ENTRE SOMBRAS DIGITALES Y GRIETAS NORMATIVAS

EL CIBERESPACIO COMO EL NUEVO CAMPO MINADO DEL IUS AD BELLUM

Autores
Liz Cachi
0009-0000-9969-6789

Ana Lucia Campos
0009-0002-7602-4079

Resumen

La disrupción de las tecnologías digitales ha consolidado al ciberespacio como un nuevo escenario de confrontación interestatal en el que las operaciones o ataques cibernéticos pueden generar efectos comparables con los de una agresión armada convencional y directa. Sin embargo, *el ius ad bellum*, concebido para regular la guerra en contextos tradicionales (es decir, físicos o directos) podría verse limitado en brindar respuesta y un marco jurídico aplicable a las dinámicas digitales. En ese sentido, la presente investigación parte de la hipótesis de que el marco jurídico vigente —que tiene como piedra angular a las máximas de prohibición de uso de la fuerza y el derecho a la legítima defensa consagrados en la Carta de las Naciones Unidas— debe ser adaptado para responder a las particularidades técnicas y estratégicas de una "guerra cibernética".

Así, el objetivo central de este estudio es reinterpretar el *ius ad bellum* incorporando el umbral cibernético. Para esto, se propone redefinir el concepto de "ataque armado", fortalecer los mecanismos de atribución y responsabilidad internacional, así como la aplicación de los principios de proporcionalidad y necesidad a la legítima defensa digital. Mediante un análisis cualitativo de las normas, doctrinas y casos empíricos se busca arribar a una propuesta útil de reinterpretación del ius ad bellum y un marco híbrido que articule el Derecho Internacional con la seguridad digital, integrando herramientas jurídicas y técnicas que brinden una respuesta legítima, eficaz y verificable ante casos de ataques cibernéticos interestatales.

► ***Palabras claves:*** *Ciberespacio, ius ad bellum, uso de la fuerza, ciberataque, poder, Relaciones Internacionales*

Between Digital Shadows and Normative Gaps: Cyberspace as the New Minefield of Ius ad Bellum

Abstract

The disruption of digital technologies has consolidated cyberspace as a new arena for interstate confrontation, in which cyber operations or attacks can have effects comparable to those of conventional, direct armed aggression. However, ius ad bellum, designed to regulate warfare in traditional (i.e., physical or direct) contexts, may be limited in providing a response and a legal framework applicable to digital dynamics. In this regard, this research is based on the hypothesis that the current legal framework—whose cornerstone is the prohibition of the use of force and the right to self-defense enshrined in the Charter of the United Nations—must be adapted to respond to the technical and strategic particularities of 'cyberwarfare'.

Thus, the central objective of this study is to reinterpret ius ad bellum by incorporating the cyber threshold. To this end, it proposes to redefine the concept of 'armed attack', strengthen mechanisms of attribution and international responsibility, as well as the application of the principles of proportionality and necessity to digital self-defense. Through a qualitative analysis of norms, doctrines, and empirical cases, it seeks to arrive at a useful proposal for the reinterpretation of ius ad bellum and a hybrid framework that articulates international law with digital security, integrating legal and technical tools that

► ***Keywords:*** *Cyberspace, ius ad bellum, use of force, cyberattack, power, International Relations*

1. Introducción

El desarrollo exponencial de tecnologías disruptivas y el ambiente digital ha puesto de relieve al ciberespacio como nuevo dominio de conflicto, posiblemente equiparable a los escenarios bélicos tradicionales. Dicho "cibersistema", caracterizado por la interconectividad global, la intangibilidad de sus operaciones y la participación de actores (tanto estatales como no estatales) parece desafiar los fundamentos clásicos del Derecho Internacional Público (en adelante, "DI") que regulan el uso legítimo de la fuerza.

De hecho, la realización de ciberataques dirigidos a infraestructuras críticas, sistemas financieros, redes de comunicación estatal, entre otros elementos fundamentales para los Estados, pueden producir efectos comparables a los de una agresión armada convencional. Pero dicha calificación presenta problemas y ambigüedades en relación a la virtualidad como el espacio en el que dichos ataques se desarrollan o son ejecutados, así como a la dificultad para atribuir responsabilidades y la ausencia o inexistencia de daños físicos inmediatos.

Es así que el presente trabajo tiene como propósito analizar la forma en la que el concepto de *ius ad bellum* enfrenta los desafíos que plantea el considerar a los conflictos cibernéticos (y al ciberespacio en general) como un nuevo espacio para el ejercicio del uso de la fuerza. En efecto, la relevancia de esta investigación radica en el hecho de que el ciberespacio conmina a redefinir las fronteras del poder y la soberanía estatal, erosionando los paradigmas sobre los que se construyó el *ius ad bellum* original, así como a redefinir dicho concepto desde una perspectiva adaptativa, superando la dicotomía entre lo normativo y la *praxis*.

Para ello, se formula la siguiente pregunta: "¿Cómo debe reinterpretarse el *ius ad bellum* para responder adecuadamente a los desafíos jurídicos que plantea el considerar al ciberespacio como un nuevo escenario de conflicto internacional?", para lo cual se aplica una metodología cualitativa, analítica y comparativa, basada en la revisión sistemática de fuentes primarias del derecho internacional (tales como la Carta de la ONU) en diálogo con doctrina internacional especializada, a efectos de evaluar la adaptación conceptual referida.

2. El marco jurídico internacional y sus límites

El derecho internacional público consolidó desde 1945 un marco jurídico claro respecto del uso de la fuerza: la Carta de las Naciones Unidas prohíbe el recurrir a la fuerza armada en las relaciones internacionales, exceptuando el ejercicio de la legítima defensa. Esta normativa sigue vigente y, por ello, se aplica incluso frente a escenarios de amenaza y conflicto modernos tales como los ciberataques. No obstante, el escenario del ciberespacio plantea límites y ambigüedades en la aplicación de este marco jurídico.

Y es que la ONU tuvo como propósito originario asegurar la paz y la seguridad dentro de la comunidad internacional, puesto que, para 1945, el contexto global se encontraba marcado por una historia reciente de violencia, conflictos armados y una serie de prácticas que se buscaban erradicar definitivamente (Álvarez, 2020, p. 4). Por ello, se estableció el principio que prohíbe el uso de la fuerza en las relaciones entre Estados; sin embargo, y como se abordará a lo largo del presente trabajo, en la actualidad, con el surgimiento de capacidades en el ciberespacio, surge una interrogante inevitable: ¿Qué ocurre si los Estados deciden emprender una guerra cibernética? (Álvarez, 2020, p. 4). En efecto, la Carta de las Naciones Unidas (en adelante, la "Carta de la ONU") fue pensada en un contexto de agresiones y conflictos bélicos tradicionales (por vía terrestre, aérea o marítima) sin prever un dominio virtual en el que los ataques no encajen de forma perfecta en las nociones o definiciones clásicas que aborda el ius ad bellum. Por tanto, cuando se aplican las normas tradicionales a tecnologías o situaciones emergentes, el ejercicio de traducción a menudo pone de manifiesto lagunas o incongruencias que antes no se habían previsto ni anticipado (Corn y Jensen, 2018, p. 127).

De esta forma, en ausencia de un tratado específico para el ciberespacio, el DI preexistente debería resultar aplicable a los ataques cibernéticos. ¿Pero realmente otorga una respuesta idónea a la modalidad cibernética de los conflictos en la era de las nuevas tecnologías? A efectos de responder ello, la presente sección se centrará en desarrollar los principios fundamentales de la Carta de la ONU respecto del uso de la fuerza y, seguidamente, se analizarán algunas lagunas o desafíos que surgen de su aplicación ante los ciberataques.

2.1 Dificultad para definir "ataque armado"

De forma preliminar, el numeral 4 del artículo 2 de la Carta de la ONU establece que "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". Asimismo, el artículo 51 de la Carta de la ONU define las bases para ejercer el derecho de legítima defensa, estipulando que un Estado puede ejercer tal derecho si se produce un ataque armado contra un miembro de las Naciones Unidas hasta que el Consejo de Seguridad haya tomado medidas para mantener la paz internacional.

Al respecto, es menester señalar que el principio rector en el DI es la prohibición del uso de la fuerza en las relaciones entre Estados; a excepción de si se gatilla la legítima defensa (Álvarez, 2020, p. 5). Ahora, aún cuando un Estado es objeto de un ataque y tiene el derecho de defenderse, hay algunas condiciones: primero, debe haberse producido un "ataque armado"; segundo, la respuesta debe ajustarse a elementos como i) la necesidad, esto es, que no exista otro medio eficaz para repeler la agresión; ii) la proporcionalidad, que implica que la reacción se corresponda con la magnitud del daño ocasionado; y iii) oportunidad, que exige actuar en un plazo razonable sin dilaciones indebidas (Álvarez, 2020, p. 5).

No obstante, pese a estos alcances que brindan las disposiciones de la ONU, se ve que en ninguno de estos artículos se define lo que es un "ataque armado" ni se especifica cómo traducir o aplicar dicho concepto a ofensivas cibernéticas. Así, si bien se puede partir de una definición clásica que contempla a dicha figura sólo como la acción de fuerzas armadas regulares a través de una frontera internacional, se partirá de la (re)definición brindada por Burkadze, quien sostiene que ello consiste también en los actos de fuerza que ejerce un Estado o sus grupos armados, de todo tipo, contra otro Estado y que, por su gravedad, equivalen a un ataque armado real llevado a cabo por fuerzas regulares (2022, p. 18).

Al respecto, los Estados han tenido que extrapolar los criterios basados en los efectos de dicha acción y, por ello, la opinión prevalente es que el ciberataque puede equivaler a un ataque armado si sus consecuencias son comparables a las de un ataque militar convencional. En esa línea, la norma 13 del Manual de Tallin, un estudio académico no vinculante organizado por el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN, precisa que una operación cibernética constituirá un ataque armado dependiendo de su magnitud y sus efectos, y que un Estado que sea objeto de ello puede ejercer su derecho inherente a la defensa (Schmitt, 2013).

Ante ello, entonces, se presenta la dificultad de determinar qué es lo que se puede considerar como un "daño menor" que no active la legítima defensa armada en escenarios de ciberataques. Asimismo, se debe determinar lo entendido como comparable a un ataque armado clásico, considerando que el espacio en el que los ciberataques se producen no es tradicional, sino virtual e indirecto, y no producen la pérdida de vidas, daños físicos, entre otras consecuencias que, a simple vista, alcancen de forma efectiva la categoría especial de ataque armado y justifiquen una contraofensiva militar.

2.2 El problema de la atribución a actores estatales y no estatales

La atribución se refiere al proceso de identificar el origen de un ciberataque malicioso y es fundamental para adoptar medidas legales, técnicas, entre otras, destinadas a prevenir y reprimir los ciberataques, disuadir nuevos y exigir responsabilidades a los autores y patrocinadores de estos. Así, la atribución puede fomentar el cumplimiento del DI aplicable al ciberespacio que regula la conducta cibernética (Tsagourias, 2024, pp. 24-25).

El artículo 8 del proyecto de la Comisión de Derecho Internacional sobre responsabilidad del Estado, prevé, además de la responsabilidad tradicional por ataques perpetrados de forma directa, que un Estado sólo será responsable de actos cometidos por individuos o grupos privados si estos "actúan siguiendo sus instrucciones, bajo su dirección o bajo su control". Al respecto, la Corte Internacional de Justicia planteó que tal control debe ser efectivo en operaciones concretas para imputar tales actos como propios del Estado (Caso Nicaragua vs. EE.UU., 1986).

De esa forma, el segundo gran desafío jurídico que se presenta al aplicar el ius ad bellum ante supuestos de ciberataques es el determinar o identificar quién es el responsable de dichas ofensivas. En efecto, en el ámbito del ciberespacio, la atribución de responsabilidad internacional es más opaca y complicada en la medida en que los atacantes pueden ocultar su rastro técnico empleando servidores especializados; pueden ser grupos independientes, tales como hackers o colectivos terroristas; y el Estado responsable puede negar su responsabilidad alegando que se trataron de ataques particulares y desvinculados de su instrucción o control.

La práctica reciente demostró que ciertas agresiones pueden considerarse como ataques armados que habilitan la defensa propia, pero la dificultad sigue estando en las herramientas con las que se cuenta para probar ello. Optar por reconocer plenamente que los ataques cibernéticos, sobre todo aquellos que obedecen a ofensivas independientes, habilitan al Estado víctima a ejercer su derecho a responder en legítima defensa con fuerza contra sus agresores, alegando una necesidad urgente, sigue siendo una posición controversial.

Entonces, la falta de atribución clara debería, en primera instancia, frenar la respuesta armada del Estado víctima por razones jurídicas y políticas, pues actuar militarmente sin tener certeza de a quién atribuir el ataque puede violar los principios de la Carta de la ONU y producir agresiones ilegítimas. De esta forma, tal como lo plantea Martabit, la dificultad de determinar la atribución de actos hostiles en el ciberespacio es alta y la tentación política a justificar actos de defensa, sin legitimidad jurídica, también lo es (2019, p. 9)

3. El ciberespacio como desafío disruptivo

En este apartado resulta fundamental precisar el concepto de "ciberespacio". Aunque existen diversas definiciones, para efectos prácticos se tomará la más sencilla: el ciberespacio es el lugar inmaterial que no se limita únicamente a todo lo que ocurre en Internet (Campos, 2022, p. 6). Es decir, se trata de un espacio radicalmente distinto a los ámbitos tradicionales, intangible, creado artificialmente, reconocido e instaurado como un nuevo dominio de operaciones, junto con los espacios terrestre, marítimo, aéreo o espacial (Campos, 2022, p. 6).

Ahora bien, a partir de lo desarrollado en los apartados anteriores, se puede afirmar claramente que el arribo del ciberespacio como dominio operativo, entendido como el entorno en el que se desarrollan acciones ofensivas y defensivas, y también como dominio estratégico, por su papel determinante en las dinámicas de poder global, pone a prueba los cimientos del ius ad bellum. En otras palabras, el ciberespacio transformó profundamente el paradigma de aplicación de los principios de prohibición de la amenaza y el uso de la fuerza, los cuales son descritos como "la piedra angular de la paz, el corazón de la Carta de Naciones Unidas y la regla básica del derecho internacional

contemporáneo" (Robles, 2016, p. 111).

Y es que, a diferencia de los conflictos armados convencionales, las agresiones en el entorno digital pueden ser simultáneamente transnacionales, anónimas, de rápida expansión y ejecutadas tanto por Estados como por intermediarios o individuos, lo que complica la aplicación de las categorías jurídicas clásicas propuestas por el DI. Sobre todo, si se tiene en cuenta que ese entorno virtual, desde el punto de vista jurídico, no se encuentra bajo la soberanía de ningún Estado (Quispe, 2024, p. 157).

Es precisamente por ello que este apartado sostiene que la verdadera "disrupción" del fenómeno cibernético no reside únicamente en su carácter tecnológico, sino en la desproporción entre los grandes y diversos efectos que puede generar y los umbrales jurídicos establecidos para lo considerado como "uso de la fuerza armada tradicional". Ello, debido a que la arquitectura jurídica existente no fue pensada teniendo en cuenta este nuevo fenómeno, exige replantear no solo las categorías jurídicas vigentes, sino también la forma en que interactúan el DI y la seguridad global.

Por esta razón, esta sección se enfocará i) en el análisis de casos emblemáticos relacionados con esta problemática; ii) en la diferenciación entre espionaje, sabotaje y uso de la fuerza, lo que se denomina la "zona gris"; iii) así como en las implicancias estratégicas del ciberespacio como instrumento de poder y coerción. Se resaltará la tensión existente entre la necesidad de (i) adaptación normativa, pues, si el derecho no evoluciona, corre el riesgo de volverse obsoleto y quedarse sin respuesta ante ataques digitales altamente perjudiciales; y (ii) los riesgos asociados a una posible escalada, ya que podría reducir excesivamente el umbral del "uso de la fuerza" y justificar respuestas militares que antes no hubieran sido legítimas.

3.1 Casos paradigmáticos: Estonia (2007), Stuxnet (2010) y Ucrania

Se mencionó que el estudio de la práctica internacional permite identificar situaciones en las que se emplean acciones cibernéticas con fines específicos, que no siempre son lícitos y cuya calificación jurídica resulta compleja al tratarse de un problema emergente con varias aristas (Robles, 2016, p. 115). En ese sentido, conviene mencionar casos ilustrativos que permiten comprender mejor los desafíos que plantea el uso del ciberespacio como herramienta de poder.

3.1.1. Estonia 2007: umbral del uso de la fuerza

Para comprender adecuadamente este caso, es necesario remontarse a su contexto histórico. Durante la Segunda Guerra Mundial, la entonces Unión Soviética erigió una estatua de bronce en la ciudad de Tallin, capital de Estonia (Repetto, 2021, p. 31). Este monumento generó una profunda división de opiniones: mientras que la población estonia lo interpretaba como un símbolo de ocupación y represión soviética, los rusos étnicos residentes en Estonia lo consideraban un homenaje a los soldados soviéticos caídos en combate (Repetto, 2021, p. 31). Esta tensión histórica constituye el trasfondo del conflicto que, años más tarde, desembocará en uno de los ciberataques más emblemáticos registrados a nivel estatal.

En abril de 2007, el gobierno estonio optó por retirar dicha estatua. Sin embargo, a consecuencia de ello, se produjeron dos noches de intensas protestas y disturbios en Tallin, conocidas como la "Noche de Bronce" (Repetto, 2021, p. 32). Tras esto, Estonia fue víctima de un ciberataque masivo, cuya fuente principal se identificó en territorio ruso (Repetto, 2021, p. 32). La modalidad empleada fue un ataque distribuido de denegación de servicio (DDoS), dirigido principalmente contra sitios web gubernamentales, medios de comunicación y entidades bancarias (Repetto, 2021, p. 32). Por su parte, los servicios de emergencia también se vieron afectados, poniendo en riesgo la vida de miles (Repetto, 2021, p. 32).

Ahora bien, lo resaltante de este caso es que la comunidad internacional no llegó a calificar este hecho como un "ataque armado", pues se consideraba que no se había alcanzado el umbral de escala y efectos para definirlo como tal en el marco del ius ad bellum (Repetto, 2021, p. 32). No obstante, a raíz de este, la OTAN decidió crear el Centro de Excelencia para la Ciberdefensa Cooperativa (CCDCOE), que a su vez estableció un Grupo Internacional de Expertos compuesto por juristas y técnicos, con el objetivo de sistematizar y establecer un conjunto de reglas de DI aplicables o susceptibles de ser aplicadas al ciberespacio, lo que dio como resultado el denominado "Manual de Tallin" (Campos, 2022, p. 13).

Este manual constituyó un instrumento de soft law que recopiló principios y normas aplicables al ámbito del ciberespacio, sustentado en el consenso de un grupo de académicos especializados (Campos, 2022, p. 13). Es por esto que el caso de Estonia representa un ejemplo paradigmático no solo por evidenciar las consecuencias concretas de una acción cibernética sobre un Estado, sino también por marcar un punto de inflexión en la forma en que los países y las organizaciones internacionales comenzaron a abordar el problema de la ciberseguridad (Robles, 2016, p. 115).

3.1.2. Stuxnet 2010: sabotaje con daños físicos y la frontera del “ataque armado”

También existen casos que han marcado hitos significativos sobre todo por su impacto técnico, estratégico y jurídico. Uno de los más emblemáticos es el ataque con el software malicioso (*malware*) conocido como Stuxnet, cuyo análisis permite comprender cómo el ciberespacio es utilizado como un instrumento de sabotaje con consecuencias concretas.

Este malware fue diseñado específicamente para manipular controladores industriales (PLC) e interferir en el funcionamiento de las centrifugadoras de la planta nuclear de Natanz, en Irán (Silva, 2018, p. 303). Esta amenaza pronto despertó un inusitado interés entre los expertos en seguridad informática, debido al alto nivel de sofisticación y al impacto potencial que podía generar (Silva, 2018, p. 300). Es así que Stuxnet empezó a ser considerado una auténtica revolución en el ámbito militar, al traspasar los límites del ciberespacio y provocar daños físicos en el mundo real, evidenciando el potencial del ciberespacio como herramienta de sabotaje con efectos materiales directos (Silva, 2018, p. 301).

Al respecto, de acuerdo con las interpretaciones sobre DI recogidas en el Manual de Tallin, los ciberataques pueden ser considerados como “ataques armados” únicamente cuando provocan daños físicos significativos, como lesiones, muertes o destrucción de bienes (Silva, 2018, p. 307). En cambio, aquellos vinculados a actividades de inteligencia, robo de información o interferencias menores no alcanzan el umbral jurídico y, por ende, no podrían considerarse como ataques armados (Silva, 2018, p. 307).

Además, la comunidad internacional no ha calificado a ningún ciberataque como ataque armado. Aunque a pesar de ello, el caso de Stuxnet, a diferencia de otros como el ataque a Estonia mencionado previamente, parece haber alcanzado ese umbral, al haber paralizado el programa nuclear iraní, aunque sigue sin haber consenso de ello (Silva, 2018, p. 307).

Y es que “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” (Almache y Berríos, 2025, p. 58).

3.1.3. Ucrania: ciberataques a infraestructura crítica en contexto de conflicto

La invasión rusa a Ucrania, iniciada en el 2022, marcó el estallido de una guerra abierta entre ambos Estados, cuyo conflicto se venía gestando desde 2014 (Campos, 2025, p. 5). Este escenario bélico no solo ha tenido consecuencias devastadoras en el plano humano y geopolítico, sino que también ha revelado una nueva dimensión del enfrentamiento interestatal: la integración estratégica de las ciberoperaciones en el desarrollo del conflicto.

En este sentido, Ucrania se configura como un laboratorio donde convergen las tecnologías digitales y las dinámicas propias de la guerra entre Estados, planteando serios desafíos para el DI. Y es que, con el objetivo de desestabilizar al gobierno ucraniano, los ciberataques han tenido como blanco infraestructuras críticas (Muñoz, 2024, p. 17). Entre ellas, están los sistemas eléctricos, entidades financieras y plataformas gubernamentales (Arré, 2025, p. 46). Un caso emblemático es la operación WhisperGate, llevada a cabo en Ucrania en 2022, cuyo objetivo fue la destrucción de información sensible y la interrupción de sistemas informáticos estratégicos en el contexto previo a la invasión rusa (Arré, 2025, p. 46).

Por ello, una de las principales lecciones que deja este conflicto es la importancia de promover una respuesta articulada entre las agencias gubernamentales y los privados (Muñoz, 2024, p. 17). De hecho, tanto la Unión Europea como la OTAN, apoyaron el desarrollo y capacidad de reacción de Ucrania frente a los ataques digitales de los cuales puede ser víctima, además de estimular la inserción de programas dirigidos a disminuir los efectos negativos de la desinformación (Muñoz, 2024, p. 17).

En definitiva, al poner en evidencia vulnerabilidades críticas, desde sistemas financieros hasta infraestructuras nucleares y redes eléctricas, los casos de Estonia, Stuxnet y Ucrania revelan que el ciberespacio se ha consolidado como un escenario que ha transformado profundamente los parámetros tradicionales establecidos por el DI.

3.2. Delitos informáticos y uso de la fuerza: la "zona gris"

3.2.1. Definiciones de espionaje y sabotaje

En este apartado es clave señalar que, en virtud del contexto actual de creciente digitalización de las relaciones sociales y económicas, el derecho se vió obligado a adaptarse a nuevas formas de criminalidad vinculadas al uso de tecnologías de la información. Así, resulta esencial abordar dos delitos informáticos frecuentes que afectan directamente a los sistemas informáticos de cualquier país. El sabotaje y el espionaje son delitos que se pueden ejecutar sin necesidad de internet y cuya manifestación de su significativo potencial se da dentro del entorno digital (Mayer y Vera, 2020, p. 223). Sin embargo, para efectos del presente trabajo no se profundizará a detalle en cada uno, sino que se van a resaltar sus particularidades.

Por un lado, el término "espionaje" se configura como una conducta vinculada a la vulneración de secretos, la cual puede manifestarse tanto mediante el acceso no autorizado a información confidencial como a través de la divulgación indebida de datos obtenidos legítimamente (Mayer y Vera, 2020, p. 225). Además, este delito adquiere especial relevancia cuando se orienta a objetivos estratégicos, como el acceso a información confidencial estatal, especialmente si se trata de defensa y seguridad (Romeo, 1996, p. 434).

En ese sentido, el espionaje informático constituye una forma sofisticada de intrusión digital que busca acceder, sin autorización, a información confidencial almacenada en sistemas informáticos y está principalmente orientado a la obtención estratégica de datos sensibles, lo que lo convierte en una herramienta clave dentro de los conflictos interestatales.

Por otro lado, el sabotaje se refiere a acciones que alteran, degradan o destruyen sistemas o datos, y cuyo objetivo principal es afectar funcionalidades críticas. De hecho, este tipo de acciones llegan a involucrar estrategias militares o la estructura operativa de las fuerzas armadas, lo que representa una amenaza directa a la soberanía nacional y, consecuentemente, a la estabilidad internacional (Romeo, 1996, p. 439).

Lo relevante y crítico de esta conducta es que, a diferencia del espionaje que busca obtener información, el sabotaje tiene como finalidad directa la paralización o el deterioro de los sistemas atacados. Es por ello que su ejecución puede traer graves consecuencias, especialmente en contextos de conflicto armado o de tensión internacional.

3.2.2. La zona gris

En palabras de Rodríguez, la denominada "zona gris" es aquel espacio intermedio en el que se desdibujan las fronteras de la guerra y la paz (2025, p. 2). Es un espacio en el que, aunque no alcanza el umbral de conflicto, sí posee acciones hostiles o coercitivas lo suficientemente significativas como para llegar a comprometer la seguridad global (Rodríguez, 2025, p. 2).

Se trata, pues, de una zona cuyas acciones hostiles se sitúan debajo de los umbrales que jurídicamente se consideran como "uso de la fuerza" o "ataque armado", pero que de todas formas conllevan un enfrentamiento no convencional, desgastando las capacidades de los Estados, generando costos e involucrando objetivos estratégicos.

En este contexto, no es ajeno afirmar que el ciberespacio se ha consolidado como uno de los principales escenarios de la zona gris, al permitir la ejecución de tácticas como la guerra cibernética, operaciones encubiertas, desinformación, entre otros (Rodríguez, 2025, p. 2).

Por lo tanto, la "zona gris" representa un desafío complejo y multidimensional que exige una respuesta igualmente estructurada y estratégica (Rodríguez, 2025, p. 3). Esto es para que las amenazas que surgen dentro del ciberespacio y que tratan de soslayar las reglas del DI sean enfrentadas eficazmente. Comprender a la zona gris y su relación con el escenario "ciberespacial" resulta imperativo para empezar a construir la defensa cibernética reconociendo a la cooperación internacional como un factor primordial.

3.3. El ciberespacio como instrumento de poder y coerción

De lo anteriormente analizado, se afirma que el ciberespacio se ha convertido en un instrumento estratégico de poder, utilizado por los Estados para fines políticos, económicos, militares, entre otros. Con lo cual, en este nuevo escenario, lo que se puede denominar como "ciberpoder" no solo emerge como un componente esencial de la seguridad nacional y de la defensa en el entorno digital, sino también como un reto para el DI.

Y es que el ciberespacio es descrito como un entorno amorfo no circunscrito a un lugar físico o geográfico determinado; sino presente en todas partes y al mismo tiempo en ninguna (Llorens, 2017, p. 792). A partir de aquí es que el DI y sus conceptos convencionales tienen el desafío de adaptarse a esta nueva realidad con características únicas (Llorens, 2017, p. 792).

Se trata de uno de los debates más importantes en relación a las operaciones cibernéticas: la aplicabilidad del ius ad bellum, es decir, de las normas que regulan el uso de la fuerza (Llorens, 2017, p. 797). Convencionalmente, es menester acudir al ya comentado artículo 2, párrafo 4, de la Carta de las Naciones Unidas, que establece la obligación de los Estados de "abstenerse de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado" (Llorens, 2017, p. 798).

Aunado a ello, es importante señalar que, precisamente, el ius ad bellum se fundamenta en la prohibición de amenazar o emplear la fuerza contra otro Estado; no obstante, existe la posibilidad de que un Estado otorgue su consentimiento para que otro utilice la fuerza armada, lo que, a priori, constituye una vulneración del principio que proscribe el ius ad bellum (Regueiro, 2025, p. 6).

Sin embargo, es evidente que para ello también se deben seguir una serie de criterios, entre los cuales se encuentra el que el accionar del Estado que recibe el consentimiento debe ajustarse estrictamente a límites fijados, dado que cualquier actuación fuera de estos límites daría como consecuencia su inmediata exclusión como excepción de ilicitud (Regueiro, 2025, p. 6). Dada la delicadeza del tema, es imperativo que se pueda analizar la existencia del consentimiento en función a si es conforme con las normas propuestas por el DI de los Derechos Humanos y el Derecho Internacional Humanitario (Regueiro, 2025, p. 6).

Ahora bien, extrapolando lo comentado al contexto cibernético, es claro que el consentimiento de la fuerza armada mediante el uso de armas cibernéticas abre una nueva puerta de análisis respecto a los alcances de este consentimiento. Asimismo, cabe mencionar que uno de los principales problemas surge al determinar en qué circunstancias una operación cibernética infringe la prohibición contenida en el artículo 2 antes señalado; sin embargo, se estima que este desafío hermenéutico exige, ante todo, precisar el alcance del concepto de "fuerza" y establecer cuándo una operación cibernética alcanza el umbral previsto por el DI para ser calificada como violatoria de la norma (Llorens, 2017, p. 801).

Siguiendo el mismo orden de ideas, también surgen varios problemas en torno al derecho de legítima defensa frente a las ciberoperaciones, entre las cuales se encuentran las siguientes: (i) si un ataque contra infraestructuras cibernéticas civiles puede considerarse un "ataque armado" que active la legítima defensa; (ii) si operaciones que no causen daños físicos, pero que generen consecuencias graves de carácter funcional o económico, pueden alcanzar dicho umbral; y (iii) si las operaciones cibernéticas ejecutadas por actores no estatales pueden dar lugar al ejercicio del derecho de legítima defensa (Llorens, 2017, pp. 808-809).

Sin embargo, pese a todos los problemas que pueden surgir es imperativo tener en cuenta que los que tienen en "última instancia" el poder de decisión son los Estados. Y es que, según lo dispuesto en el artículo 36 del Protocolo Adicional de 1977 a los Convenios de Ginebra de 1949, los Estados son los que evalúan si una nueva arma resulta incompatible con alguna norma del DI (Regueiro, 2025, p. 5). Al respecto, el Comité Internacional de la Cruz Roja precisa que esta valoración debe considerar el uso ordinario previsto para el arma en el momento de la revisión, puesto que si se omite este análisis es claro que el responsable por un potencial daño ilícito que se produzca será el Estado (Regueiro, 2025, p. 5).

Por otro lado, es claro que el empleo de drones operados a distancia introduce una creciente automatización en el campo de batalla, en la medida en que la intervención humana se vuelve cada vez menos relevante y que estas armas no están prohibidas por el DI (Regueiro, 2025, p. 5). Ello se debe a que el vínculo, aunque remoto, entre el operador humano y la máquina se considera suficiente para garantizar un control efectivo que asegure el cumplimiento de las normas internacionales (Regueiro, 2025, p. 5). Se considera que el operador humano será el encargado de dirigir el sistema hacia objetivos militares específicos y obligar a la máquina a respetar el principio de distinción, evitar ataques indiscriminados y garantizar la observancia de los derechos humanos (Reguiero, 2025, pp. 5-6).

Son consideraciones que, aunque resaltan la importancia del control humano, no se debe olvidar que este control debe ser efectivo no solo en la teoría sino en la práctica. Y lo que se observa es que la capacidad humana para intervenir de manera efectiva se reduce y la posibilidad de cometer errores se incrementa debido a la automatización, cuestionando si el control remoto asegura la aplicación de principios como distinción y proporcionalidad.

Sea como fuere, lo cierto es que lo comentado permite afirmar que el ciberespacio se ha consolidado como un multiplicador estratégico de poder, al permitir la ejecución de acciones coercitivas discretas, pero altamente efectivas, sin necesidad de cruzar los umbrales establecidos por el ius ad bellum. Esta característica lo convierte en un escenario privilegiado para la confrontación dentro de la denominada zona gris, donde las distinciones entre paz y conflicto se tornan difusas. Ello pone de manifiesto, por una parte, que el DI enfrenta el desafío de adaptarse a estas nuevas formas de hostilidad y, por otra, que el ciberespacio debe ser entendido como un escenario de poder estratégico y cuya regulación es imperativa e ineludible, tomando como eje central la importancia del control humano.

4. Aportes desde las Relaciones Internacionales a los desafíos que plantea el ciberespacio

Ahora bien, el ciberespacio, al tiempo que debilita nociones tradicionales como la soberanía y las fronteras físicas, refuerza dinámicas de competencia interestatal en un entorno digital. Con lo cual, es evidente que su estudio como escenario de conflicto no puede abordarse únicamente desde el Derecho, ya que sus efectos van más allá de la interpretación normativa, en la medida en que repercuten directamente en la estructura del poder y la seguridad global.

En esa línea, las Relaciones Internacionales (en adelante: RRII) ofrecen otras perspectivas para comprender cómo los Estados, y cada vez más los actores no estatales, se posicionan frente a los desafíos que plantea este nuevo espacio disruptivo. Sobre todo si se tiene en cuenta que el ciberespacio ha dejado de ser solo una herramienta técnica para convertirse en un escenario autónomo de confrontación estratégica que exige una redefinición profunda de los principios postulados por el DI.

4.1. Las dinámicas de poder en el ciberespacio

En línea con lo señalado previamente, los desafíos propios del ciberespacio han producido una transformación significativa al conferir una capacidad de influencia inédita a los distintos actores e instituciones involucrados en su regulación y gestión global (Aguirre y Morandé, 2016, p. 3). Precisamente por ello es importante mencionar que este escenario ha sido la oportunidad perfecta de expansión del ámbito de acción de aquellos que siempre han aspirado a definir reglas y a ejercer el control.

En este sentido cobra relevancia la definición dada a las potencias dentro de la disciplina de las RRII, es decir, "aquellos estados que establecen las reglas del juego y que disponen de recursos y son capaces de movilizarlos para defender dichas reglas" (Franco, 2024, p. 8). Además, esa capacidad para establecer las reglas viene acompañada con el poder suficiente como para influenciar en la dinámica interestatal (Franco, 2024, p. 8).

Ahora bien, en el contexto del sistema cibernético, se considera como ciberpotencias a aquellos Estados que poseen ciberpoder, entendido como la capacidad de utilizar el ciberespacio para alcanzar determinados objetivos estratégicos (Franco, 2024, p. 8). Este poder digital se convierte en una herramienta clave para proyectar influencia y ejercer control en el ámbito internacional.

Así, mientras potencias como Estados Unidos, China y varios países de la Unión Europea buscan mantener su liderazgo en el ciberespacio, lo que refleja la estructura jerárquica del sistema internacional, basada en sus capacidades e influencia en el entorno digital; al mismo tiempo, los actores no estatales han identificado que el desarrollo y el acceso a las tecnologías de la información y comunicación (TIC) ampliaron significativamente sus posibilidades de participación en la esfera internacional (Aguirre y Morandé, 2016, pp. 3-4).

En otras palabras, las potencias han reconocido que el entorno digital constituye un componente esencial para proyectar su poder a nivel global y, por ello, se ven obligadas a desarrollar capacidades tanto ofensivas como defensivas para la protección de su principal interés: mantener su dominio global.

Al respecto, se encuentran una serie de potencias que desempeñan papeles importantes dentro de la dinámica de poder que rige el orden mundial actual y que, evidentemente, buscan copar el ciberespacio para mantener su dominio. En primer lugar, no es ajeno señalar que Estados Unidos ocupa el liderazgo global en materia de ciberpoder, siendo considerado por la doctrina como una "hiperpotencia" cibernética; mientras que, por otro lado, China se posiciona como una "superpotencia" ubicada muy cerca, pues ambos destacan por su capacidad tecnológica y económica (Franco, 2024, p. 8). Rusia, por su parte, completa el top 3 al ser calificada como una "gran potencia" en el ámbito cibernético, al ejecutar operaciones ofensivas y ejercer un notable control sobre la información digital (Franco, 2024, p. 9).

En un nivel inferior a estas tres principales potencias, podemos encontrar a países como Reino Unido, Australia, Países Bajos, Corea del Sur, Vietnam y Francia, que, si bien no cuentan con la misma infraestructura, influencia ni capacidades tecnológicas, logran destacar por encima de otras naciones en el ámbito del ciberpoder, razón por la cual son calificados como "potencias" (Franco, 2024, p. 9). Finalmente, no se debe dejar de lado el papel que están empezando a tomar países como Israel o Corea del Norte al insertarse cada vez más en el desarrollo cibernético y la ciberdefensa, de ahí que sean calificadas como "potencias emergentes" (Franco, 2024, p. 9).

Por lo expuesto, resultan cruciales los aportes que nos ofrecen las RRII, en tanto observan al ciberespacio como un escenario en donde se reconfiguran las dinámicas clásicas de poder y cooperación. Y ello, a su vez, lleva a una tensión jurídica relevante que empieza con la pregunta de en qué medida los Estados pueden implementar políticas de control y vigilancia como manifestación de su soberanía, sin contradecir principios internacionales fundamentales, en un espacio cuyas acciones trascienden las fronteras y cuestionan permanentemente la capacidad de los Estados.

4.2. El uso de las teorías de las Relaciones Internacionales como marco interpretativo

Ahora bien, dada la ya comentada complejidad del ciberespacio, es necesario contar con marcos teóricos que ayuden a interpretar las motivaciones y comportamientos de los Estados en este entorno. Las principales escuelas de pensamiento en RRII, como el realismo, el liberalismo y el constructivismo, ofrecen enfoques distintos, pero complementarios para analizar el papel del ciberpoder en la dinámica global, así como los desafíos y posibilidades que plantea para la evolución del ius ad bellum frente a las amenazas digitales.

4.2.1. Realismo: el ciberpoder como equilibrio estratégico

El enfoque realista sostiene que el sistema internacional en el que interactúan los Estados se caracteriza por su estructura anárquica; sin embargo, lejos de ser un sinónimo de caos o ausencia de orden, se refiere a la inexistencia de una autoridad superior que regule sus relaciones (Jaquenod, 2013, p. 2). En este escenario, los Estados operan de manera autónoma y deben asumir la responsabilidad de garantizar su propia seguridad (Jaquenod, 2013, p. 2).

No obstante, respecto a esta teoría resulta esencial tener en cuenta que, para autores como Morgenthau, el realismo es una teoría que si bien reconoce que el poder ocupa un lugar central en la política internacional, esto no implica equipararla a la violencia ni limitarla a dimensiones meramente materiales (como se citó en Williams, 2004, p. 643). Es decir, su propósito es salvaguardar la autonomía de lo político y conservarlo como un ámbito donde sea posible la deliberación y la transformación, evitando que derive en una competencia desbordada por la supremacía (como se citó en Williams, 2004, p. 643).

Ahora bien, si se extrapola este concepto al escenario del ciberespacio, se puede afirmar que este constituye un nuevo terreno de competición por el poder, donde los Estados buscan asegurar ventajas estratégicas frente a sus adversarios. Es un panorama que, al dejar que el ámbito de actuación de los Estados se base en su autonomía, hace que el ciberpoder sea el instrumento perfecto con la capacidad de alterar las dinámicas internacionales. Al final, se trata de que cada Estado se encuentra en una constante pugna para obtener el máximo beneficio del sistema internacional (Jaquenod, 2013, p. 3).

En este contexto, el ius ad bellum, al desarrollarse en una "zona gris", permite a los Estados obtener ventajas estratégicas al ser una herramienta útil para incrementar el poder estatal y asegurar su supervivencia en un entorno internacional competitivo.

Siguiendo esta lógica, resulta imprescindible citar a Morgenthau en la medida en que advierte que para evitar que la política se convierta en una fuerza ilimitada y destructiva, es necesario mantener su autonomía frente a la lógica expansiva del poder (como se citó en Williams, 2004, p. 650). En este sentido, señala que las distintas esferas sociales (especialmente la económica y la moral), al operar bajo sus propias lógicas y formas de poder, pueden actuar como límites (como se citó en Williams, 2004, p. 650).

Y es que el pensamiento realista de Morgenthau ofrece una advertencia que resulta especialmente pertinente en el ciberespacio: la ausencia de límites claros en este ámbito puede convertirlo en un escenario donde la lógica del poder se expanda sin control, reproduciendo dinámicas de dominación y exclusión. Con lo cual, así como Morgenthau propone equilibrar las esferas sociales para preservar la apertura democrática, en el entorno digital se requiere un marco ético que impida que el ciberpoder se convierta en un instrumento de supremacía absoluta, garantizando que la competencia tecnológica no perjudique las relaciones internacionales.

4.2.2. Liberalismo: insuficiencia de la cooperación internacional actual

Alternativamente al realismo, está el liberalismo, el cual se fundamenta en el principio evolutivo, en virtud del cual el futuro de las RRII es bastante esperanzador al estar caracterizado por la prosperidad, la libertad y la paz (Jaquenod, 2013, p. 5). Y es que esta corriente se nutre de la creencia de que al ser humano lo impulsa al desarrollo colectivo y es guiado por la constante preocupación en el bienestar general (Jaquenod, 2013, p. 5).

Por este motivo, para el pensamiento liberalista la existencia de una cooperación internacional efectiva es clave (Jaquenod, 2013, p. 5). Es más, "la cooperación se vuelve entonces necesaria para maximizar los posibles beneficios y minimizar los posibles daños de las interacciones internacionales y de la interdependencia" (Jaquenod, 2013, p. 7).

Bajo esta visión, la interdependencia digital debería incentivar no tanto la competencia por el poder, sino la creación de marcos normativos compartidos que reduzcan la inseguridad y los incentivos "pro conflicto". Sin embargo, la realidad ha mostrado que los esfuerzos de gobernanza global carecen de mecanismos vinculantes efectivos.

Ahora bien, desde el punto de vista del ius ad bellum, existen una serie de factores tales como la fragmentación política, los intereses divergentes de las potencias y la falta de confianza recíproca, que dan como resultado una ausencia de criterios consensuados para calificar una ciberoperación como "uso de la fuerza" o "ataque armado". Por consiguiente, el liberalismo revela la paradoja del ciberespacio: pese a que la cooperación internacional es indispensable para garantizar su estabilidad, las dinámicas de poder actuales dificultan su consolidación, lo que refuerza el carácter anárquico del sistema internacional.

4.2.3. Constructivismo: la oportunidad de moldear nuevas normas

Finalmente, el enfoque constructivista parte de la premisa de que los seres humanos habitan un mundo construido por sí mismos, lo que los convierte, al mismo tiempo, en los actores centrales en la configuración del mismo (Enrique Sánchez, 2012, p. 118). Desde esta perspectiva, la realidad internacional es una construcción social: todo lo que forma parte del entorno social de los individuos es producto de sus propias acciones y decisiones (Enrique Sánchez, 2012, p. 118).

Así, en virtud de esta teoría, las prácticas internacionales no son estáticas, sino el resultado de interacciones, discursos y consensos entre participantes. Por ello, el ciberespacio se constituye como un escenario que ofrece una oportunidad para la "construcción" de nuevas normas y estándares que definan conductas aceptables o inaceptables en el ámbito digital.

Al respecto, un ejemplo que ilustra este proceso de construcción normativa es el denominado "Manual de Tallin", previamente comentado, sobre comportamiento responsable en el ciberespacio. Aunque carezca de carácter vinculante, es un instrumento que refleja el incipiente consenso internacional que podría, con el tiempo, consolidarse en normas consuetudinarias o incluso en tratados específicos.

Así pues, desde el punto de vista del ius ad bellum, el constructivismo permite imaginar un escenario en el que la propia comunidad internacional redefina conceptos tradicionales, especialmente "uso de la fuerza" o "ataque armado", a la luz de los impactos propios de las ciberoperaciones. Y es que el constructivismo abre una ventana de oportunidad: la posibilidad de moldear un marco que reduzca la incertidumbre que caracteriza al ciberespacio.

Ahora bien, también corresponde señalar que aunque tradicionalmente se han considerado enfoques opuestos, el realismo y el constructivismo comparten puntos de convergencia en el análisis de la formación de identidades colectivas (Williams, 2004, p. 650). Mientras el constructivismo identifica un rol activo en la construcción del orden internacional; el realismo concebido por Morgenthau también reconoce construcciones sociales determinantes en la dinámica del poder y de los conflictos, pues estos no solo surgen de intereses materiales, sino también de construcciones sociales que definen la identidad (Williams, 2004, p. 650).

En síntesis, el haber extrapolado el análisis jurídico a una disciplina como las RRII permite comprender que el ciberespacio no es únicamente un ámbito tecnológico, sino un terreno donde se reconfiguran las dinámicas clásicas de poder, cooperación y construcción normativa. El realismo evidencia la lógica de competencia y equilibrio estratégico; el liberalismo, las limitaciones de una gobernanza global aún insuficiente; y el constructivismo, la posibilidad de moldear nuevas reglas adaptadas a los desafíos digitales, pero sobre todo de adaptar las ya existentes.

Sea como fuere, estos enfoques arriban a una misma conclusión: el marco vigente del ius ad bellum resulta insuficiente para responder a las transformaciones del entorno cibernético. De allí viene no solo la importancia, sino la necesidad de abogar por una reinterpretación de sus categorías centrales, lo que abre paso al análisis del apartado siguiente.

5. Hacia una reinterpretación del *ius ad bellum*

La emergencia del ciberespacio como dominio estratégico ha puesto de manifiesto la brecha entre las normas y la realidad, lo que plantea la necesidad de una reinterpretación que, sin desnaturalizar los principios fundamentales del DI, permita dar respuestas eficaces a las amenazas, y los riesgos que surgen en el entorno digital.

En este marco, el presente artículo propone avanzar hacia una reconceptualización del ius ad bellum que integre el impacto del ciberespacio en tres direcciones principales: una redefinición del concepto de "ataque armado" que contemple el umbral de daños cibernéticos; el fortalecimiento de los mecanismos de atribución y responsabilidad internacional, indispensables en un ámbito donde la autoría suele permanecer en la sombra; y la incorporación de criterios de proporcionalidad y necesidad adaptados a la legítima defensa en el entorno digital. Luego, se concluirá con una propuesta de un marco híbrido, en el que DI y las RRII dialoguen, con el fin de garantizar la vigencia del principio cardinal en este contexto: que el uso de la fuerza permanezca limitado, incluso frente a las innovaciones tecnológicas.

5.1. Redefinir el concepto de “ataque armado” incorporando el umbral cibernético

Tradicionalmente, la noción de “ataque armado” en el ius ad bellum ha estado asociada tanto al empleo de la fuerza física como a los daños materiales provocados por medios bélicos convencionales. No obstante, la aparición del ciberespacio y todas las actuaciones que se vienen presentando en este escenario han demostrado que el impacto destructivo o paralizante de las herramientas digitales puede equipararse o superar al de la fuerza militar tradicional.

En el estudio normativo lo que buscan establecer los especialistas es, al menos, un conjunto mínimo de normas que regulen las relaciones sociales, con el objetivo de crear un marco que facilite la convivencia y garantice el respeto de los derechos (Reguera, 2015, p. 5). Sin embargo, pese a que, siguiendo a Llorens, los desafíos que surgen en el ámbito cibernético aún están lejos de ser completamente resueltos, también es cierto que actualmente no se identifica una situación de desprotección total (2017, p. 812).

Por poner un ejemplo, en lo que respecta al uso de la fuerza dentro del marco del ius ad bellum, es evidente que la regulación actual, integrada por normas como el artículo 2 de la Carta de las Naciones Unidas, ofrece una solución que, si bien es adecuada, termina siendo temporal frente a los desafíos emergentes del ciberespacio (Llorens, 2017, p. 812). Por eso conviene recurrir a una de las características más importantes del Derecho: su adaptabilidad.

Ahora bien, la propuesta de redefinir el concepto de “ataque armado” no es sencilla, puesto que primero se requiere de dilucidar una serie de aspectos preliminares como, siguiendo a Llorens, la soberanía y la jurisdicción, en tanto coadyuvan en la delimitación de las competencias estatales en el ciberespacio, así como las actividades que se desarrollan en él (2017, p. 812). Ello, a su vez, permite que la responsabilidad internacional de los Estados en torno a potenciales conductas delictivas en dicho escenario sea esclarecida, puesto que se precisan los actos que les pueden ser, efectivamente, atribuibles; y encontrar la razón de los mismos, vale decir, si no se ha tratado de un legítimo ejercicio de su legítima defensa (Llorens, 2017, p. 812).

De hecho, últimamente se ha empezado a hablar de “arma cibernética” calificándola como tal cuando cumple una función ofensiva o defensiva y susceptible de materializarse (Robles, 2016, p. 365). Sin embargo, surge nuevamente uno de los principales desafíos: la dificultad de encuadrar todas las acciones hostiles en el ciberespacio dentro de la categoría de “ataque armado” tal como lo contempla el DI tradicional: ¿hasta qué punto los ataques con armas cibernéticas pueden ser calificados como ataques armados o uso de la fuerza?, ¿cómo se debe responder frente a estas nuevas posibilidades de agresión?, etc.

Desde una perspectiva interdisciplinaria, la redefinición del concepto debe incorporar no solo criterios jurídicos, sino también técnicos, económicos y, sobre todo, sociales. Por ejemplo, un ciberataque cuyo objetivo son las redes de energía de los hospitales, puede no producir bajas inmediatas, pero sí generar consecuencias equivalentes a las de un bombardeo: pérdida de vidas. En este sentido, la valoración del impacto cibernético requiere integrar distintas variables para así abogar por una adecuada redefinición de “ataque armado”.

En esta línea se postula que una adecuada redefinición de “ataque armado” pasa por dejar de enfocarse en el daño o la intencionalidad del mismo y tomar como criterio lo que se denominará “umbral cibernético”: toda vez que, en el ciberespacio, muchas operaciones si bien no generan víctimas inmediatas, sí pueden afectar la estabilidad de un Estado. Con lo cual corresponde redirigir la pregunta y empezar a considerar si los ataques cibernéticos logran comprometer la seguridad nacional o la estabilidad sociopolítica de un Estado, y hasta qué punto lo hacen.

Sin embargo, se reconoce que ampliar excesivamente la noción de ataque armado podría generar ambigüedades en la interpretación del ius ad bellum, como el evidente riesgo que se corre al militarizar el ciberespacio al legitimar el uso de la fuerza en un espacio en el que las conductas son difusas. Lo cierto es que el debate no debería centrarse en si es que el concepto de ataque armado debe ampliarse o no, sino en cómo hacerlo de manera legítima, previsible y compatible con la estabilidad internacional.

Por ello, se postula que el introducir el concepto de “umbral cibernético” trae consigo dar un giro que no busca sustituir la regulación clásica, sino más bien complementarla, evitando la impunidad jurídica, al mismo tiempo que preserva la coherencia normativa de una disciplina (DI) que debe adaptarse a los desafíos de la era tecnológica.

5.2. Fortalecer mecanismos de atribución y responsabilidad internacional

Tal como se esbozó en las secciones anteriores, el carácter anónimo y transfronterizo de los ciberataques plantea desafíos importantes para el ius ad bellum. Sin una adecuada atribución, un Estado víctima no puede identificar con certeza al agresor, lo que dificulta invocar su derecho a la legítima defensa o exigir responsabilidad internacional. En efecto, atribuir técnicamente un ataque es complejo debido al anonimato, suplantación de identidad y la naturaleza multinodal de las redes. De esa forma, el problema principal reside en la dificultad probatoria para aplicar las normas existentes en estos casos concretos.

Es por eso que para que el ius ad bellum sea realmente eficaz frente a las agresiones en el ciberespacio, es imprescindible reforzar los mecanismos de atribución y responsabilidad internacional. Sin embargo, fortalecer estos mecanismos no solo implica desarrollar mejores capacidades técnicas de rastreo acorde a los estándares internacionales, sino también reconocer la influencia de la cooperación interestatal en la adaptabilidad del DI.

5.3. Considerar proporcionalidad y necesidad en la legítima defensa cibernética

En un tercer plano, la defensa propia frente a un ataque armado cibernético debe regirse por los mismos principios de necesidad y proporcionalidad que operan en los conflictos tradicionales. Cualquier respuesta en legítima defensa debe limitarse a lo estrictamente necesario y proporcional para repeler el ataque o prevenir uno inminente (O'Meara, 2025, pp. 3-4). En ese sentido, se pueden aterrizar dichos criterios de la siguiente manera:

5.3.1. Necesidad

Este principio exige que la fuerza (sea cinética o cibernética) sólo se emplee si es imprescindible para detener o repeler el ataque armado en curso o inminente. En primer lugar, debe existir un ataque armado real o inminente: el derecho internacional no ampara respuestas armadas contra meras amenazas potenciales o hipotéticas. Ello supone que la legítima defensa preventiva (actuar antes de tener evidencia de un ataque inminente) no es lícita, a diferencia de la defensa anticipada frente a un ataque claramente inminente y en vías de materializarse.
En la práctica, la naturaleza sorpresiva y sigilosa de muchos ciberataques dificulta cumplir con la exigencia de inmediatez pues, a menudo, el Estado afectado solo detecta el ataque cuando el daño ya está hecho, retrasando la respuesta (Pérez, 2021). Pese a ello, sigue siendo necesario que cualquier contraataque cibernético se justifique como último recurso, cuando no haya medios pacíficos o menos lesivos eficaces para frenar la agresión.

5.3.2. Proporcionalidad

El principio de proporcionalidad complementa al de necesidad, delimitando la intensidad y tipo de fuerza permisible en la respuesta. No se trata de simetría estricta (no obliga a responder con "un ataque cibernético por otro") sino de asegurar que la respuesta no exceda en magnitud, gravedad y objetivos al ataque sufrido. En el ámbito cibernético, ello implicaría calibrar cuidadosamente los efectos de la contraofensiva, pues la fuerza empleada debe ser proporcional al daño causado o el peligro que se busca prevenir

En ese sentido, la proporcionalidad exige que se limite la respuesta a los objetivos directamente implicados en el ataque, ya que atacar infraestructuras o sistemas ajenos al agresor original sería desproporcionado y violaría el derecho internacional. Asimismo, debe ponderarse el riesgo de daños colaterales en el entorno digital interconectado. Las armas cibernéticas, como virus o malware, pueden propagarse más allá de su blanco previsto o causar efectos imprevistos en terceros Estados o en la población civil.

5.4. Propuesta de un marco híbrido entre Derecho Internacional y seguridad digital

Por todo lo señalado en el presente artículo, se colige que la transformación digital ha generado un entorno de conflicto que desafía las categorías tradicionales del DI, especialmente aquellas vinculadas al ius ad bellum. La propia naturaleza intangible y compleja de las acciones, conductas, actividades en las ciberoperaciones, escapa de lo que tradicionalmente se concibe como "ataque armado", lo que genera un vacío que no solo debe ser regulado, sino que debe serlo eficazmente.

Es precisamente por ello que la propuesta aquí presentada busca ir más allá de una mera "actualización" conceptual del marco jurídico internacional. De hecho, la capacidad de adaptabilidad del derecho es tal que, a raíz de los propios problemas, surge como contrapartida una nueva regulación. Probablemente uno de los mayores ejemplos sea el Manual de Tallin, producto del conflicto en Estonia.
Sin embargo, dado que la tecnología presenta una naturaleza dual, en tanto que los sistemas tecnológicos pueden ser empleados tanto para propósitos legítimos como para acciones malintencionadas, se complica la identificación y gestión de las amenazas que enfrentan los Estados y otros actores (García, 2021, pp. 54-55).

Por tanto, esta propuesta no solo aboga por una redefinición de uno de los conceptos clave como lo es "ataque armado", puesto que, tarde o temprano, el DI se adaptará a esta realidad emergente, sino que su innovación radica en la articulación de un enfoque interdisciplinario que, además de revisar críticamente los conceptos del DI, incorpora a las RRII como disciplina complementaria para este análisis: concretamente los postulados del constructivismo.

Bajo esta lógica, se propone un marco híbrido que combine tanto las normas del DI como las RRII y reconozca la capacidad que tiene la humanidad de moldear reglas y crear nuevas, adaptadas al ciberespacio. Lo que se plantea es una suerte de "arquitectura" normativa que combine lo mejor de ambas disciplinas y pueda arribar a una o varias soluciones efectivas, que aseguren que, aún en la intangibilidad de lo digital, prevalecerán reglas que contengan la violencia. Después de todo, en un horizonte incierto como el ciberespacio, la intervención humana eficaz no radica en el poder, sino en las ideas que la construyen y orientan su ejercicio.

6. Conclusiones

El presente trabajo ha demostrado que el ciberespacio es un nuevo escenario operativo y transformador que tensiona las bases conceptuales y normativas del ius ad bellum. A través del análisis de la Carta de la ONU, algunos casos prácticos y doctrina especializada, se ha evidenciado que marcos jurídicos tradicionales o clásicos muchas veces resultan insuficientes para responder con claridad, eficacia y legitimidad a los desafíos que plantea la guerra cibernética. Al respecto, conviene sintetizar los principales puntos de este breve estudio:

En primer lugar, el ciberespacio exige repensar el ius ad bellum. El escenario del ciberespacio ha desbordado las categorías jurídicas tradicionales, obligando a revisar conceptos clave como el "uso de la fuerza", "ataque armado" y "legítima defensa" a la luz de las particularidades del entorno digital y los principales desafíos que esta presenta. El Derecho Internacional no puede seguir interpretando estas nociones únicamente desde una lógica territorial o clásica, en la medida en que los ataques cibernéticos son capaces de paralizar las infraestructuras críticas de los Estados y causar efectos comparables a los de un ataque armado tradicional.

En segundo lugar, casos como Estonia (2007), Stuxnet (2010) y los ataques a infraestructura crítica en la guerra de Ucrania muestran que los efectos reales de operaciones cibernéticas pueden ser significativos, aun cuando jurídicamente no siempre alcancen el umbral de "ataque armado". Se introduce lo que se denomina la "zona gris", es decir, operaciones hostiles que permanecen por debajo del umbral jurídico de fuerza, pero que buscan efectos coercitivos significativos. Es por eso que, sin una evolución normativa, los umbrales legales podrían hacerse obsoletos, pero también una interpretación demasiado amplia podría legitimar respuestas militares injustificadas.

En tercer lugar, la integración entre Derecho Internacional y Relaciones Internacionales es esencial para abordar los desafíos del ciberespacio porque cada disciplina complementa lo que la otra no puede abarcar por sí sola. Mientras que el DI aporta un marco normativo y jurídico que regula y analiza el uso de la fuerza; las RRII aportan herramientas analíticas para entender cómo los Estados y actores no estatales compiten, cooperan o construyen poder en este nuevo entorno. Esta colaboración permite anticipar cómo la interacción estatal potenciada por el ciberespacio impacta en las normas jurídicas existentes, y a la vez posibilita que esas normas se adapten o se reformulen a la luz de las emergentes dinámicas de poder, las tecnologías disruptivas y nuevas amenazas.

En tercer lugar, se evidencia la necesidad de normas más claras y adaptadas a la era digital. La falta de consenso sobre los umbrales de gravedad, estándares de atribución y condiciones de respuesta legítima frente a los ciberataques genera un espacio de ambigüedad jurídica que debilita la seguridad en las relaciones internacionales. La práctica estatal demuestra que, en ausencia de reglas claras, los Estados optan por respuestas informales o extralegales, lo que pone en riesgo la estabilidad del sistema y hace imperativo el avance hacia criterios jurídicos compartidos que, en el caso del ciberespacio, permitan arribar a la construcción de un marco híbrido jurídico-técnico que brinde una solución real frente a dicha modalidad de ataques.

7. Referencias

Aguirre, D. y Morandé, J. (2016). El ciberespacio y las relaciones internacionales en la era digital. En Cátedra Michel Foucault (Ed.), *Espacios del conocimiento: sujeto, verdad, heterotopías. A 30 años de la muerte de Michel Foucault* (pp. 139-152). CMF. https://www.researchgate.net/profile/Daniel-Aguirre-8/publication/327392167_El_ciberespacio_y_las_relaciones_internacionales_en_la_era_digital/links/5b8c96c0299bf1d5a73a05ec/El-ciberespacio-y-las-relaciones-internacionales-en-la-era-digital.pdf

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), 56-67. https://revistas.utm.edu.ec/index.php/revistanullius/article/view/7619/10040

Álvarez, I. (2020). El Derecho del ciberespacio. Una aproximación. *Revista de Internet, Derecho y Política*, (30), 1-13. https://doi.org/10.7238/10.7238/idp.v0i30.3201

Arré, G. (2025). Guerra híbrida y amenazas: hechos y tendencias. *Escenarios Actuales*, *30*(1), 35-52. https://www.ejercito.cl/descargas/desktop/NDYxOA==

Burkadze, K. (2022). International Legal Basis for the Right to Defense in the Cyber Era. *Law and World: International Journal of Law*, *8*(22), 17-23. https://doi.org/10.36475/8.2.2

Campos, B. (2022). *El uso de la fuerza en el ciberespacio* [Tesis de Máster, Universidad Da Coruña]. https://ruc.udc.es/rest/api/core/bitstreams/498c7f1a-7b66-4a62-9edb-7c5337c451de/content

Corn, G. y Jensen, E. (2018). The Use of Force and Cyber Countermeasures. *Temple International & Comparative Law Journal*, *32*(2), 127-133. https://sites.temple.edu/ticlj/files/2020/02/32.2_Corn_Article02-header-deleted.pdf

Enrique Sánchez, L. (2012). ¿De qué se habla cuando se habla de Constructivismo? *Revista de Relaciones Internacionales de la UNAM*, (114), 107-129. https://www.revistas.unam.mx/index.php/rri/article/view/48992

Franco, Á. (2024). *El ciberespacio, el poder del siglo XXI: análisis del impacto de la ciberseguridad en las dinámicas de poder del sistema internacional*. https://ddd.uab.cat/pub/tfg/2023/tfg_2497154/Trabajo_final_de_estudios_1604400.pdf

García, B. (2021). El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra. *Revista chilena de derecho y tecnología*, *10*(2), 43-68. https://doi.org/10.5354/0719-2584.2021.57077

Jaquenod, A. (2013). El realismo y el liberalismo internacionalista. Una introducción crítica a las teorías clásicas de las relaciones internacionales. En J. Kan y R. Pascua (Eds.), *Integrados (?) Debates sobre las relaciones internacionales y la integración regional latinoamericana y europea* (pp. 1-24). https://n9.cl/rrao3u

Llorens, M. (2017). Los desafíos del uso de la fuerza en el ciberespacio. *Anuario mexicano de derecho internacional*, (17), 785-816. https://doi.org/10.22201/iij.24487872e.2017.17.11052

Martabit, P. (2019). *Atribución en el ciberespacio: piedra tope en el Derecho Internacional* (Cuaderno de Trabajo No. 14-2019 del Centro de Investigaciones y Estudios Estratégicos, 14, 1-18). https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N14-2019.pdf

Mayer, L. y Vera, J. (2020). El delito de espionaje informático: Concepto y delimitación. *Revista chilena de derecho y tecnología*, *9*(2), 221-256. https://doi.org/10.5354/0719-2584.2020.59236

Muñoz, R. (2024). *Desafíos y soluciones en la defensa nacional: un marco integral para contrarrestar amenazas híbridas* [Tesis de Maestría, Escuela Superior de Guerra "General Rafael Reyes Prieto"]. Repositorio Institucional ESDG. https://www.esdegrepositorio.edu.co/bitstream/handle/20.500.14205/11266/TG-MY%20MU%C3%91OZ%20RONALD-MAESD%20AULA%20I.pdf?sequence=1&isAllowed=y

O'Meara, C. (2025). Exploring the Necessity and Proportionality of Self-Defense in the Cyber Context. *Working Paper Series del Exeter Centre for International Law*, (2), 1-14. https://www.exeter.ac.uk/v8media/facultysites/hass/law/OMeara_-Necessity_and_Proportionality_in_the_Cyber_Context-_ECIL_WP_2025-2.pdf

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

Quispe, F. (2024). Los problemas ciber vistos desde el Derecho Internacional. Un gran reto a enfrentar. *Eunomía. Revista en Cultura de la Legalidad*, (27), 155-182. https://doi.org/10.20318/eunomia.2024.9005

Reguera, J. (2015). *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario*. Análisis GESI. https://www.ugr.es/~gesi/analisis/7-2015.pdf

Regueiro, R. (2025). The use of armed drones against State actors: The killing of General Soleimani in Iraq. *Behavior & Law Journal*, *11*(1), 4-14. https://doi.org/10.47442/blj.2025.136

Repetto, F. (2021). *La aplicación del derecho internacional humanitario en el marco de los ataques informáticos: casos Stuxnet, Estonia, Georgia* [Tesis de Doctorado, Universidad de Belgrano-Facultad de Derecho y Ciencias Sociales-Licenciatura en Relaciones Internacionales]. http://190.221.29.250/bitstream/handle/123456789/9573/Repetto.pdf?sequence=1&isAllowed=y

Robles, M. (2016). Amenaza y uso de la fuerza a través del ciberespacio: un cambio de paradigma. *Revista Latinoamericana de Derecho Internacional*, (4), 110-188. https://www.revistaladi.com.ar/index.php/revista-ladi/article/view/124

Robles, M. (2016). El concepto de arma cibernética en el marco internacional: una aproximación funcional. *Boletín IEEE*, (4), 353-370. https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEE0101-2016_Arma_Cibernetica_MargaritaRobles.pdf

Rodríguez, A. (2025). Conflictos en la zona gris: la nueva amenaza universal. *European Public & Social Innovation Review*, (10), 1-15. https://doi.org/10.31637/epsir-2025-1603

Romeo, C. (1996). Delitos informáticos de carácter patrimonial. *Informática y derecho: revista iberoamericana de derecho informático*, (9), 413-442. https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&q=Delitos+Inform%C3%A1ticos+de+car%C3%A1cter+patrimonial&btnG=

Schmitt, M. (Ed.). (s.f.). *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Silva, F. (2018). StuxNet-El software como herramienta de control geopolítico. *Revista PUCE*, (106), 297-314. https://www.revistapuce.edu.ec/index.php/revpuce/article/view/141/243

Tsagourias, N. (2024). Cyber Attribution Agencies: A Sceptical View. *Questions of International Law*, (106), 23-38. https://doi.org/10.26807/revpuce.v0i106.141

Williams, M. (2004). Why Ideas Matter in International Relations: Hans Morgenthau, Classical Realism, and the Moral Construction of Power Politics. *International Organization*, *58*(4), 633-665. https://doi.org/10.1017/S0020818304040202