UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Jurisprudencia

La necesidad de una definición precisa del término ataque en el ciberespacio bajo el Derecho Internacional Humanitario

Emilio José Molina Narváez

Jurisprudencia

Trabajo de fin de carrera presentado como requisito para la obtención del título de Abogado

Quito, 28 de noviembre de 2024

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechosde propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación deeste trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica deEducación Superior del Ecuador.

Nombres y apellidos:	Emilio José Molina Narváez
Código:	00320768
Cédula de identidad:	1720851649
Lugar y Fecha:	Quito, 28 de noviembre de 2024

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The followuing capstone Project is available through Universidad San Francisco de Quito USFQ institutional repository. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

LA NECESIDAD DE UNA DEFINICIÓN PRECISA DEL TÉRMINO ATAQUE EN EL CIBERESPACIO BAJO EL DERECHO INTERNACIONAL HUMANITARIO[1]

THE NEED FOR A PRECISE DEFINITION OF THE TERM ATTACK IN CYBERSPACE UNDER INTERNATIONAL HUMANITARIAN LAW

Emilio José Molina Narváez[2]
emiliomolina2002@gmail.com

RESUMEN

El ciberespacio bajo el derecho internacional humanitario plantea desafíos sustanciales para la protección de la población civil y la regulación de las ciberoperaciones. Este estudio examinó las lagunas normativas del marco jurídico vigente, analizando las posiciones de Estados como Francia, Alemania y Estados Unidos, así como del Comité Internacional de la Cruz Roja. Los resultados subrayan la necesidad de redefinir el concepto de ataque para abarcar ciberoperaciones. Las interpretaciones divergentes entre Estados generan inconsistencias normativas, dificultando la aplicación de principios del derecho internacional humanitario, como distinción, proporcionalidad y precaución, en el ámbito digital. El estudio recomienda la ampliación del concepto de ataque y la creación de un tratado internacional específico para regular las ciberoperaciones, con el fin de garantizar una protección más adecuada, superar la fragmentación normativa y asegurar la vigencia del derecho ante las dinámicas del entorno cibernético.

PALABRAS CLAVE

Derecho Internacional Humanitario, ciberoperaciones, ataque, principios fundamentales

ABSTRACT

Cyberspace under International Humanitarian Law presents substantial challenges for the protection of civilians and the regulation of cyberoperations. This study examined the normative gaps in the current legal framework, analyzing the positions of states such as France, Germany, and the United States, as well as the International Committee of the Red Cross. The findings underscore the need to redefine the concept of attack to encompass cyber operations. Divergent interpretations among states create normative inconsistencies, hindering the application of International Humanitarian Law principles such as distinction, proportionality, and precaution in the digital realm. The study recommends expanding the concept of attack and creating a specific international treaty to regulate cyber operations, aiming to ensure better protection, overcome normative fragmentation, and maintain the relevance of the law amidst the dynamics of the cyber environment.

KEY WORDS

International Humanitarian Law, cyberoperations, attack, fundamental principles

[1] Trabajo de titulación presentado como requisito para la obtención del título de Abogada. Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Dirigido por Hugo Washington Cahueñas Muñoz.

[2] © DERECHOS DE AUTOR: Por medio del presente documento certifico que he leído la Política de Propiedad Intelectual de la Universidad San Francisco de Quito y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo de investigación quedan sujetos a lo dispuesto en la Política. Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad con lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Fecha de lectura: 28 de noviembre de 20224

Fecha de publicidad: 28 de noviembre de 202

SUMARIO

1. Introducción

El Derecho Internacional Humanitario, DIH, se ha consolidado como un conjunto de normas fundamentales para regular los conflictos armados, con el objetivo primordial de proteger a las personas que no participan activamente en las hostilidades, así como restringir los métodos y medios de combate[3]. Tradicionalmente, el DIH ha regulado los conflictos armados convencionales, en los que los ataques implican violencia física directa, destrucción de infraestructura y pérdida de vidas humanas. No obstante, con el auge de las ciberoperaciones como medio de confrontación, el DIH enfrenta nuevos retos, particularmente en lo que respecta a la definición del término ataque[4]. El ciberespacio nos da una plataforma conflictiva que no se adapta a las formas tradicionales de los conflictos, esto genera ambigüedades en la aplicación del DIH y deja varios vacíos normativos[5].

La presente discusión analiza cómo la falta de una definición precisa de ataque en el contexto del ciberespacio ha sido identificada como uno de los mayores desafíos para la correcta aplicación del DIH en las ciberoperaciones. En este entorno, las acciones que

[3] Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Cheltenham: Edward Elgar Publishing, 2019),100-110.
[4] Terry Gill, *Conflictos cibernéticos y derecho internacional: análisis de los límites* (Leiden: Brill Nijhoff, 2019), 100-120.
[5] *Ibidem.*

afectan significativamente la seguridad y estabilidad de los Estados pueden no manifestarse a través de la destrucción física inmediata, lo que dificulta su clasificación bajo las normas del DIH.

Para ello, la metodología propuesta será la siguiente: deductiva, por lo cual se hará un análisis normativo centrado dentro del ámbito del DIH, partiendo de los principios generales de la materia hasta llegar a su aplicación dentro del contexto concreto de las ciberoperaciones; mixta, ya que se emplearán técnicas cualitativas para analizar interpretaciones doctrinales y normativas y objetivos cuantitativos para evaluar tendencias con respecto a ciberataques; comparativa, al obtener información en cuanto a las discrepancias de criterio de los Estados, así como también del Comité Internacional de las Cruz Roja, CICR.

2. Estado del Arte

El DIH ha generado debates sobre la manera en que se deben aplicar las normas de los conflictos armados en este ámbito. El Manual de Tallinn, ha sido un intento de sistematizar las normas internacionales aplicables a las ciberoperaciones, define un ataque como cualquier operación que cause muerte, lesiones o destrucción física. [6] Este enfoque ha presentado varias criticado porque, aunque admite que las ciberoperaciones pueden tener alertas, existen varios campos en los que las operaciones cibernéticas no causan un daño físico directo, sino que tienen efectos indirectos horrendos para la población civil y las infraestructuras críticas no están completamente contemplados de la forma en la que deberían [7].

Existen diversos enfoques respecto a la definición de "ataque" en el ciberespacio bajo el DIH, se analizará cuatro enfoques. Un enfoque **pragmatista** propone ampliar la definición de ataque para incluir cualquier operación que afecte la funcionalidad de infraestructuras críticas, independientemente de si causan daños físicos inmediatos[8]. Este enfoque parte de la creciente dependencia tecnológica de la sociedad moderna y la necesidad de proteger los servicios civiles vulnerables a ciberataques[9].

[6]Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017),105-111.
[7] Jonathan Horowitz, *"Operaciones cibernéticas bajo el derecho internacional humanitario: perspectivas desde el CICR"* (Washington, DC: Sociedad Americana de Derecho Internacional, 2020).
[8] François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020).
[9] Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace*, (2019),11-15.

El enfoque expansivo propone una interpretación del término ataque bajo el DIH que traspasa las limitaciones de los conflictos armados convencionales para incluir las ciberoperaciones que interfieran con sistemas esenciales o infraestructuras críticas[10]. Este marco conceptual también aboga por considerar las consecuencias indirectas de las ciberoperaciones, subrayando que los efectos no visibles o inmediatos no deben quedar fuera del ámbito normativo del DIH, en aras de garantizar una protección adecuada frente a las dinámicas del ciberespacio[11]. Este enfoque argumenta que la disrupción de estos servicios puede tener efectos perjudiciales equiparables o incluso superiores a los daños físicos directos, dado que pueden afectar gravemente la funcionalidad de los sistemas[12].

En contraste, el enfoque **tradicionalista** se centra en limitar el concepto de ataque a aquellas ciberoperaciones que causan daños físicos comparables a ataques convencionales[13]. No obstante, este enfoque contempla ciertos elementos de la realidad del ciberespacio, destacando la relevancia de la soberanía estatal y la prohibición de intervenir en asuntos internos, lo que sugiere que las ciberoperaciones que afectan sistemas críticos podrían constituir violaciones del derecho internacional[14]. Aun así, sigue existiendo un debate sobre si dichas interferencias debieran clasificarse formalmente como ataques bajo el DIH[15].

El enfoque humanitario evolutivo del CICR destaca las dificultades inherentes a la aplicación de las normas tradicionales del DIH en el ciberespacio, especialmente en lo relativo a la definición de ataque[16]. Mientras que las ciberoperaciones que resultan en muerte, lesiones o daño físico son sin duda ataques en virtud del DIH, el CICR también reconoce la dificultad añadida de las ciberoperaciones, que no causan un daño físico directo, pero que causan disrupciones, como la interrupción de la electricidad o las telecomunicaciones, interrumpiendo masivamente la población civil[17].Tales disrupciones pueden ser tan perjudiciales como los ataques cinéticos tradicionales. En este sentido, el CICR resalta la necesidad de que los Estados revisen la interpretación del DIH en el contexto del ciberespacio, proponiendo que estos coincidan en la definición de ataque

[10] The Federal Government, "*Federal Foreign Office and Federal Ministry of Defence*", *On the Application of International Law in Cyberspace: Position Paper* (2021).
[11] Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace*,11-15.
[12] *Ibidem.*
[13]Office of General Counsel Department of Defense, "Cyber Operations", *Law of War Manual* (Washington, D.C: Department of Defense, 2023),1030-1040.
[14] *Ibidem.*
[15] *Ibidem.*
[16] Comité Internacional de la Cruz Roja. *Derecho Internacional Humanitario y Ciberoperaciones Durante Conflictos Armados*. (Ginebra: CICR, 2019), 9.
[17] *Ibidem.*

para incluir aquellas ciberoperaciones que, sin generar destrucción física, comprometen el acceso a servicios fundamentales para la sociedad civil[18].

3. Marco Normativo

El DIH, está basado principalmente en los Convenciones de Ginebra y sus Protocolos Adicionales. Estas normativas, originalmente, fueron diseñadas para conflictos convencionales. Un tema central del DIH para las ciberoperaciones es la definición de "ataque" o hostilidad en el ciberespacio[19]. Actualmente, existe una ambigüedad en torno a qué constituye un ataque bajo el DIH en el contexto cibernético. El artículo 49 del Protocolo Adicional I, que define los ataques como "actos de violencia contra el adversario"[20].

En segundo lugar, el Protocolo Adicional I a los Convenios de Ginebra en el artículo 36 establece que la obligación de los Estados a confirmar la legalidad de cualquier nuevo método y medio de guerra, que incluye en este ámbito incluiría el campo del ciberespacio, asegurándose de esta forma que se de en el cumplimiento del DIH[21]. El Protocolo Adicional I, en su Artículo 48, define que el principio de distinción, que obliga a las partes en conflicto armado internacional, CAI, o, conflicto armado no internacional, CANI, a diferenciar entre objetivos militares y bienes civiles[22]. Sin embargo, en las ciberoperaciones, esta distinción se complica debido a la interconexión entre sistemas civiles y militares. Por ejemplo, las redes de telecomunicación o las redes eléctricas, aunque de naturaleza civil, son utilizados con fines militares, lo que en algunos casos los convierte en objetivos militares legítimos[23]. Esta dualidad que pueden tener este tipo de lugares ha generado debates sobre si la interrupción de estas infraestructuras, que afecta a millones de civiles, puede considerarse un ataque bajo el DIH si los mismos fueron atacados por un ciberataque[24].

---

[18] Comité Internacional de la Cruz Roja. *Derecho Internacional Humanitario y Ciberoperaciones Durante Conflictos Armados*.
[19] Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales,*Ginebra,* 8 de junio de 1977.
[20] Artículo 49, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[21] Artículo 36, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[22] Artículo 48, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[23] Michael Schmitt, *Manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética*,115-123.
[24] François Delerue, *Cyber Operations and International Law,* 172-179.

Asimismo, el artículo 51 del Protocolo Adicional I prohíbe los ataques indiscriminados, entendidos como aquellos que no diferencian entre objetivos militares y civiles, o que causan daños colaterales excesivos en relación con la ventaja militar obtenida[25]. El artículo 52 del protocolo Adicional I a los Convenios de Ginebra menciona que los bienes civiles tienen una protección general y que se prohíbe los ataques a infraestructuras esenciales para la población civil[26]. El artículo 57 del Protocolo Adicional I a los Convenios de Ginebra obliga a las partes en conflicto a tomar todas las medidas posibles para evitar daños colaterales hacia las personas civiles, población civil y bienes de carácter, dando a entender que se debe respetar el principio de precaución del DIH[27].

Por otro lado, el artículo 54 del Protocolo Adicional I a los Convenios de Ginebra prohíbe los ataques contra bienes indispensables para la supervivencia de la población civil, como el suministro de agua y alimentos [28]. Las ciberoperaciones que interrumpen estos servicios, aunque no causen destrucción física inmediata, pueden tener consecuencias graves para la población civil, lo que las convierte en una violación directa del DIH. Las proyecciones futuras para la regulación de las ciberoperaciones bajo el DIH destacan la necesidad de actualizar y ampliar las normas vigentes. Como se mencionó, el Manual de Tallin 2.0 es un esfuerzo normativo desarrollado por expertos en derecho internacional, cuyo objetivo es interpretar y aplicar las normas del DIH al ciberespacio[29].

El DIH varía según el enfoque adoptado por cada país en su derecho interno. Como se señaló anteriormente, el gobierno francés ha sido uno de los principales defensores de la incorporación del ciberespacio en el DIH. El gobierno francés por su Ministerio de Armas en 2019 público el "*Droit International Appliqué aux Opérations dans le Cyberespace*" en el cual Francia amplía la definición de ataque para incluir cualquier operación que comprometa la funcionalidad de infraestructuras esenciales[30].

El gobierno alemán a través de su Ministerio de Relaciones Exteriores y Ministerio de Defensa adoptaron una posición país enfocada en los ciberataques y en la

[25] Artículo 51, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[26] Artículo 52, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[27] Artículo 57, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[28] Artículo 54, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[29] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
[30] Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace*.

definición del término ataque en un contexto en el cual el DIH sea aplicable[31]. El departamento de defensa del gobierno estadounidense mediante su "Law War Manual" de 2023 ha mantenido un enfoque más tradicional en la interpretación de "ataque" bajo el DIH en el contexto cibernético, limitándolo a aquellas operaciones que causen daños físicos[32]. El Comité Internacional de la Cruz Roja emite informes como lo son: *The Potential Human Cost of Cyber Operations, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Customary International Humanitarian Law Database*[33]. Dando así su punto de vista sobre las fuentes del DIH y cómo deben ser aplicadas.

4. Marco Teórico

El DIH, enfrenta la necesidad de adaptarse a nuevas formas de ejecutar las hostilidades, como las ciberoperaciones. Uno de los principales desafíos es la falta de una definición clara y unificada del término "ataque" en el contexto del ciberespacio. Los conceptos de los principios del DIH se vuelven ambiguos cuando se trata de ciberoperaciones, donde a entender que los daños físicos inmediatos pueden no ser evidentes, pero las consecuencias sobre infraestructuras críticas y la población civil pueden ser igualmente devastadoras.

Los primeros intentos de abordar el impacto del ciberespacio en el DIH, define los ataques cibernéticos de manera similar a los ataques convencionales, es decir, como acciones que provocan daños físicos directos[34]. No obstante, este enfoque ha sido cuestionado por académicos como Michael Schmitt, quienes argumenta que el concepto de ataque debe ampliarse para incluir operaciones que, aunque no destruyan físicamente bienes civiles o militares, interrumpen infraestructuras esenciales[35]. Schmitt resalta que las consecuencias indirectas de los ciberataques pueden ser tan graves como los daños físicos directos, por lo que deberían ser consideradas dentro del mismo marco del DIH[36].

Según François Delerue, esta interconexión entre bienes civiles y militares en el

[31] The Federal Government, "*Federal Foreign Office and Federal Ministry of Defence*", *On the Application of International Law in Cyberspace: Position Paper*.
[32] Office of General Counsel Department of Defense, "Cyber Operations", *Law of War Manual*.

[33] Comité Internacional de la Cruz Roja, *The Potential Human Cost of Cyber Operations, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Customary International Humanitarian Law Database* (Ginebra: Comité Internacional de la Cruz Roja, 2019).
[34] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,70-75.
[35] *Ibidme*,93-94.
[36] *Ibidem*,94-98.

ciberespacio obliga a reconsiderar la definición de ataque, sugiriendo que cualquier operación que comprometa la funcionalidad de infraestructuras críticas debe incluirse dentro de la definición de ataque[37]. Nils Melzer y Michael Schmitt han argumentado que los ciberataques pueden causar daños humanitarios significativos si afectan infraestructuras críticas como hospitales o sistemas de agua, y que estos efectos deben ser considerados dentro del marco del DIH, incluso si no se produce un daño físico directo[38].

La interconexión de los sistemas en el ciberespacio hace que los ataques dirigidos contra objetivos militares puedan tener efectos imprevistos en infraestructuras civiles, lo que representa un desafío en la interpretación del término ataque[39]. Delerue y otros expertos coinciden en que las operaciones en el ciberespacio deben ser cuidadosamente evaluadas para evitar efectos colaterales no deseados, reforzando así el principio de precaución en este nuevo entorno[40].

5. Definición Tradicional de Ataque en el DIH

En el contexto de los CAI tradicionales, el Protocolo Adicional I de las Convenciones de Ginebra ofrece una definición del concepto ataque. El Artículo 49 del Protocolo Adicional I define los ataques como " los actos de violencia contra el adversario sean ofensivos o defensivos"[41]. Esta definición se enfoca en los daños físicos directos en donde las hostilidades sin el medio para causar daño o destruir objetivos militares[42]. El DIH regula la conducta de las partes en conflicto y establece limitaciones estrictas sobre los métodos y medios de guerra para minimizar los daños a los civiles y proteger las infraestructuras esenciales para la vida diaria[43].Esta definición, fue creada para los conflictos armados convencionales, de esta forma se vuelve incongruente cuando pasa al ámbito del ciberespacio[44]. En las ciberoperaciones, puede como no tener violencia física directa, pero igualmente catastróficos[45].

---

[37] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,180.
[38] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities* (Geneva: ICRC, 2009), 103-106.
[39] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 209-210.
[40] François Delerue, *Cyber Operations and International Law*,208-213.
[41] Artículo 49, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[42] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 19-24.
[43] Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[44] François Delerue, *Operaciones cibernéticas y derecho internacional*,110-120.
[45] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,.

Clasificar adecuadamente los objetivos militares de las ciberoperaciones resulta esencial para proteger a la población civil y limitar el impacto en los conflictos[46]. El DIH distingue entre objetivos militares y civiles, con una tercera categoría para bienes de doble uso, que cumplen funciones tanto civiles como militares[47]. Los objetivos militares incluyen infraestructuras que contribuyen directamente a la acción bélica, como redes de defensa y sistemas de comunicaciones militares, y su ataque es legítimo bajo el DIH si se respeta la proporcionalidad y la necesidad militar[48]. esencial para proteger a la población civil y limitar el impacto en los conflictos[49]. El DIH distingue entre objetivos militares y civiles, con una tercera categoría para bienes de doble uso, que cumplen funciones tanto civiles como militares[50].Los objetivos militares incluyen infraestructuras que contribuyen directamente a la acción bélica, como redes de defensa y sistemas de comunicaciones militares, y su ataque es legítimo bajo el DIH si se respeta la proporcionalidad y la necesidad militar[51].Los bienes de doble uso, como las redes de telecomunicaciones que pueden tener aplicaciones tanto militares como civiles, plantean un desafío al principio de distinción, ya que su ataque podría generar graves consecuencias para la población civil[52].

5.1. Desafíos de la falta de definición precisa de ataque en el ciberespacio

En ausencia de una definición clara, resulta complicado determinar qué ciberataques deben considerarse equivalentes a ataques tradicionales bajo el marco del DIH, lo que provoca inconsistencias en la interpretación y aplicación de las normas por parte de los Estados[53]. Esta falta de claridad genera problemas que comprometen la protección de los civiles y dificultan la atribución de responsabilidades en el marco de las

[46] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge: Cambridge University Press, 2016)
[47] Emily Crawford y Alison Pert, *International Humanitarian Law* (Cambridge: Cambridge University Press, 2020),130-135.
[48] Noam Lubell, *El derecho de los conflictos armados y el uso de la fuerza: La enciclopedia Max Planck de derecho internacional público* (Oxford: Oxford University Press, 2020), 90-94.
[49] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge: Cambridge University Press, 2016)
[50] Emily Crawford y Alison Pert, *International Humanitarian Law* (Cambridge: Cambridge University Press, 2020),130-135.
[51] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2021), 46-48.
[52] Robert McLaughlin, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2022), 127-130.
[53] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,42-48.

ciberoperaciones [54].El DIH se basa en principios fundamentales como la distinción, la proporcionalidad y la precaución, cuyo propósito es reducir al mínimo los daños a los civiles y asegurar que las partes en conflicto respeten las normas del DIH durante las hostilidades[55]. No obstante, la falta de una definición clara de ataque en el ciberespacio dificulta la aplicación de estos principios[56].

El principio de distinción obliga a las partes del conflicto a distinguir en todo momento entre los objetivos militares y los bienes civiles, así como dirigir las operaciones solo contra aquellos objetivos que ofrezcan una ventaja militar[57]. En las ciberoperaciones, esta distinción se vuelve difusa debido a la interconexión entre los bienes civiles y militares pudiendo así aplicarse el doble uso[58]. Las redes de telecomunicaciones, los sistemas financieros y los sistemas eléctricos, que también pueden ser utilizados para fines militares son un ejemplo de aquello[59]. La interrupción de estos sistemas, aunque no implique destrucción física, puede tener consecuencias graves para la población civil, lo que plantea la pregunta de si estas acciones deben considerarse ataques bajo el DIH[60]. Desde una postura más tradicional Elizabeth Salmón mencionaria que se podría entenderse como un bien con objetivo dual [61].

El principio de proporcionalidad menciona que los ataques no deben ser excesivos en relación con la ventaja militar concreta y directamente obtenida[62].En el ciberespacio cuando una ciberoperación hace un daño indirecto hacia la población civil la evaluación de este es especialmente compleja, ya que los efectos de los ataques cibernéticos pueden no ser visibles de inmediato y sus consecuencias a largo plazo pueden ser graves y difíciles de predecir[63]. Por ejemplo, un ataque que inhabilite un sistema de control de tráfico aéreo o el sistema hidroeléctrico de un país puede no causar daños físicos inmediatos, pero sus consecuencias para la población civil y la economía de un país

[54] Nils Melzer, *Orientación interpretativa sobre la noción de participación directa en las hostilidades según el derecho internacional humanitario* (Ginebra: Comité Internacional de la Cruz Roja, 2009), 60-70.
[55] Artículo 51, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[56] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*,184-190.
[57]Elizabeth Salmón, *Introducción al Derecho Internacional Humanitario* (Lima: Pontificia Universidad Católica del Perú, 2016), 58.
[58] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*,192-198.
[59] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 54-57.
[60] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 198-203.
[61] Elizabeth Salmón, *Introducción al Derecho Internacional Humanitario*, 58-60.
[62] Artículo 51, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[63] Eric Talbot, *" Cyber Attacks: Proportionality and Precautions in Attack"*(Newport: *International Law Studies* 89,2013), 198-215.

podrían ser desproporcionadas respecto al objetivo militar alcanzado. Si el daño colateral supera la ventaja militar directa, el ataque constituiría una violación del DIH[64].

Asimismo, el principio de precaución requiere que las partes en conflicto tomen todas las medidas posibles para evitar o minimizar los daños a los civiles y a sus bienes con las debidas excepciones[65]. Sin una definición clara de "ataque" en el ciberespacio, resulta difícil aplicar este principio de manera efectiva, ya que los efectos de las ciberoperaciones pueden extenderse más allá de los objetivos previstos debido a la interconexión tecnológica[66]. En este contexto, se debe realizar análisis previos exhaustivos de los posibles efectos no intencionados, emplear tecnologías de precisión que minimicen el daño colateral, y evaluar el daño potencial sobre infraestructuras civiles críticas, como sistemas de energía o telecomunicaciones[67]. En caso donde las consecuencias no pueden ser anticipadas, el Protocolo Adicional I a los Convenios de Ginebra en su artículo 57 establece que el ataque deberá ser suspendido o anulado ya que, el accionar de ataque se volverían excesivo comparándolo con la ventaja militar que se pudiere obtener, volviéndolo así una violación del DIH [68].

5.2. Interpretaciones del DIH en Ciberoperaciones

La falta de una definición clara de ataque también ha llevado a interpretaciones divergentes entre los Estados y los actores internacionales[69]. Mientras que algunos países han adoptado una interpretación más amplia, considerando cualquier acción que comprometa la funcionalidad de infraestructuras críticas como un ataque, otros han mantenido una postura más restrictiva, limitando el concepto de ataque a aquellos actos que causan destrucción física inmediata[70]. Esta falta de consenso entre los Estados ha generado una falta de coherencia en la aplicación del DIH en ciberoperaciones, lo que crea un vacío normativo que deja a los civiles y a sus bienes vulnerables[71].

Francia ha adoptado un enfoque pragmatista, ya que, en su documento *"Droit*

---

[64] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 208-220.
[65] Elizabeth Salmón, *Introducción al Derecho Internacional Humanitario*.
[66] Ashley Deeks y Noam Lubell, "*The Due Diligence Principle and Cyber Operations*"(*American Journal of International Law,*2022), 556-584.
[67] *Ibidem.*
[68] Ashley Deeks y Noam Lubell, "*The Due Diligence Principle and Cyber Operations*",556-584.
[69] Dapo Akande y Antonios Tzanakopoulos, *The Application of International Law to Cyber Operations* (Oxford: Oxford University Press, 2020), 45.
[70] Amos Guiora y Peter Schwab, *Cyber Warfare: Law and Policy in the 21st Century* (London: Routledge, 2022), 52-55.
[71]Jason Barkham, *International Law and Cyber Operations: Bridging the Gap in Humanitarian Protection*. (Cambridge: Cambridge University Press, 2021),135.

International Appliqué aux Opérations dans le Cyberespace" de 2019, ha defendido que cualquier operación cibernética en un contexto de CAI que afecte la funcionalidad de infraestructuras críticas debe considerarse un ataque, independientemente de si causa daños físicos directos[72].

> Francia considera que un ataque en el sentido del artículo 49 del Protocolo Adicional I puede caracterizarse incluso en ausencia de lesiones o pérdidas humanas, o de daños físicos a bienes. Así, una ciberoperación constituye un ataque si los equipos o sistemas afectados dejan de prestar el servicio para el que fueron diseñados, incluso de manera temporal y reversible, siempre que se requiera una intervención del adversario para restaurar la infraestructura o el sistema a su funcionamiento operativo[73].

Este enfoque refleja el reconocimiento de que la sociedad moderna depende en gran medida de las tecnologías digitales y que las interrupciones en estas infraestructuras pueden tener consecuencias catastróficas para la población.

Alemania ha seguido el enfoque expansivo, argumentando que cualquier ciberoperación en el marco de un CAI que interfiera con sistemas de información, comunicación o infraestructura esencial debe considerarse un ataque bajo el DIH, incluso si no hay destrucción física inmediata. Para Alemania, el impacto en la seguridad y el bienestar de la población civil es suficiente para justificar la aplicación del DIH en estas operaciones[74].

> Los principios básicos que rigen la conducción de las hostilidades, incluso mediante medios cibernéticos, como los principios de distinción, proporcionalidad, precauciones en el ataque y la prohibición del sufrimiento innecesario y los daños superfluos, se aplican a los ciberataques[75].

Estados Unidos, por otro lado, ha adoptado un enfoque tradicionalista. En su "*Law of War Manual of 2023"*, Estados Unidos ha definido el término "ataque" de manera más restrictiva, limitándolo a las ciberoperaciones que causan daños físicos directos comparables a los ataques convencionales[76]. Aunque reconoce que las ciberoperaciones pueden tener un impacto significativo en la seguridad nacional, Estados Unidos prefiere mantener una definición más tradicional del concepto[77].

---

[72] Ministerio de Armas. *Droit International Appliqué aux Opérations dans le Cyberspace*.
[73] *Ministère des Armées." Droit International Appliqué aux Opérations dans le Cyberespace."* Francia,2019, (*traducción no oficial).*
[74] The Federal Government, "*Federal Foreign Office and Federal Ministry of Defence*", *On the Application of International Law in Cyberspace: Position Paper*.
[75] The Federal Government, "*Federal Foreign Office and Federal Ministry of Defence*", *On the Application of International Law in Cyberspace: Position Paper*, 2021, 8, (traducción no oficial).
[76] Office of General Counsel Department of Defense, "Cyber Operations", *Law of War Manual*, 350.
[77] *Ibidem.*

Estas diferencias en la interpretación del término "ataque" han creado una zona gris normativa en el ciberespacio, donde algunas ciberoperaciones quedan fuera del alcance del DIH, lo que resulta en una protección insuficiente para los civiles[78].

5.3. Criticas para Ampliar la Definición de "Ataque" en el Ciberespacio

CICR también ha expresado su enfoque más evolutivo, ya que a expresado su preocupación por la falta de una definición clara de ataque en el ciberespacio[79]. En varios informes, el CICR ha señalado que los ataques en el ciberespacio que interrumpen servicios esenciales deberían ser tratadas como ataques bajo el DIH, ya que los efectos sobre la población civil y sus bienes pueden ser arrasadores[80]. El CICR ha instado a la comunidad internacional a revisar la interpretación del DIH y a desarrollar nuevas normas que reflejen mejor los desafíos de los conflictos cibernéticos[81].

Dada la ambigüedad actual, varios expertos en derecho internacional y seguridad han propuesto una ampliación del término "ataque" en el DIH para abarcar las ciberoperaciones que, aunque no resulten en destrucción física directa, comprometan la funcionalidad de infraestructuras esenciales y afecten significativamente a la población civil[82]. Estas propuestas sugieren que el DIH debe adaptarse a las realidades del siglo XXI, donde los conflictos no solo se libran en los campos de batalla, sino también en el ciberespacio, con consecuencias invisibles, pero igualmente devastadoras.

6. Sobre el término “Ataque" en el Ciberespacio

Uno de los desafíos normativos más importantes que surge de estos debates doctrinales es la falta de consenso internacional sobre cómo definir y regular los ataques en el ciberespacio[83]. Mientras que algunos Estados y organizaciones internacionales han adoptado enfoques más actuales, otros se muestran reticentes a aceptar una definición más inclusiva de "ataque"[84]. Esta incompatibilidad normativa ha generado una falta de coherencia en la aplicación del DIH en la comunidad internación en el ámbito del ciberespacio, lo que deja a los civiles y sus bienes vulnerables ante los daños indirectos

[78] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2021).
[79] Comité Internacional de la Cruz Roja, *The Potential Human Cost of Cyber Operations.*
[80] *Ibidem.*.
[81] Comité Internacional de la Cruz Roja, *The Potential Human Cost of Cyber Operations.*
[82] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 305.
[83] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*,55.
[84] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 360.

que puedan generar las ciberoperaciones[85].

El CICR ha siempre desempeñado un papel importante en el desarrollo de propuestas para la regulación de nuevas normativas en el DIH y con esta costumbre lo hace en el ámbito de la normativa de las ciberoperaciones bajo el DIH[86]. En varios informes recientes, el CICR ha subrayado la importancia de proteger a la población civil de las consecuencias indirectas de las ciberoperaciones, y ha instado a los Estados a trabajar conjuntamente para desarrollar un marco normativo claro y coherente[87].

El CICR en sus informes y artículos a expuesto que las infraestructuras críticas, como los sistemas de agua, electricidad y salud, deben recibir una protección especial bajo el DIH, incluso cuando los ataques no resulten en destrucción física inmediata[88]. En su informe "The Potential Human Cost of Cyber Operations", el CICR señaló que las ciberoperaciones que interrumpen estos servicios esenciales pueden tener consecuencias humanitarias devastadoras, lo que justifica su tratamiento como ataques bajo el DIH[89].

Además, el CICR no se opone a que la comunidad internacional desarrolle un tratado vinculante o un protocolo adicional a las Convenciones de Ginebra que aborde específicamente las ciberoperaciones y establezca normas claras para regularlas:

> Los Estados también pueden decidir imponer límites adicionales a las ciberoperaciones que se sumen a los del derecho vigente, así como desarrollar normas complementarias, en particular, para reforzar la protección de las personas civiles y de la infraestructura civil contra los efectos de las ciberoperaciones[90].

Esta iniciativa permitiría dialogar los vacíos normativos actuales y garantizar que el DIH siga siendo relevante y efectivo en la protección de los civiles en el ciberespacio si estos llegaran a un consenso[91].

Para avanzar hacia un marco normativo coherente, será necesario que la comunidad internacional trabaje conjuntamente para desarrollar un consenso sobre la definición de ataque en el ciberespacio[92]. Esto podría lograrse a través de foros multilaterales, como las Naciones Unidas, donde los Estados puedan debatir y acordar

---

[85] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 40.
[86] Comité Internacional de la Cruz Roja, *The Potential Human Cost of Cyber Operations*
[87] *Ibidem.*
[88] *Ibidem.*
[89] *Ibidem.*
[90] Comité Internacional de la Cruz Roja, *Derecho internacional humanitario y operaciones cibernéticas durante los conflictos armados*, 6.
[91] Comité Internacional de la Cruz Roja, *Derecho internacional humanitario y operaciones cibernéticas durante los conflictos armados*, 6.
[92] *Ibidem*, 29-30.

una interpretación común del DIH en el ciberespacio[93]. Un consenso internacional permitiría una aplicación más uniforme del DIH y garantizaría una mayor protección para los civiles y sus bienes en los conflictos armados que usen el ciberespacio para causar daño[94].

7. Atribución de responsabilidades en el ciberespacio: La necesidad de una definición precisa de ataque en el DIH

El ciberespacio ofrece un entorno único y desafiante para la atribución de responsabilidades debido a su naturaleza descentralizada y anónima[95]. A diferencia de los ataques convencionales, que se pueden vincular fácilmente a un Estado, a través de la observación directa de fuerzas militares o mediante el uso de armamento trazable, las ciberoperaciones permiten a los actores operar desde cualquier parte del mundo, utilizando infraestructuras distribuidas y, en muchos casos, cubriendo sus huellas[96].

Los involucrados en los ciberataques pueden emplear una variedad de tácticas para ocultar su identidad y desviar la atribución, como utilizar servidores proxy, técnicas de encriptación, redes de dispositivos infectados y ataques de falsa bandera, donde un Estado o actor simula ser otro para evitar la responsabilidad[97]. Esto crea un ambiente en el cual los Estados encuentran dificultades en el proceso de rastrear el origen de los ataques y, por lo tanto, para atribución de responsabilidad clara[98].

Además, sin una definición precisa de lo que constituye un ataque bajo el DIH, es difícil identificar qué acciones cibernéticas pueden ser consideradas violaciones de las normas internacionales[99]. Esto también afecta la capacidad de determinar qué actores deben rendir cuentas y cómo deben ser sancionados[100]. En muchos casos, los Estados y actores no estatales pueden realizar ciberoperaciones sin causar daños físicos visibles o inmediatos y además ocultar el rastro de su identidad, lo que permite que sus acciones en términos legales no puedan ser determinadas la responsabilidad[101].

---

[93] Comité Internacional de la Cruz Roja, *The Potential Human Cost of Cyber Operations.*
[94] *Ibidem.*
[95] Dunn Cavelty, Myriam. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2020).
[96] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* 138-143.
[97] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 400-405.
[98] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 149-153.
[99] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law,* 65.
[100] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 418-426.
[101] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* 155.

7.1. Mejora en la identificación de los responsables

Con una definición más precisa los Estados tendrían una base legal más sólida para identificar qué acciones cibernéticas deben considerarse ataques bajo el DIH[102]. Esto permitiría a los Estados desarrollar capacidades más efectivas para rastrear el origen de los ciberataques y atribuir responsabilidades de manera más efectiva y exacta[103]. En muchos casos, la falta de claridad sobre lo que constituye un ataque ha impedido que los Estados actúen de manera decisiva, ya que temen acusar erróneamente a otros Estados o actores sin pruebas suficientes[104].

Un ejemplo claro de este desafío se observó en el caso de los ataques cibernéticos a infraestructuras eléctricas en Ucrania en 2015 y 2016.[105] Estos ataques, que interrumpieron el suministro eléctrico a cientos de miles de personas, fueron ampliamente atribuidos a actores respaldados por el Estado ruso, pero la atribución oficial fue extremadamente complicada debido a la falta de evidencia concluyente y la capacidad de los atacantes para ocultar sus rastros en el ciberespacio[106]. Una definición más clara de lo que constituye un ataque cibernético bajo el DIH podría haber facilitado una atribución más rápida y precisa de responsabilidades en este caso[107].

7.2. Creación de normas y sanciones internacionales

Una definición más precisa de "ataque" también permitiría la creación de normas internacionales claras y la imposición de sancione a quienes que violen el DIH en el ciberespacio.[108]

Este marco normativo permitiría imponer sanciones económicas y diplomáticas concretas como respuesta a las ciberoperaciones En el ámbito del derecho público internacional, las sanciones económicas se utilizan frecuentemente como un medio de disuasión y represalia frente a acciones que se consideran una amenaza para la paz y la seguridad internacionales[109]. En el marco del DIH, dichos mecanismos podrían aplicarse en ciberoperaciones si se demuestra que un Estado ha apoyado o permitido actividades

[102] *Ibidem,* 110.
[103] François Delerue, *Operaciones Cibernéticas y Derecho Internacional,* 390.
[104] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law,* 70.
[105] Andy Greenberg, *Sandworm: Una Nueva Era de Guerra Cibernética y la Caza de los Hackers más Peligrosos del Kremlin* (Nueva York: Doubleday, 2019), 85–87.
[106] *Ibidem.*
[107] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,115.
[108] François Delerue, *Operaciones Cibernéticas y Derecho Internacional,* 395.
[109] Claus Kreß, *International Cyber Law in Practice* (Oxford: Oxford University Press, 2021), 115.

que afectan la infraestructura de otro Estado. [110]. Además, estas medidas podrían incluir restricciones diplomáticas y comerciales, limitando la participación del Estado infractor en foros internacionales o excluyéndolo de ciertas alianzas estratégicas[111].

Para los casos donde los efectos de una ciberoperación sean comparables a los daños de un CAI, podría considerarse la intervención de la Corte Penal Internacional (CPI)[112]. Si un ciberataque se clasifica como un crimen de guerra bajo el DIH, sería posible enjuiciar a los responsables en la CPI, ampliando así el ámbito de la justicia penal internacional para abarcar estos nuevos desafíos en el ciberespacio[113]. La CPI ya contempla ciertos delitos de alta gravedad, y una extensión de su mandato permitiría abordar ciberoperaciones que constituyan violaciones significativas del DIH[114].

7.3. Fortalecimiento de la cooperación internacional

La naturaleza transnacional del ciberespacio significa que los ciberataques a menudo atraviesan múltiples jurisdicciones, lo que dificulta que un solo Estado pueda investigar y atribuir responsabilidades por sí solo[115]. Los actores responsables pueden utilizar servidores en varios países, distribuir el ataque a través de redes globales de bots o emplear infraestructuras digitales complejas para ocultar su origen[116].

Al tener una definición más clara de "ataque", los Estados y las organizaciones internacionales podrían coordinar mejor sus esfuerzos para rastrear los ataques cibernéticos y compartir información crítica[117]. Esta cooperación podría involucrar la creación de grupos internacionales de trabajo que investiguen ciberataques y desarrollen estrategias conjuntas para responsabilizar a los actores involucrados en las ciberoperaciones[118].Además, los mecanismos existentes, como los centros de intercambio de información sobre amenazas cibernéticas podrían expandirse para facilitar la colaboración entre los Estados en la atribución de responsabilidades, siendo estos las partes de los Estados que puedan conformar este grupo internacional de trabajo[119].

---

[110] Christian Tams, *Sanciones diplomáticas y derecho internacional* (Londres: Routledge, 2022), 78.
[111] Ian Henderson, *La guerra cibernética y el derecho de los conflictos armados.* (Leiden: Brill Nijhoff, 2020), 132.
[112] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* ,160.
[113] *Ibidem.*
[114] *Ibidem.*
[115] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 400-405.
[116] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,150.
[117] François Delerue, *Operaciones Cibernéticas y Derecho Internacional*, 410.
[118] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 150-155.
[119] Ian Henderson. *La guerra cibernética y el derecho de los conflictos armados.*

8. Perspectivas futuras

La creciente dependencia de las infraestructuras digitales y la interconexión global hacen que las ciberoperaciones sean una amenaza significativa para la seguridad de los Estados y la población civil[120]. En el ciberespacio, los ataques no siempre implican destrucción física inmediata, pero pueden tener consecuencias devastadoras, como la interrupción de servicios esenciales[121]. Esta capacidad no normada para afectar indirectamente a la población civil, sin recurrir a la violencia física, ha expuesto la urgente necesidad de adaptar las normativas existentes para garantizar una protección adecuada bajo el DIH[122].

La definición tradicional de "ataque", basada en el Artículo 49 del Protocolo Adicional I de las Convenciones de Ginebra, se centra en "actos de violencia contra el adversario"[123].Una de las propuestas más destacadas para la redefinición de "ataque" es la de ampliar el término para incluir cualquier acción cibernética que afecte significativamente la funcionalidad de infraestructuras críticas, incluso si no hay destrucción física directa[124]. Esto se debe a que la interrupción de estos sistemas puede tener efectos desastrosos para la población civil, ya que, en muchos países, los servicios básicos como el agua, la electricidad o el transporte dependen de infraestructuras digitales[125].

François Delerue, sostiene que cualquier ciberoperación que comprometa la seguridad o la funcionalidad de infraestructuras esenciales debe considerarse un ataque, independientemente de si causa destrucción física[126]. Delerue argumenta que la interconexión de los sistemas civiles y militares en el ciberespacio justifica la ampliación del concepto de ataque, dado que las operaciones dirigidas contra un objetivo militar pueden tener consecuencias indirectas devastadoras para la población civil[127].

8.1. Ampliar los principios del DIH

[120] *Ibidem,15.*
[121] Hitoshi Nasu, *Advanced Technology and the Law of Armed Conflict* (Cambridge: Cambridge University Press, 2021).
[122] *Ibidem.*
[123] Artículo 49, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[124] *Ibidem*, 90-92.
[125] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 43-45.
[126] François Delerue, *Operaciones cibernéticas y derecho internacional*, 101.
[127] *Ibidem.*

Otra propuesta importante es la revisión de los principios tradicionales del DIH, como la proporcionalidad y la precaución, para adaptarlos al contexto de las ciberoperaciones[128]. En los conflictos tradicionales, el principio de proporcionalidad exige que los daños colaterales causados por un ataque no sean excesivos en relación con la ventaja militar obtenida[129]. Sin embargo, en el ciberespacio, evaluar la proporcionalidad en los ciberataques es complejo, ya que los efectos indirectos de una ciberoperación no siempre son evidentes de manera inmediata.[130]

Se ha sugerido que el principio de proporcionalidad debe incluir una evaluación de los efectos a largo plazo de las ciberoperaciones, en lugar de limitarse a los daños físicos inmediatos: ¨El principio de proporcionalidad requiere una evaluación que considere no solo los daños inmediatos, sino también las consecuencias a largo plazo de las ciberoperaciones sobre la población civil y las infraestructuras críticas¨[131]. Esto incluiría considerar el impacto humanitario que pueden tener las interrupciones prolongadas de servicios esenciales, como el agua o la electricidad, incluso si no se produce destrucción física directa de estos bienes que pueden ser duales[132].

Además, el principio de precaución también debe ampliarse para incluir las ciberoperaciones[133].En el ciberespacio, los ataques pueden propagarse involuntariamente, afectando infraestructuras civiles no previstas como objetivos[134]. Esto plantea un desafío para la aplicación del principio de precaución, ya que los Estados deben tomar todas las medidas posibles para evitar daños a la población civil[135]. Por lo tanto, se propone que las medidas de precaución en el ciberespacio incluyan una evaluación amplia y taxativo de los posibles efectos colaterales, antes de llevar a cabo cualquier operación cibernética de carácter militar[136].

8.2. Mejorar la Atribución de Responsabilidades

[128] Nils Melzer, *Orientación interpretativa sobre la noción de participación directa en las hostilidades según el derecho internacional humanitario*, 55.
[129]Artículo 51, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[130] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 152-155.
[131]Paola Velásquez & CamiloPrieto, etivaProblemas abiertos en torno del principio de proporcionalidad: análisis desde el DIDH y el DIH (Bogatá: Sello Editorial Esmic, 2024), 141-160.
[132] Ian Henderson, *La guerra cibernética y el derecho de los conflictos armados*.
[133]Artículo 57, Protocolo adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales.
[134] *François* Delerue, *Operaciones cibernéticas y derecho internacional*, 145-147.
[135] *Ibidem.149-150.*
[136] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 158-160.

Una definición más clara de "ataque" en el ciberespacio también podría facilitar la atribución de responsabilidades, uno de los mayores desafíos que enfrenta el DIH en este ámbito[137]. Las ciberoperaciones son difíciles de rastrear debido a la naturaleza anónima y dispersa del ciberespacio, lo que permite a los actores esconderse detrás de redes o técnicas de encriptación[138]. Sin embargo, con una definición más precisa, sería más fácil para los Estados y los tribunales internacionales atribuir responsabilidades y sancionar a los actores involucrados en ciberoperaciones ilícitas[139].

9. Recomendaciones

Ante estas complejidades, es imperativo que los Estados adopten medidas para adaptar el DIH a las realidades que te puede dar el ciberespacio, A continuación, se dará algunas recomendaciones clave para mejorar la regulación de las ciberoperaciones bajo el DIH y garantizar una protección eficaz una protección para la población y bienes civiles. La redefinición del término ataque es un paso necesario para garantizar que el DIH pueda aplicarse de manera efectiva en el ciberespacio. Se recomienda que los Estados y las organizaciones internacionales trabajen conjuntamente para ampliar la definición de ataque, de manera que incluya no solo las ciberoperaciones que causan daños físicos directos, sino también aquellas que comprometan la funcionalidad de infraestructuras críticas o que tengan efectos indirectos sobre la población civil. Esto permitirá que el DIH se adapte mejor a las nuevas formas de conflicto y garantice una protección más adecuada.

Es indispensable la formación de normativa internacional específica como la adopción de un nuevo tratado internacional subsecuente a los Convenios de Ginebra o un protocolo adicional a los mismo, ya que, se debe abordar de manera concreta las operaciones cibernéticas y proteja tanto a la población como a los bienes civiles de los ataques digitales. Este marco normativo lograría implementar criterios certeros de los principios distinción y proporcionalidad aplicables en el espacio cibernético, además de definir responsabilidades claras de los Estados en cuanto a la, mitigación, prevención y atribución de ciberataques. De esta manera, se busca consolidar las posiciones

[137] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,175-178.
[138] François Delerue, *Operaciones cibernéticas y derecho internacional*, 161-163.
[139] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 179-181.

internacionales, creando un sistema de sanciones competente que permita una protección razonable, considerando las propiedades del ciberespacio, los riesgos asociados a la dependencia de infraestructura.

Con el fin de mejorar la atribución de responsabilidad en ciberespacio, es indispensable consolidar la cooperación internacional entre los Estados en la investigación y sanción de ciberoperaciones ilícitas. Esto podría incluir la creación de grupos de trabajo internacionales y la expansión de los centros de intercambio de inteligencia sobre amenazas cibernéticas, lo que permitiría una mejor coordinación en la identificación de los perpetradores de ciberataques.

Se recomienda una revisión de los principios de proporcionalidad, precaución y distinción para adaptarlos al contexto de las ciberoperaciones. Los efectos indirectos de una ciberoperación, como la interrupción de servicios esenciales o la desestabilización de infraestructuras críticas, deben ser considerados al evaluar la proporcionalidad de un ataque. Del mismo modo, el principio de precaución debe ampliarse para incluir medidas que minimicen los daños colaterales a los civiles en el ciberespacio. Así mismo, el principio de distinción para saber cuál es el perpetrador del acto.

10. Conclusiones

A partir de los hallazgos de esta investigación, se pueden extraer varias ideas clave sobre la aplicación del DIH en el contexto del ciberespacio y los desafíos que enfrentan los Estados y las instituciones internacionales en la regulación de las ciberoperaciones.

Primero la ausencia de una definición precisa de "ataque" en el ciberespacio representa una laguna jurídica significativa que dificulta la adecuada protección de la población civil y las infraestructuras críticas. Las cualidades representativas de las ciberoperaciones, que varias ocasiones no causan daño físico inmediato, pero pueden tener consecuencias catastróficas, dan a conocer las limitaciones del marco normativo actual del DIH, que fue creado para conflictos convencionales. Además, por otro lado, cabe aclarar que hay un riesgo evidente que cualquier ataque que cause un daño indirecto, se implemente como un ataque en el DIH.

Se evidencia la necesidad de revisar los principios de distinción, proporcionalidad y precaución en el contexto de las ciberoperaciones. Estos principios, esenciales para limitar los efectos de la guerra sobre los civiles, son difíciles de aplicar en el ciberespacio debido a la interconexión de infraestructuras civiles y militares y a la naturaleza indirecta de muchos efectos cibernéticos. Esto implica que el DIH, tal como está estructurado

actualmente, no logra responder adecuadamente a los riesgos inherentes a las operaciones cibernéticas.

La investigación muestra que existen divergencias significativas en la interpretación de "ataque" entre diferentes Estados, lo que genera incoherencias en la aplicación del DIH en el ciberespacio. Mientras algunos países avanzan hacia una definición que abarca las ciberoperaciones contra infraestructuras críticas, otros mantienen una interpretación conservadora que limita el término a los ataques físicos. Este desacuerdo normativo subraya la urgencia de alcanzar un consenso internacional que permita una aplicación coherente del DIH en este ámbito.

Los esfuerzos actuales, como el Manual de Tallin 2.0, aunque constituyen un avance en la interpretación del DIH para el ciberespacio, no logran cubrir plenamente los riesgos y características particulares de las ciberoperaciones. La falta de un consenso más amplio refleja las limitaciones de los enfoques actuales y señala la necesidad de desarrollar una normativa específica que regule el ciberespacio en el marco del DIH.

Esta investigación concluye que el desarrollo de un marco normativo adaptado a las ciberoperaciones requiere una acción concertada a nivel internacional. La cooperación entre Estados y la creación de normas precisas para el ciberespacio permitirían que el DIH continúe cumpliendo su propósito de proteger a la población civil y limitar el impacto de los conflictos armados en un entorno cada vez más digitalizado. Esta adecuación normativa es necesaria tanto para la protección de los sujetos protegidos por el DIH, así como, para garantizar la estabilidad y seguridad internacional en una era marcada por la interdependencia tecnológica.