podría ser también configurada como expresión de dolo tecnológico, especialmente si dicha omisión responde a una estrategia premeditada de maximizar el daño o la imprevisibilidad de los efectos. En consecuencia, en el marco del **ius** ad bellum y del ius in bello, resulta imprescindible establecer parámetros normativos que permitan sancionar el dolo tecnológico como forma agravada de violación de la paz internacional y del derecho humanitario. La creación y diseminación de herramientas tecnológicas diseñadas para violar masivamente derechos humanos o atacar infraestructuras críticas civiles debe ser considerada no solo como un acto hostil, sino como un crimen internacional cuando se cumplan los requisitos de gravedad, intencionalidad programada y consecuencias catastróficas.

El análisis de la ciberguerra desde la perspectiva del dolo tecnológico también obliga a repensar las nociones de proporcionalidad y necesidad en el uso de la fuerza. ¿Es proporcional la respuesta militar ante un ataque informático cuya devastación fue provocada por sistemas autónomos? ¿Es admisible como defensa legítima preventiva la neutralización de programas de software malicioso detectados antes de su activación? Estas interrogantes demandan una evolución dogmática profunda que reconozca el carácter disruptivo de la intencionalidad tecnológica en el campo de los conflictos armados.

Finalmente, debemos advertir que el dolo tecnológico plantea no solo problemas de imputabilidad estatal, sino también de responsabilidad individual internacional. El programador que diseña sistemas de ataque autónomo, el ingeniero que inserta vulnerabilidades deliberadas o el científico que desarrolla algoritmos para manipular procesos democráticos podrían ser considerados como perpetradores indirectos de crímenes internacionales, ampliando así la teoría de la autoría mediata a través de un instrumento no humano, pero igualmente determinante. En palabras de Ambos (2013), "el dominio del hecho puede ejercerse también a través de aparatos organizados de poder, y en el caso de la ciberguerra, los algoritmos pueden funcionar como tales aparatos" (p. 126).

2.2. Umbrales de Hostilidad Algorítmica: De la mínima intervención al conflicto digital latente

La emergencia de algoritmos autónomos capaces de ejecutar acciones hostiles transforma radicalmente el entendimiento tradicional del umbral de uso de la fuerza en el derecho internacional, particularmente en el marco del Ius ad Bellum. Históricamente, la noción de "ataque armado" ha sido interpretada conforme al artículo 51 de la Carta de las Naciones Unidas, exigiendo violencia física, destrucción material tangible y atribución humana directa. Sin embargo, con el auge de la inteligencia artificial autónoma, surge la necesidad de repensar la noción de mínima intervención y los requisitos de la legítima defensa frente a "hostilidades algorítmicas" que erosionan progresivamente la estabilidad estatal.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

Autores recientes destacan este problema con creciente urgencia. Schmitt y Vihul (2020) sostienen que "un ciberataque que cause efectos comparables a los de un ataque cinético, aunque sea ejecutado por un algoritmo autónomo, puede constituir uso de la fuerza bajo el derecho internacional" (p. 65), aunque reconocen que el análisis debe extenderse también a efectos acumulativos no inmediatamente visibles. Esta advertencia es crucial: cuando un algoritmo altera infraestructuras críticas, distorsiona mercados financieros o manipula servicios básicos, el daño sistémico puede ser más profundo que el impacto físico directo. Las hostilidades digitales latentes no se manifiestan en un único acto, sino en una cadena prolongada de acciones que subvierten las bases funcionales del Estado.

En este sentido, Tsagourias y Buchan (2021) enfatizan que "el derecho internacional contemporáneo debe reconocer el carácter incremental y adaptativo de las amenazas digitales" (p. 112), advirtiendo que la tradicional visión binaria de paz y guerra resulta insuficiente. Así, el surgimiento de acciones hostiles algorítmicas genera una nueva categoría de conflicto: el *conflicto digital latente*, caracterizado por intervenciones persistentes y disimuladas que afectan la soberanía sin detonar una confrontación armada abierta.

La cuestión de la atribución agrava aún más el escenario. Asaf Lubin (2021) subraya que "el uso de sistemas autónomos difumina las líneas de responsabilidad estatal bajo el derecho internacional" (p. 45), dificultando la activación legítima de mecanismos de defensa frente a ataques cuya autoría humana directa es incierta o deliberadamente oculta. Esta ambigüedad estratégica es aprovechada tanto por Estados como por grupos no estatales, que actúan dentro de lo que Shackelford et al.(2022) describe como una "zona gris": un entorno de confrontación digital cuidadosamente calculado para mantenerse por debajo del umbral que desencadenaría una respuesta militar convencional. En este espacio difuso, las operaciones cibernéticas son diseñadas para ser lo suficientemente disruptivas sin cruzar las líneas claras del conflicto armado, lo que dificulta la aplicación del derecho internacional tradicional. .

A ello se suma el desfase entre el avance tecnológico y la capacidad de adaptación normativa. Dinniss (2021) señala que "la rapidez de la innovación algorítmica supera la capacidad del derecho para responder de manera efectiva" (p. 28), generando un vacío jurídico que favorece la impunidad en el ciberespacio. Ante esta evolución, la noción clásica de *uso de la fuerza* debe expandirse para abarcar el daño progresivo e intangible causado por algoritmos autónomos que atacan los cimientos funcionales de los Estados.

El desafío no es menor: ignorar estas nuevas formas de agresión sería aceptar pasivamente la desintegración paulatina de las normas fundamentales que sostienen el orden internacional. Por ello, se hace imperativo construir una arquitectura jurídica que reconozca y sancione no solo los estallidos súbitos de violencia, sino también las hostilidades silenciosas y constantes del ciberconflicto algorítmico.

2.3. Responsabilidad Estatal por Inteligencia Artificial Autónoma en Conflictos Cibernéticos

La irrupción de sistemas de IA autónoma en escenarios de conflictos cibernéticos exige una revisión profunda de las reglas de responsabilidad estatal en el derecho internacional. Mientras las doctrinas tradicionales de atribución se basaban en el control humano efectivo sobre los actos ilícitos, el desarrollo de agentes cibernéticos capaces de actuar de manera independiente ha generado una disrupción estructural que, si no se aborda normativamente, podría vaciar de contenido la noción misma de responsabilidad internacional. Como advierte Fleur Johns (2020), "la creciente autonomía tecnológica desestabiliza la arquitectura legal internacional basada en sujetos humanos y acciones intencionadas" (p. 612), lo que obliga a repensar los fundamentos de imputación.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

Desde 2020, los debates en foros académicos han reconocido que la IA no solo ejecuta instrucciones humanas, sino que, debido a procesos de autoaprendizaje o programación adaptativa, puede originar comportamientos hostiles no previstos por sus diseñadores. En este sentido, Dapo Akande y otros (2021) sostienen que "los Estados deben ser considerados responsables por los actos de sistemas autónomos cuando estos han sido desplegados por ellos y actúan dentro del ámbito de las funciones para las cuales fueron programados, incluso si actúan de manera no anticipada" (p. 31). Esta propuesta de responsabilidad expandida introduce una lógica de imputabilidad basada en el riesgo tecnológico y en el principio de precaución reforzada.

La doctrina más reciente también ha planteado que la responsabilidad estatal debería extenderse a los fallos algorítmicos derivados de defectos de diseño, entrenamiento o supervisión de los sistemas de IA utilizados en operaciones internacionales. Así, Veronika Bílková (2022) advierte que "el control previo ejercido por los Estados sobre el diseño y despliegue de tecnologías autónomas debe ser el criterio determinante para la atribución de responsabilidad, desplazando el énfasis en el control sobre actos específicos" (p. 344). Esto significa que un Estado no podría eximirse de responsabilidad simplemente alegando que su IA actuó fuera de sus parámetros originales si no implementó medidas de control diligente.

A su vez, el informe del Panel de Alto Nivel sobre Comportamiento Responsable en el Ciberespacio (2021) enfatiza que "los Estados no deben utilizar sistemas autónomos como medios para evadir su responsabilidad internacional" (p. 19), subrayando que la creación o el despliegue de agentes cibernéticos autónomos genera obligaciones internacionales específicas de monitoreo, corrección y, en caso de daño, reparación. Este principio rompe con la ficción jurídica de la autonomía tecnológica como excusa y refuerza la noción de responsabilidad soberana en el entorno digital.

En consecuencia, es necesaria la creación conceptual de la "responsabilidad por delegación algorítmica programada", una figura de imputabilidad que reconoce que la liberación de IA autónoma en conflictos equivale jurídicamente a un acto de delegación de funciones estatales, y que los actos subsiguientes, previsibles o no, deben ser imputados al Estado creador. Esta noción permitiría llenar los vacíos que las nuevas tecnologías abren en los estándares clásicos de imputación derivados de los artículos 4 a 11 del Proyecto de Artículos sobre Responsabilidad del Estado por hechos internacionalmente ilícitos, adoptado por la Comisión de Derecho Internacional (CDI) en su 53º período de sesiones (A/56/10) y, finalmente anexados por la Asamblea General de la ONU en su Resolución A/RES/56/83, de 28 de enero del 2002.

En términos de teoría del derecho internacional, como destaca Kubo Mačák (2021), "la creciente delegación de funciones tradicionalmente estatales a sistemas de IA obliga a repensar los conceptos de atribución y responsabilidad a la luz del principio de efectividad tecnológica" (p. 218). No basta con evaluar quién da la orden directa, sino analizarse quién crea las condiciones materiales para que el acto hostil ocurra mediante agentes tecnológicos.

2.4. Arquitectura jurídica del contraataque cibernético: ¿Defensa preventiva, legítima defensa o agresión?

La arquitectura jurídica que debe regir el contraataque cibernético en el siglo XXI requiere una reconsideración profunda de los principios tradicionales del derecho internacional. La expansión de las hostilidades al ciberespacio ha transformado no solo las dinámicas del conflicto, sino también las concepciones sobre legítima defensa, defensa preventiva y agresión. Esta mutación exige nuevas categorías interpretativas que permitan evaluar cuándo un acto de respuesta estatal ante un ciberataque constituye una

acción justificada y cuándo, por el contrario, deviene en una transgresión al artículo 2(4) de la Carta de las Naciones Unidas.

En primer lugar, la defensa preventiva digital se configura como una doctrina sumamente controvertida. Tradicionalmente, la legítima defensa bajo el artículo 51 de la Carta solo se permite frente a un "ataque armado" efectivo. Sin embargo, en el ciberespacio, las amenazas pueden desplegarse de manera encubierta, silenciosa y devastadora antes de materializarse de forma física. De acuerdo con Lin (2021), los Estados enfrentan ataques que pueden degradar redes eléctricas, alterar infraestructuras críticas o minar la seguridad nacional sin necesidad de una confrontación armada tradicional. Por esta razón, algunos proponen la ampliación conceptual de la defensa anticipada, basándola no solo en la inminencia física, sino también en la inminencia de la degradación digital irreversible. Esta interpretación, aunque seductora para la protección estatal, debe ser manejada con cautela para no desdibujar los límites jurídicos que separan la prevención legítima de la agresión ilícita.

La legítima defensa en el contexto cibernético tiende a ser considerada como un derecho inherente de los Estados, aunque su aplicación concreta aún genera debates dentro del marco del derecho internacional, pero su ejercicio requiere superar varios filtros conceptuales. Según Hathaway y Klimburg (2021), para que un ciberataque justifique una respuesta armada legítima, debe alcanzar un nivel de gravedad comparable a un ataque convencional, ya sea causando muertes, daños físicos sustanciales o la paralización masiva de funciones estatales esenciales. Esto introduce una dificultad crítica: evaluar la magnitud del daño digital en un ecosistema donde los efectos son, muchas veces, intangibles, acumulativos y de largo plazo. Así, no todo acceso indebido o alteración de datos puede ser considerado un "uso de la fuerza" que active el derecho a la legítima defensa, exigiéndose un análisis pormenorizado caso por caso.

Por otro lado, el concepto de agresión en el ciberespacio debe ser reformulado para enfrentar las sutilezas del conflicto digital. No todos los ciberataques deben ser interpretados automáticamente como actos de agresión. Como subraya Kello (2020), muchos ciberoperativos se ubican en una "zona gris" entre la mera competencia estatal y la violencia prohibida, caracterizados por su ambigüedad estratégica y su dificultad de atribución. En este sentido, responder de manera desproporcionada a una operación de espionaje cibernético o a un sabotaje de bajo nivel podría convertir a un Estado defensor en un agresor internacional, comprometiendo su legitimidad y violando el orden jurídico global.

Así, la propuesta de clasificación jurídica del contraataque cibernético debe construirse sobre tres pilares fundamentales. Primero, la defensa preventiva digital debe ser restringida a situaciones de daño digital inminente, cierto y grave, bajo estándares probatorios exigentes que eviten abusos. Segundo, la legítima defensa debe ser proporcional al daño sufrido y solo ejercida cuando no existan alternativas razonables para detener o repeler el ataque, como lo establece el principio de necesidad. Tercero, toda respuesta estatal debe ser calibrada para no constituir, por sí misma, un acto de agresión prohibido, tomando en cuenta la naturaleza, el origen, la intensidad y los efectos del ciberataque inicial.

La arquitectura jurídica del contraataque cibernético, por tanto, no puede sostenerse únicamente en traslaciones mecánicas del derecho clásico. Se requiere una interpretación dinámica, informada por la realidad tecnológica y por los principios éticos de minimización de daños y preservación del orden internacional. Como plantea Shackelford (2014), la evolución del derecho internacional en el ámbito de la ciberguerra no se limitará a la creación de nuevos tratados o normas escritas, sino que también dependerá profundamente de cómo los Estados actúen de forma responsable en el ciberespacio. La supervivencia del marco jurídico contemporáneo

frente a la nueva amenaza digital dependerá, en última instancia, de nuestra capacidad para innovar dentro de los principios fundamentales que han regido la convivencia internacional desde 1945.

Metodología

Para la realización de este artículo científico, se utiliza una metodología cualitativa, enfocada principalmente en el análisis doctrinal y la revisión exhaustiva de textos legales y académicos que abordan la interacción entre el Derecho Internacional Humanitario (DIH) y las operaciones cibernéticas. La investigación se basa en la revisión de obras clave de autores reconocidos, quienes han tratado ampliamente la problemática del ciberespacio y su relación con las normas tradicionales de los conflictos armados. Entre los textos fundamentales se incluyen los trabajos de Schmitt y Vihul (2020), cuyas contribuciones proporcionan una base sólida para entender los desafíos legales derivados de los ciberataques.

Uno de los estudios relevantes se identifica con la obra de Michael N. Schmitt, quien en su libro "Cyber Operations and the Law of Armed Conflict" (2017), aborda de manera detallada cómo el Derecho Internacional Humanitario debe adaptarse al nuevo contexto de las operaciones cibernéticas. Schmitt destaca la necesidad de redefinir los principios fundamentales del DIH para abordar las particularidades de la ciberguerra, especialmente en lo que respecta a la distinción entre los ataques cibernéticos y las operaciones militares tradicionales. Su análisis sobre la ambigüedad de las acciones hostiles en el ciberespacio y su impacto sobre los principios de proporcionalidad y necesidad son fundamentales para examinar la legitimidad de las respuestas estatales a los ciberataques y las implicaciones para la soberanía digital de los Estados.

Por otro lado, la obra de Timothy L. H. McCormack, "The Law of Cyber Warfare" (2020), ofrece un enfoque integral sobre la intersección entre el DIH y el ciberespacio. McCormack analiza los marcos legales internacionales actuales y cómo estos se ven desbordados por la naturaleza transnacional y anónima de los ciberataques, lo que genera incertidumbre sobre cuándo y cómo se activan los derechos de autodefensa en el contexto de un conflicto armado. Esta obra es esencial para entender las complejidades de los ataques cibernéticos y su impacto en el Ius ad Bellum y el Ius in Bello, los cuales, según McCormack, deben evolucionar para enfrentar la realidad de los conflictos en el ciberespacio.

El enfoque metodológico de esta investigación también incluye un análisis comparativo de las normas internacionales vigentes, especialmente aquellas desarrolladas por las Naciones Unidas en relación con la ciberseguridad y los ciberataques, así como los Protocolos Adicionales de los Convenios de Ginebra del 12 de agosto de 1949. La revisión de estos textos permite identificar las brechas normativas existentes y ofrecer propuestas para actualizar las leyes internacionales en respuesta a las nuevas formas de guerra. Además, se realiza un análisis de las implicaciones jurídicas de las operaciones cibernéticas dentro del contexto de las nuevas amenazas globales y la desafiante naturaleza jurídica del ciberespacio, lo que abre la puerta a una mayor reflexión sobre cómo los marcos legales internacionales pueden ser reformados.

En resumen, esta metodología se basa en la recopilación de información a partir de la obra de autores clave, cuyas investigaciones proporcionan un marco teórico robusto para analizar las implicaciones legales de las ciberoperaciones. A través de este enfoque, se buscará aportar una comprensión profunda de los desafíos actuales que enfrenta el Derecho Internacional Humanitario en relación con los ciberataques, proponiendo también recomendaciones para una mayor adaptación de las normas tradicionales a las realidades del ciberespacio.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

Resultados

El análisis efectuado en este trabajo revela que la emergencia del ciberespacio como un dominio operativo autónomo ha generado una ruptura radical en los fundamentos del Derecho Internacional Humanitario y el Ius ad Bellum. Los ciberataques con efectos cinéticos, ejemplificados en los casos Stuxnet, NotPetya y Colonial Pipeline, han desdibujado las fronteras tradicionales entre acto de guerra, sabotaje y hostilidad estatal, planteando un escenario donde la atribución técnica, la proporcionalidad de las respuestas y la misma noción de ataque armado exigen reformulaciones profundas. El estudio demuestra que la infraestructura crítica, al ser blanco principal de los ataques, transforma el concepto mismo de vulnerabilidad estatal, desplazándolo del espacio territorial al espacio digital, y que la acumulación de daños en sistemas de servicios esenciales puede equivaler, en términos jurídicos y humanitarios, a una agresión armada convencional. Además, se constata que la atribución de ciberataques sigue representando un talón de Aquiles para el derecho internacional, dado que las complejidades técnicas de identificación impiden respuestas legítimas claras y fomentan un entorno de impunidad estratégica. También se ha puesto en evidencia que la noción emergente de "conflicto digital latente" y "dolo tecnológico" son conceptos que deben incorporarse a la doctrina jurídica si se pretende regular de forma efectiva las nuevas manifestaciones de violencia algorítmica.

Discusión

La discusión de los hallazgos evidencia la necesidad imperiosa de que el Derecho Internacional evolucione para afrontar los fenómenos disruptivos introducidos por la ciberguerra. No basta con interpretar extensivamente las categorías clásicas del Ius ad Bellum y del Ius in Bello; es necesario un rediseño doctrinal que reconozca como actos hostiles no solo los ataques físicos sino también las alteraciones funcionales, acumulativas y sistémicas provocadas por algoritmos autónomos. La incapacidad de los marcos jurídicos actuales para afrontar la violencia difusa y silenciosa de los ciberataques pone en riesgo la estabilidad internacional y la protección de los derechos humanos en situaciones de conflicto. Es fundamental integrar en el análisis jurídico el concepto de “dolo tecnológico” como un modo de responsabilidad autónoma, donde la intención programada sustituye a la voluntad humana directa, y la manipulación de datos deviene en un acto de guerra. Asimismo, el tratamiento de la atribución como un proceso exclusivamente técnico ha mostrado sus límites, siendo imprescindible incorporar procedimientos jurídicos multilaterales que otorguen legitimidad a los actos de imputación y respuesta. La discusión también evidencia que la transición hacia un enfoque que considere la ocupación y la dominación digital como formas de agresión estatal requiere una reelaboración de los principios de soberanía, protección de civiles y proporcionalidad, en consonancia con las nuevas realidades tecnológicas y estratégicas del ciberespacio.

e-ISSN: 2737-6125 Vol. 6 Núm. 1 pp.100-117 Enero-Junio 2025 https://doi.org/10.33936/nullius.v6i1.7619

Conclusión

Este estudio sostiene que la ciberguerra constituye no una evolución técnica marginal, sino una transformación estructural del conflicto armado, que exige respuestas normativas innovadoras y urgentes. El Derecho Internacional vigente, anclado en paradigmas físicos de violencia armada, debe expandir sus categorías para incluir las agresiones algorítmicas que afectan de manera sistémica la estabilidad de los Estados y la protección de los civiles. Resulta indispensable reconocer jurídicamente el concepto de "conflicto digital latente" y establecer estándares normativos claros sobre el "dolo tecnológico" como forma de imputabilidad internacional, pues la atribución de ciberataques deberá combinar evidencia técnica y procedimientos políticos multilaterales para evitar escaladas injustificadas. La redefinición de los umbrales de hostilidad, el fortalecimiento de mecanismos de verificación internacional, y la construcción de una arquitectura jurídica específica para el contraataque cibernético son tareas inaplazables para preservar la paz, la seguridad y la dignidad humana en la era digital, infiriéndose que sólo mediante una actualización profunda y proactiva de los marcos jurídicos será posible evitar que el ciberespacio se convierta en el nuevo espacio de impunidad bélica.

Referencias bibliográficas

Ambos, K. (2021). *La parte general del derecho penal internacional: Bases de la responsabilidad individual en derecho penal internacional*. Tirant lo Blanch. https://editorial.tirant.com/es/libro/la-parte-general-del-derecho-penal-internacional-kai-ambos-9788413784879

Aparicio, J. F. (2023). Ciberguerra y cibercrimen global, cuando lo virtual transciende a lo real. *bie3: Boletín IEEE,* (31), 44-71. https://dialnet.unirioja.es/servlet/articulo?codigo=8781086

Ávila, F.(2015). *Evolución e impacto del ransomware en américa latina desde el Año 2015.* [Proyecto de grado, Universidad Nacional Abierta y a distancia UNAD] Repository Unad. https://repository.unad.edu.co/bitstream/handle/10596/42667/fyavilan.pdf?sequence=3isAllowed=y

Cassese, A. (2005). *International Law* (2nd ed.). Oxford University Press. https://global.oup.com/academic/product/international-law-9780199259397

Comisión de Derecho Internacional. (2002). *Responsabilidad del Estado por hechos internacionalmente ilícitos: Proyecto de artículos aprobado en el 53° período de sesiones (A/56/10), adoptado por la Asamblea General de las Naciones Unidas en la resolución A/RES/56/83, de 28 de enero de 2002.* Naciones Unidas. https://docs.un.org/en/A/RES/56/83

Comité Internacional de la Cruz Roja (CICR). (1977). *Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I).* https://ihl-databases.icrc.org/es/ihl-treaties/api-1977

Consejo de Europa. (2024). *El Convenio de Budapest contra la Ciberdelincuencia suma ya 75 Estados Parte*. https://www.coe.int/es/web/portal/-/budapest-convention-reaches-75-parties

Deeks, A. S. (2021). The law of cyber operations and the sovereignty of states. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (2nd ed., pp. 103–123). Edward Elgar Publishing. https://doi.org/10.4337/9781789904253.00014

Dinniss, H. A. (2021). *Cyber Operations and International Law*. Oxford University Press. https://global.oup.com/academic/product/cyber-operations-and-international-law-9780198780097

Finlay, L., & Payne, C. (2019). *The Attribution Problem and Cyber Armed Attacks*. *American Journal of International Law, 113*(2), 202–206. https://doi.org/10.1017/aju.2019.35

Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

Hathaway, O. A., & Klimburg, A. (2021). *The Law of Cyber Conflict: Advances and Emerging Challenges*. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/3283/Law_of_Cyber.pdf

Hollis, D. (2020). *Cyber Operations and International Law*. Cambridge University Press.

Instituto Nacional de Ciberseguridad (INCIBE). (2021, 26 de abril). *Proxy: navega y utiliza tu equipo de forma más segura*. https://www.incibe.es/ciudadania/blog/proxy-navega-y-utiliza-tu-equipo-de-forma-mas-segura

International Committee of the Red Cross (ICRC). (2019). *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*. https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014

International Committee of the Red Cross (ICRC). (2019). *International Humanitarian Law and Cyber Operations during Armed Conflicts*. https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

Jensen, E. T. (2015). *Cyber Warfare and Precautions Against the Effects of Attacks*. *International Law Studies*, *91*(2), 547–570. https://digital-commons.usnwc.edu/ils/vol91/iss1/21/

Kello, L. (2020). *Striking Back: The End of Peace in Cyberspace and How to Restore It*. Yale University Press. https://yalebooks.yale.edu/book/9780300253039/striking-back/

Koh, H. H. (2012). *International Law in Cyberspace*. *Harvard International Law Journal, 54*(1), 1–21. https://harvardilj.org/wp-content/uploads/sites/15/2012/04/Koh.pdf

Lin, H. (2010). *Cyber conflict and international humanitarian law*. *International Review of the Red Cross, 94*(886) https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf

Lin, H. (2021). *Cyber Threats and Norm Evolution: International Security in the Digital Age*. Stanford University Press. https://es.everand.com/book/520038645/Cyber-Threats-and-Nuclear-Weapons

Lubin, A. (2021). *The Rights to Privacy and Data Protection in Times of Armed Conflict*. *International Review of the Red Cross, 102*(913), 43–73. https://international-review.icrc.org/articles/the-rights-to-privacy-and-data-protection-923

Martínez, M. (2011). *Cuestionando la desterritorialización. Hiperterritorio, dimensiones imaginarias del espacio y nuevas cartografías.* https://catalogus.boekman.nl/pub/P13-0092.pdf#page=81

McCormack, T. L. H. (2020). *The Law of Cyber Warfare*. Cambridge University Press. https://www.cambridge.org/core/books/law-of-cyber-warfare/

Naciones Unidas. (1945). *Carta de las Naciones Unidas.* https://www.oas.org/36ag/espanol/doc_referencia/carta_nu.pdf

Naciones Unidas. (2021, 7 de julio). *Consejo de Seguridad, documento S/2021/621*. Naciones Unidas. https://docs.un.org/es/s/2021/621

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux. https://us.macmillan.com/books/9780374287269/activemeasures

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169285

Schmitt, M. N., & Vihul, L. (2020). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524

Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.* Cambridge University Press.

Shackelford, S. J. (2020). *Cyber War and Peace: Building a Safer Digital World*. Cambridge University Press.

Shackelford, S. J., Douzet, F., & Ankersen, C. (Eds.). (2022). *Cyber peace: Charting a path toward a sustainable, stable, and secure cyberspace*. Cambridge University Press.

Tsagourias, N., & Buchan, R. (2021). *Research Handbook on International Law and Cyberspace* (2nd ed.). Edward Elgar Publishing. https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781789904246.html

Valencia. E. (2024). Implicaciones y desafíos del ciberespacio para la aplicación del Derecho Internacional. *Revista Política Internacional, 6*(1), 219-233. https://doi.org/10.5281/zenodo.10396392