DILEMAS ÉTICOS QUE SURGEN DE LAS TÁCTICAS Y TECNOLOGÍAS UTILIZADAS EN LA GUERRA CIBERNÉTICA

ETHICAL DILEMMAS ARISING FROM THE TACTICS AND TECHNOLOGIES USED IN CYBER WARFARE

Daniel David Vegas Rincón [8]
https://orcid.org/0000-0003-2877-6786

Resumen

Estudiar los dilemas éticos que surgen de las tácticas y tecnologías utilizadas en la guerra cibernética radica en un fenómeno que redefine las dinámicas del conflicto armado. No se trata únicamente de vulnerar sistemas digitales, sino de exponer a poblaciones a riesgos que afectan derechos fundamentales como la seguridad, salud y la vida. En este sentido, reflexionar sobre la dimensión ética y legal de la guerra cibernética resulta crucial para evitar que la tecnología se convierta en un terreno sin normas, donde la eficacia técnica prime sobre los valores humanos universales, poniendo en entredicho la vigencia del Derecho Internacional Humanitario y los principios básicos de justicia y equidad. Se concluye que los dilemas éticos en la guerra cibernética son complejos, pues el uso de tecnologías ofensivas puede afectar a civiles y comprometer la integridad de infraestructuras críticas, evidenciando la urgencia de criterios claros y universales. El marco normativo internacional en ocasiones dificulta la atribución de responsabilidades y la aplicación efectiva del Derecho Internacional Humanitario, existiendo la necesidad de articular principios éticos, respetando los derechos humanos y la soberanía estatal, a fin de construir un marco internacional preciso y responsable, capaz de enfrentar retos en ciberseguridad y guerra cibernética.

Palabras clave: dilemas éticos, tecnologías, guerra cibernética, ciberseguridad.

Abstract

Studying the ethical dilemmas that arise from the tactics and technologies used in cyber warfare lies in a phenomenon that redefines the dynamics of armed conflict. It is not only about breaching digital systems, but also about exposing populations to risks that affect fundamental rights such as security, health, and life. In this sense, reflecting on the ethical and legal dimension of cyber warfare becomes crucial to prevent technology from turning into a lawless arena, where technical efficiency prevails over universal human values, undermining the validity of International Humanitarian Law and the basic principles of justice and equity. It is concluded that ethical dilemmas in cyber warfare are complex, since the use of offensive technologies can affect civilians and compromise the integrity of critical infrastructures, highlighting the urgency of clear and

[8] Independiente
Venezuela
Correo: Juris.vegas@gmail.com

Recibido: 11-09-25
Aceptado: 13-10-25

universal criteria. The international regulatory framework at times hinders the attribution of responsibilities and the effective application of International Humanitarian Law, evidencing the need to articulate ethical principles while respecting human rights and state sovereignty, in order to build a precise and responsible international framework capable of addressing the challenges of cybersecurity and cyber warfare.

Keywords: ethical dilemmas; technologies; cyber warfare; cybersecurity.

Introducción

En la actualidad, la guerra cibernética se ha convertido en uno de los fenómenos más complejos y desafiantes del escenario internacional. La creciente dependencia de la tecnología en todos los ámbitos de la vida social, política y económica ha abierto nuevas puertas para que los conflictos se desarrollen más allá del espacio físico tradicional, trasladándose al ciberespacio. Y es que, a diferencia de los conflictos convencionales, las operaciones cibernéticas permiten atacar infraestructuras críticas, manipular información y afectar la seguridad de Estados y ciudadanos sin necesidad de disparar un solo proyectil, lo que genera dilemas éticos y legales sin precedentes.

El principal desafío reside en la ausencia de consensos claros sobre lo que constituye un "ataque armado" en el ciberespacio y en cómo deben aplicarse los principios del Derecho Internacional Humanitario en este contexto. La dificultad para atribuir responsabilidades, la multiplicidad de actores involucrados (estados y organizaciones no estatales) y la velocidad de las operaciones cibernéticas generan un panorama donde los marcos normativos existentes resultan insuficientes. De esta manera, se evidencia la necesidad de revisar críticamente las normas internacionales y los principios éticos que regulan el uso de tecnologías ofensivas, garantizando a la vez la protección de los derechos humanos y la soberanía estatal.

Por otra parte, la guerra cibernética plantea interrogantes éticos fundamentales. ¿Hasta qué punto es legítimo emplear ciberataques que puedan afectar indirectamente a la población civil? ¿Cómo se equilibran los objetivos estratégicos de seguridad con los valores universales de la dignidad humana? Estas tensiones subrayan la importancia de generar criterios claros que guíen las acciones de los Estados y actores involucrados, evitando arbitrariedades y promoviendo una cultura de responsabilidad y ética en el ciberespacio. Casos como Stuxnet y WannaCry ilustran de manera contundente cómo la falta de regulación específica puede tener impactos de largo alcance, tanto en términos de seguridad como de ética y legalidad.

En este contexto, el objetivo general de esta investigación es desarrollar un análisis crítico sobre los aspectos éticos y legales que emergen de las tácticas y tecnologías utilizadas en la guerra cibernética, con base en el Derecho Internacional y los principios fundamentales de la ética aplicada al conflicto armado. Asimismo, el estudio busca identificar las lagunas normativas existentes, analizar los dilemas éticos más relevantes y proponer estrategias orientadas a la construcción de un marco jurídico internacional más preciso y responsable, capaz de enfrentar los desafíos de la guerra cibernética en el siglo XXI.

Desarrollo

En el actual escenario geopolítico, el desarrollo tecnológico ha transformado profundamente la naturaleza de los conflictos armados, dando lugar a nuevas modalidades de enfrentamiento que trascienden los límites físicos tradicionales. Entre estas, la guerra cibernética se ha consolidado como una amenaza silenciosa pero poderosa, en la que los ataques a infraestructuras críticas, sistemas de defensa, plataformas de información y redes gubernamentales pueden generar consecuencias devastadoras sin necesidad de intervención militar directa. Esta realidad plantea desafíos significativos al Derecho Internacional y a la ética de la guerra, ya que los marcos normativos existentes no han evolucionado al ritmo del progreso tecnológico.

Indica Giudici (2021) que “durante los últimos años la Guerra Cibernética o Ciberguerra se ha transformado en un desafío para aquellos que custodian la soberanía y los intereses nacionales de los Estados” (p. 5), lo cual es un claro ejemplo de cómo en un conflicto multidimensional un actor utiliza los medios técnicos de ciberguerra en su maniobra estratégica, buscando resolver el conflicto a su favor, evitando que otros actores usaran medios más violentos y ganando tiempo político en todo el escenario.

La guerra ya no se libra únicamente en trincheras físicas ni en campos de batalla visibles. Hoy, un ataque puede originarse desde una computadora ubicada a miles de kilómetros y causar estragos en infraestructuras críticas, como plantas energéticas, hospitales o sistemas financieros. La llamada guerra cibernética plantea un reto profundo porque no encaja del todo en las categorías tradicionales del derecho internacional humanitario ni en las normas clásicas sobre el uso de la fuerza entre Estados.

Como advierte Llorens (2017), "la mayor dependencia de los Estados de las tecnologías de la información y comunicación y consecuentemente su mayor vulnerabilidad ha provocado que la ciberseguridad se convierta en uno de los principales tópicos de debate de la comunidad internacional" (p. 1), de ahí que el ciberespacio no respeta fronteras soberanas de la misma manera que lo hace el territorio físico, lo que complica la atribución de responsabilidades y la aplicación de las normas existentes.

A diferencia de los conflictos armados convencionales, en la guerra cibernética no siempre es posible identificar con claridad al agresor, ni medir los efectos inmediatos de un ataque. La atribución, la proporcionalidad del daño, la distinción entre objetivos militares y civiles, y la protección de derechos fundamentales, son elementos que generan vacíos jurídicos y dilemas éticos difíciles de resolver. Además, muchas de las tácticas cibernéticas utilizadas por Estados o actores no estatales se desarrollan en zonas grises del derecho, en las que no existe consenso internacional sobre su licitud o legitimidad.

En este contexto, se hace necesario abordar de manera crítica los aspectos éticos y legales implicados en el uso de tecnologías cibernéticas ofensivas, con el propósito de comprender sus implicaciones para la paz, la seguridad internacional y la protección de los derechos humanos. El objeto de estudio de esta investigación se centra, por tanto, en el análisis de los dilemas éticos y jurídicos que surgen del uso de tácticas de guerra cibernética, así como en la evaluación del marco legal internacional aplicable y la generación de propuestas que contribuyan a su fortalecimiento.

Comprender la complejidad del fenómeno cibernético en el ámbito bélico no solo es relevante desde una perspectiva académica, sino también estratégica, en un mundo cada vez más interconectado y vulnerable a este tipo de amenazas invisibles pero reales. El problema se intensifica cuando se piensa en los dilemas éticos, al plantearse si es legítimo un ataque cibernético que paraliza el sistema de salud de un país durante una crisis sanitaria, o que ocurre con los daños indirectos que afectan a civiles, aunque el objetivo inicial fuese militar. Ambos escenarios obligan a reflexionar sobre si el marco jurídico vigente es suficiente para dar respuestas claras o si, por el contrario, se está frente a un vacío normativo que abre la puerta a la impunidad.

Como sostiene Porche (2020), "la ambigüedad en la definición de un "acto de guerra" en el ciberespacio genera un área gris peligrosa donde los Estados pueden actuar sin temor a sanciones inmediatas" (p. 81). Es por ello, que el conflicto en el ciberespacio es cada vez más frecuente en todos los sectores públicos y privados y preocupa en muchos sentidos.

Otro aspecto crucial radica en la dificultad para establecer la autoría de un ataque. Mientras que en una agresión militar tradicional se puede identificar al atacante, en el mundo digital los ataques suelen camuflarse detrás de múltiples capas de anonimato, empleando redes de terceros o incluso equipos infectados de civiles inocentes. Esto complica la aplicación de principios fundamentales del derecho internacional, como el de proporcionalidad y distinción, previstos en los Convenios de Ginebra (Comité Internacional de la Cruz Roja, 2020).

El dilema ético en torno a la guerra cibernética radica en la necesidad de equilibrar la seguridad nacional con la protección de los derechos humanos y los valores universales de la dignidad humana. La falta de consensos claros sobre lo que constituye un "ataque armado" en el ciberespacio pone de manifiesto un desafío complejo que no se limita al ámbito jurídico, sino que alcanza también una dimensión filosófica. Este escenario evidencia que el derecho internacional enfrenta la urgencia de adaptarse a un campo de confrontación inédito, donde las tácticas y tecnologías digitales transforman las formas de agresión y redefinen las nociones tradicionales de soberanía, responsabilidad y proporcionalidad.

Asimismo, se plantea la necesidad de que los Estados y organismos multilaterales avancen hacia la construcción de un marco normativo específico, capaz de brindar respuestas claras frente a los vacíos existentes y de garantizar que los principios fundamentales del derecho internacional humanitario se apliquen también en el terreno digital.

Una de las principales causas de la problemática en torno a la guerra cibernética es la velocidad con la que avanzan las tecnologías de la información en contraste con la lentitud de los marcos normativos internacionales. Mientras los Estados y actores no estatales desarrollan capacidades ofensivas en el ciberespacio con gran rapidez, los instrumentos jurídicos existentes permanecen anclados en concepciones tradicionales del conflicto armado, lo que genera vacíos legales y dificultades interpretativas.

Otro factor determinante es la falta de consenso entre los Estados acerca de la definición misma de la guerra cibernética y de lo que constituye un "ataque armado" en este ámbito. Esta ausencia de criterios uniformes favorece la proliferación de interpretaciones ambiguas que permiten justificar acciones agresivas bajo la apariencia de operaciones defensivas o de mera ciberdelincuencia.

Además, la complejidad técnica del ciberespacio contribuye a la opacidad de los ataques, dificultando la atribución de responsabilidades. Los agresores pueden ocultar su identidad

mediante técnicas de enmascaramiento digital o utilizar redes de terceros países, lo que complica la aplicación del principio de responsabilidad internacional de los Estados. A ello se suma el creciente interés de actores privados, grupos criminales y organizaciones terroristas que encuentran en el ciberespacio un campo fértil para actuar con menores costos y altos niveles de impunidad.

No obstante, las consecuencias, son amplias y de gran impacto para la seguridad internacional. En primer lugar, los vacíos legales y éticos generan un terreno fértil para la impunidad, donde los Estados y actores no estatales pueden ejecutar ciberataques sin que existan mecanismos efectivos de sanción o disuasión. Esto debilita la confianza en el sistema internacional y puede escalar hacia conflictos híbridos de difícil contención.

En el plano humanitario, la falta de regulaciones claras expone a las poblaciones civiles a riesgos graves. Un ataque dirigido contra infraestructuras críticas, como redes eléctricas, sistemas de agua potable o servicios de salud, puede tener consecuencias devastadoras, incluso sin que se dispare una sola bala. Tal situación contraviene los principios de distinción y proporcionalidad establecidos en el Derecho Internacional Humanitario, poniendo en entredicho la vigencia de las normas diseñadas para proteger a las personas en tiempos de guerra.

En definitiva, la guerra cibernética representa un terreno de tensiones donde las fronteras entre lo legal, lo ético y lo estratégico se desdibujan, generando incertidumbres que exigen respuestas claras desde el derecho internacional y la reflexión ética. La magnitud de los riesgos y el impacto potencial sobre poblaciones civiles e infraestructuras críticas obligan a repensar los marcos normativos vigentes y a cuestionar la suficiencia de los principios tradicionales frente a un campo de confrontación en constante transformación.

Materiales y métodos

En este estudio se empleó el paradigma interpretativo, el cual se centra en comprender la realidad desde la perspectiva de los actores involucrados, reconociendo que el conocimiento no es absoluto ni objetivo, sino construido socialmente. Según Hernández, Fernández y Baptista (2014), “el paradigma interpretativo se interesa por el significado que los individuos atribuyen a los hechos, buscando comprender la realidad desde el punto de vista de quienes la viven” (p. 21).

Este enfoque resulta especialmente útil en estudios de fenómenos complejos y contextuales, como la guerra cibernética, donde las acciones de los Estados, organizaciones y actores no estatales deben analizarse considerando motivaciones, percepciones y valores culturales y éticos.

Por otra parte, se asumió como cualitativo, debido a que la realidad es compleja y aunque no es totalmente desconocida para el sujeto investigador, concibe el proceso de investigación social de manera diversa, múltiple e intersubjetiva, sustentándose en la incorporación de aspectos, a partir de fenómenos (sociales, culturales, espirituales, ideológicos, entre otros), que requieren ser estudiados desde las cualidades humanas, rasgos y comportamientos, los cuales pueden ser manifestados por los actores sociales bajo un carácter intersubjetivo de la realidad, permitiendo identificar, describir, interpretar, analizar y descubrir elementos vinculados en sus vivencias y experiencias.

La investigación cualitativa resulta especialmente pertinente para el estudio de la guerra cibernética, ya que permite explorar en profundidad los fenómenos complejos que rodean este nuevo escenario de conflicto, más allá de los datos técnicos o estadísticos. Mediante la interpretación de documentos legales, marcos normativos, informes de ciberseguridad y percepciones de actores involucrados, este enfoque posibilita comprender las dimensiones éticas, jurídicas y estratégicas de los ciberataques, así como sus implicaciones para los derechos humanos y la seguridad internacional.

De esta manera, la investigación cualitativa aporta un análisis integral, sensible al contexto y a los valores, que permite construir un conocimiento crítico y fundamentado sobre la ciberguerra y sus repercusiones globales. En cuanto a los escenarios de la investigación en el estudio de la guerra cibernética comprenden tanto contextos teóricos como prácticos en los que se manifiestan los fenómenos objeto de análisis. En el plano teórico, el escenario incluye el Derecho Internacional, los principios del Derecho Internacional Humanitario y los marcos éticos aplicados al conflicto armado, que sirven como base para interpretar y evaluar las acciones de los Estados y actores no estatales en el ciberespacio.

En el ámbito práctico, los escenarios abarcan los ataques cibernéticos reales, la operatividad de infraestructuras críticas, las políticas de ciberseguridad de los Estados y la interacción de plataformas digitales en la difusión de información, lo que permite observar las consecuencias sociales, legales y estratégicas de la ciberguerra. Así, los escenarios de la investigación

proporcionan un marco integral que articula teoría, práctica y ética, asegurando que el análisis sea contextualizado, crítico y aplicable a la realidad de los conflictos cibernéticos.

En cuanto a la investigación, las técnicas e instrumentos de recolección de datos permitieron la separación de los datos obtenidos, de manera que, una vez organizado se precedió al análisis respectivo. Es decir, que ya organizada la información se pasó a desagregar, descomponer en partes todos los elementos de tal manera que permita la profundización en el conocimiento de cada una de ellas, a la interpretación y asimismo llegar una síntesis a la luz de los conocimientos teóricos que sustentan el estudio.

Resultados o hallazgos

El uso de tecnologías cibernéticas ofensivas en conflictos contemporáneos ha abierto un terreno lleno de dilemas éticos complejos, donde la línea entre defensa y agresión se difumina peligrosamente. Y es que, a diferencia de las armas tradicionales, los ataques cibernéticos pueden afectar infraestructuras críticas sin un enfrentamiento físico directo, dejando consecuencias invisibles pero devastadoras: hospitales que dejan de funcionar, redes eléctricas que colapsan, o sistemas financieros paralizados. Este tipo de acciones plantea una pregunta ética inevitable: ¿hasta qué punto es legítimo causar daño indirecto a la población civil en nombre de objetivos militares o estratégicos? La respuesta no es sencilla, porque la virtualidad del daño no disminuye su gravedad real y tangible para quienes lo sufren.

Además, surge el dilema de la proporcionalidad y la discriminación, principios fundamentales del Derecho Internacional Humanitario. Los ataques cibernéticos a menudo no pueden limitarse únicamente a objetivos militares; los sistemas interconectados hacen que las repercusiones se propaguen como un virus, alcanzando a ciudadanos inocentes, empresas privadas o incluso naciones enteras no involucradas directamente en el conflicto. Asimismo, se enfrenta el problema de la atribución, es decir, la dificultad de identificar con certeza al responsable del ataque. Esta ambigüedad complica la rendición de cuentas y permite que Estados o actores no estatales justifiquen acciones que, en un contexto convencional, serían consideradas violaciones graves del derecho internacional.

Por otra parte, los ataques cibernéticos plantean un dilema ético relacionado con la transparencia y la responsabilidad. A diferencia de la guerra convencional, donde los combates

son visibles y sujetos a inspección, en el ciberespacio las operaciones pueden realizarse en secreto, sin que haya mecanismos claros para supervisarlas o controlarlas. Esto genera un riesgo latente de abuso: Estados o grupos pueden llevar a cabo ataques devastadores sin enfrentar consecuencias inmediatas, dejando a la comunidad internacional con una sensación de impotencia. Y es que, detrás de cada línea de código malicioso, hay vidas humanas, economías vulnerables y confianza social erosionada, elementos que no pueden pasarse por alto en un análisis ético riguroso.

La velocidad y sofisticación de estas tecnologías amplifican el dilema moral. Un ataque que hoy podría considerarse controlado puede, en cuestión de minutos, desatar un efecto dominó que nadie anticipó: sistemas de transporte que fallan, cadenas de suministro colapsadas, o información crítica manipulada para generar caos social. En este sentido, el desafío ético no solo se limita a decidir si usar o no estas herramientas, sino también a contemplar las consecuencias imprevisibles y al impacto en la vida cotidiana de millones de personas. Por ello, estudiar estos dilemas no es un lujo académico, sino una necesidad urgente para construir marcos legales y éticos que guíen la conducta de los Estados y actores no estatales en un escenario cada vez más digitalizado y complejo.

Uno de los dilemas legales más urgentes en la guerra cibernética es la falta de consenso internacional sobre la calificación de los ciberataques. ¿Constituye un ciberataque contra la red eléctrica de un país un “uso de la fuerza” en los términos del artículo 2(4) de la Carta de las Naciones Unidas? ¿O debe considerarse un “ataque armado” capaz de activar el derecho a la legítima defensa, contemplado en el artículo 51? La ambigüedad en estas definiciones genera un terreno jurídico incierto que los Estados aprovechan, ya sea para justificar represalias desproporcionadas o para evadir responsabilidades. Y es que el derecho internacional vigente fue diseñado en un mundo analógico, mientras que los conflictos actuales se libran en un entorno interconectado y digital.

Por otra parte, se encuentra el dilema de la atribución de responsabilidad internacional. En el ciberespacio, rastrear con precisión al autor de un ataque es técnicamente complejo y, muchas veces, imposible con certeza absoluta. Esto abre la puerta a acusaciones infundadas, escaladas diplomáticas injustificadas o, al contrario, a la impunidad de actores estatales y no estatales que actúan bajo la sombra del anonimato. El Proyecto de Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos, elaborado por la Comisión de Derecho Internacional

(CDI), establece parámetros de imputación de conductas a los Estados, pero su aplicación práctica en el ciberespacio aún es limitada y difusa.

Asimismo, el principio de soberanía digital ha desatado controversias legales significativas. Mientras algunos Estados sostienen que cualquier intromisión en sus sistemas informáticos constituye una violación de soberanía, otros argumentan que solo los ataques con efectos equiparables al uso de la fuerza violan este principio. Esta falta de uniformidad en la interpretación jurídica dificulta la construcción de un marco común y genera tensiones permanentes en la arena internacional. Además, pone de manifiesto un dilema de fondo: ¿hasta qué punto el derecho internacional puede adaptarse a un espacio sin fronteras físicas como el ciberespacio?

Finalmente, existe el dilema de la aplicación del Derecho Internacional Humanitario (DIH). Aunque principios como la distinción, la proporcionalidad y la necesidad militar deberían guiar cualquier operación en tiempos de conflicto, su aplicación práctica a ciberataques es altamente problemática. Por ejemplo, diferenciar entre un servidor militar y uno civil interconectado en la misma red es extremadamente difícil, lo que complica garantizar la protección de la población civil. El Comité Internacional de la Cruz Roja (2019) ha advertido que, si no se adapta y aplica el DIH al ciberespacio, la población civil quedará expuesta a riesgos inaceptables derivados de operaciones militares digitales.

En síntesis, los dilemas legales que plantea la ciberguerra reflejan un vacío normativo y una tensión constante entre el derecho internacional clásico y los desafíos de la era digital. Mientras los marcos jurídicos internacionales intentan dar respuesta, los actores estatales y no estatales ya operan en un terreno en el que las reglas son difusas, lo que incrementa la posibilidad de abusos, impunidad y conflictos no regulados.

Aunado a ello, la discusión sobre la necesidad de criterios legales y éticos claros para la regulación de los ciberataques no es un asunto de lujo académico, sino una urgencia que late en el corazón de la seguridad global. Y es que, en el ciberespacio, las fronteras se desdibujan y los ataques pueden atravesar en segundos lo que en el mundo físico tardaría meses en planificarse. Un virus informático capaz de paralizar hospitales, sistemas de agua potable o redes eléctricas no solo genera un problema técnico: también plantea un dilema humano profundo. ¿Hasta qué punto un Estado puede defenderse sin vulnerar los derechos fundamentales de la población civil que, al final del día, resulta siempre la más afectada?

Además, la soberanía estatal se convierte en un terreno frágil. Si un país logra infiltrar de manera encubierta la infraestructura crítica de otro, ¿se trata de espionaje tolerado o de un acto hostil que roza el umbral de agresión armada? Aquí la claridad legal brilla por su ausencia, lo que deja espacio a interpretaciones interesadas. Por otra parte, la ausencia de normas claras favorece la impunidad: un ataque puede ser devastador y, sin embargo, el atacante permanecer invisible, amparado en el anonimato que ofrece el ciberespacio. La falta de criterios compartidos convierte al derecho internacional en un "rompecabezas incompleto" que los Estados intentan armar con piezas prestadas de otras áreas del derecho.

Asimismo, la dimensión ética no puede quedar relegada a un segundo plano. Un ciberataque contra un sistema financiero puede desestabilizar economías enteras, afectando el acceso a bienes básicos o servicios de salud. No hablamos de daños colaterales abstractos, sino de personas reales que verían interrumpida su vida cotidiana. La ética exige preguntarse: ¿es moralmente justificable utilizar herramientas digitales que, aunque busquen objetivos militares, inevitablemente afectan a millones de civiles? Un marco regulatorio sin brújula ética corre el riesgo de convertirse en una simple técnica de control del poder, más que en una garantía de justicia y humanidad.

En definitiva, avanzar hacia criterios legales y éticos claros es una tarea pendiente que combina tanto la letra fría del derecho como la calidez de los valores humanos. Un equilibrio entre el respeto a la soberanía estatal y la protección de los derechos humanos no solo es deseable, sino imprescindible para evitar que el ciberespacio se transforme en un campo de batalla sin reglas. Tal como ocurrió con las guerras convencionales en siglos pasados, la humanidad necesita un consenso que ponga límites y recuerde que, incluso en el terreno digital, la dignidad humana debe estar en el centro de toda decisión.

La discusión sobre la necesidad de criterios legales y éticos claros para la regulación de los ciberataques no es un asunto de lujo académico, sino una urgencia que late en el corazón de la seguridad global. Y es que, en el ciberespacio, las fronteras se desdibujan y los ataques pueden atravesar en segundos lo que en el mundo físico tardaría meses en planificarse. Un virus informático capaz de paralizar hospitales, sistemas de agua potable o redes eléctricas no solo genera un problema técnico: también plantea un dilema humano profundo. ¿Hasta qué punto un Estado puede defenderse sin vulnerar los derechos fundamentales de la población civil que, al final del día, resulta siempre la más afectada?

El ejemplo más conocido es el caso de Stuxnet (2010), un malware sofisticado diseñado para sabotear el programa nuclear iraní. Aunque técnicamente fue un éxito al ralentizar las centrifugadoras de uranio, abrió un debate ético y legal que aún resuena. ¿Se trató de una operación legítima de seguridad internacional o de un acto de guerra encubierto? Lo preocupante es que, en el proceso, Stuxnet se propagó más allá de su objetivo original, demostrando que los daños colaterales en el ciberespacio son tan incontrolables como en los conflictos armados tradicionales. Además, mostró la vulnerabilidad de infraestructuras críticas que sostienen la vida cotidiana de millones de personas.

Por otra parte, está el caso del ransomware WannaCry (2017), que se expandió rápidamente a nivel global y afectó gravemente a servicios esenciales como el sistema de salud británico (NHS). Miles de cirugías fueron canceladas, ambulancias desviadas y pacientes expuestos a riesgos innecesarios por una falla digital. Aquí la pregunta ética se vuelve aún más clara: ¿cómo justificar una acción que afecta directamente la salud y la seguridad de civiles inocentes? Además, el hecho de que se atribuyera a actores no estatales con apoyo de gobiernos reveló lo difuso que es el límite entre delincuencia organizada y operaciones con motivación política.

Asimismo, otros casos como el ataque a la red eléctrica de Ucrania en 2015, que dejó sin suministro a cientos de miles de ciudadanos en pleno invierno, muestran la cara más cruda de la guerra cibernética: la capacidad de usar la tecnología para generar sufrimiento humano directo. Estos episodios no son simples “fallos técnicos”, sino recordatorios de que el ciberespacio puede convertirse en un campo de batalla donde la población civil paga el precio más alto.

En definitiva, avanzar hacia criterios legales y éticos claros es una tarea pendiente que combina tanto la letra fría del derecho como la calidez de los valores humanos. Un equilibrio entre el respeto a la soberanía estatal y la protección de los derechos humanos no solo es deseable, sino imprescindible para evitar que el ciberespacio se transforme en una guerra invisible sin reglas. Tal como ocurrió con las guerras convencionales en siglos pasados, la humanidad necesita un consenso que ponga límites y recuerde que, incluso en el terreno digital, la dignidad humana debe estar en el centro de toda decisión.

Discusión

La creciente complejidad de la guerra cibernética ha dejado en evidencia que el derecho internacional, tal como lo conocemos, no ofrece respuestas suficientes frente a los desafíos del siglo XXI. Los ciberataques, al no respetar fronteras físicas, erosionan la soberanía estatal y exponen a la población civil a riesgos inéditos, desde la interrupción de servicios hospitalarios hasta el colapso de sistemas eléctricos o financieros. Esta realidad plantea una exigencia ineludible: avanzar hacia un marco jurídico internacional más claro, preciso y éticamente responsable que reconozca la especificidad del ciberespacio como nuevo escenario de confrontación.

Hablar de guerra cibernética implica abrir un campo lleno de contradicciones y tensiones. Por un lado, está la fascinación por las tecnologías que parecen darle poder ilimitado a los Estados y actores no estatales. Por otro, aparece la inquietud sobre las consecuencias éticas de usar estas herramientas en escenarios de confrontación. ¿Hasta dónde puede justificarse una acción digital que vulnera sistemas esenciales de otro país, si al mismo tiempo deja expuesta la vida de miles de ciudadanos inocentes? Esa pregunta no tiene una respuesta simple, y allí comienza el dilema.

Uno de los aspectos más discutidos es la noción de proporcionalidad. En la guerra tradicional, los tratados internacionales fijan ciertos límites: no se puede atacar indiscriminadamente, no se pueden usar armas que provoquen sufrimiento innecesario. Pero en el ciberespacio, la línea es difusa. Un ataque contra un servidor eléctrico no solo interrumpe un servicio, también puede paralizar hospitales, dejar comunidades enteras sin agua o incluso provocar muertes indirectas. Aquí la ética se mezcla con lo imprevisible, y eso hace que cada táctica tecnológica tenga un peso moral muy difícil de medir.

Otro punto neurálgico está en la atribución. ¿Quién es el responsable cuando ocurre un ciberataque? Muchas veces no hay huellas claras, lo que genera un terreno propicio para acusaciones sin pruebas o represalias desproporcionadas. Desde una mirada ética, culpar sin certezas erosiona los principios básicos de justicia y transparencia. La ausencia de claridad no solo complica el Derecho Internacional, también alimenta una cultura de sospecha permanente que termina debilitando la confianza entre naciones.

Finalmente, hay que detenerse en la dimensión humana. Aunque se hable de algoritmos, firewalls o malware, detrás de cada clic hay vidas reales que pueden verse afectadas. El hecho de que la agresión no sea física no elimina la carga ética; por el contrario, la invisibilidad del daño puede volverlo aún más peligroso, porque se normaliza. En este punto, la discusión invita a

preguntarnos si la guerra cibernética está creando una especie de "zona gris" donde los valores humanos quedan relegados frente al poder de la técnica.

Por otra parte, resulta evidente que los vacíos normativos no solo generan incertidumbre, sino también incentivos para la impunidad y la manipulación estratégica de la ambigüedad. En este contexto, la construcción de reglas claras no puede limitarse a lo técnico o a lo militar, sino que debe incluir principios éticos, salvaguardas de derechos humanos y mecanismos prácticos de cooperación entre Estados.

En definitiva, los dilemas éticos que surgen de las tácticas y tecnologías usadas en la guerra cibernética no son meros debates académicos: son llamados de alerta. Nos obligan a repensar cómo aplicar principios universales de humanidad y justicia en un campo que, aunque intangible, es tan real y devastador como cualquier campo de batalla.

Conclusiones o Reflexiones

El ciberespacio, lejos de ser un terreno neutro, está profundamente atravesado por tensiones morales y jurídicas. La ausencia de un marco normativo consolidado deja a los Estados y actores no estatales en una zona gris donde las decisiones se toman con base en intereses estratégicos más que en principios universales. Esta indefinición multiplica el riesgo de que las operaciones cibernéticas se conviertan en instrumentos de agresión indiscriminada, afectando a poblaciones civiles que nada tienen que ver con los objetivos militares iniciales.

Por otra parte, la ciberguerra revela un dilema central: la asimetría entre la eficacia tecnológica y la protección de los derechos humanos. Mientras que la tecnología permite diseñar ataques precisos y devastadores, la falta de control ético hace que los efectos secundarios puedan ser masivos y desproporcionados. Casos como los ataques a sistemas de salud o de energía muestran que no se trata de amenazas abstractas, sino de realidades que comprometen la vida y la dignidad de millones de personas. Así, se confirma que los dilemas éticos no son meros debates teóricos, sino problemas tangibles que ponen en juego la humanidad misma en escenarios digitales.

Además, este propósito evidencia que las operaciones ofensivas en el ciberespacio no solo afectan a Estados en conflicto, sino también a la confianza internacional y la estabilidad global. La imposibilidad de atribuir con claridad la autoría de un ataque genera sospechas, escaladas de tensión y la posibilidad de represalias equivocadas. Desde la perspectiva ética, ello plantea un

problema aún más grave: la normalización del anonimato como excusa para evadir responsabilidades. La falta de atribución efectiva no debería convertirse en un salvoconducto para actuar sin límites, pues ello erosiona los principios básicos de la convivencia internacional.

De ahí que enfrentar los dilemas éticos de la ciberguerra exige ir más allá de la lógica militar o técnica. Es necesario incorporar la ética aplicada como brújula, para que los avances tecnológicos no sean usados de manera ciega, sino dentro de parámetros que resguarden la dignidad humana, la proporcionalidad en el uso de la fuerza y el respeto a la soberanía estatal. Solo al reconocer y abordar estos dilemas desde una perspectiva integral será posible construir un marco normativo y ético que responda adecuadamente a los desafíos de la guerra cibernética en el siglo XXI.

A su vez, las lagunas existentes permiten la proliferación de zonas grises en aspectos críticos como la atribución de ataques, la definición del umbral de "uso de la fuerza" en el ciberespacio y la responsabilidad de los Estados frente a actores no estatales. Estos vacíos no solo dificultan la aplicación uniforme del derecho, sino que también debilitan la capacidad de la comunidad internacional para responder con legitimidad y coherencia frente a ciberagresiones. En consecuencia, los Estados se ven tentados a actuar unilateralmente, lo que incrementa los riesgos de escalada y socava la confianza mutua.

Se evidenció que la ausencia de criterios legales y éticos claros en la regulación de los ciberataques genera un vacío normativo que dificulta la protección de los derechos humanos y la soberanía estatal. Los conflictos cibernéticos, al no estar adecuadamente delimitados, pueden provocar daños indiscriminados a infraestructuras críticas, sistemas de salud, servicios básicos y datos personales, afectando directamente a la población civil. Esto subraya la necesidad de una visualización integral de los principios rectores, que permita a los Estados y actores internacionales actuar con responsabilidad y coherencia frente a estas amenazas.

Los criterios éticos no pueden entenderse de manera aislada, sino que deben integrarse con los principios del Derecho Internacional Humanitario, la ética aplicada al conflicto armado y los estándares de protección de derechos humanos. La claridad en estos lineamientos permitirá no solo orientar la conducta de los Estados en el ciberespacio, sino también fomentar la cooperación internacional y la confianza entre actores globales, reduciendo la posibilidad de escaladas innecesarias y malentendidos en situaciones de tensión tecnológica.

Por otra parte, se resalta que la falta de parámetros definidos propicia la explotación de lagunas jurídicas por actores estatales y no estatales, lo que incrementa la vulnerabilidad de los

sistemas críticos y amenaza la estabilidad internacional. La investigación demuestra que establecer criterios claros y consistentes es indispensable para garantizar un equilibrio entre la seguridad nacional y la protección de la población, promoviendo un enfoque que respete simultáneamente la soberanía estatal y los derechos fundamentales.

La visualización de criterios éticos y legales claros constituye un eje estratégico para la construcción de un marco internacional más justo y eficaz frente a los ciberataques, permitiendo que la acción en el ciberespacio no se limite a la defensa tecnológica, sino que contemple responsabilidad, legalidad y principios humanitarios.

Referencias

Comité Internacional de la Cruz Roja (2019). *Derecho Internacional Humanitario y ciberoperaciones durante conflictos armados.* https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_armed_conflict_sp.pdf

Comité Internacional de la Cruz Roja (2020). *El Derecho Internacional Humanitario y los desafíos de los conflictos armados contemporáneos*. https://www.icrc.org/es/publication/el-derecho-internacional-humanitario-y-los-desafios-de-los-conflictos-armados

Giudici, D. (2021). *La influencia de la Guerra Cibernética en la relación entre estados Post Guerra Fría*. Trabajo de grado. Universidad de la Defensa Nacional. Argentina. https://cefadigital.edu.ar/bitstream/1847939/2749/1/TESIS%20MAESES%202021_GIUDICI.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6ª ed.). McGraw-Hill.

Llorens, M. (2017). *Los desafíos del uso de la fuerza en el ciberespacio*. https://www.sciencedirect.com/science/article/pii/S1870465417300508#:~:text=Schmitt;6262%20este%20autor,%2C70%20h)%20presunta%20legalidad.&text=Dichos%20factores%20no%20son%20exhaustivos,un%20uso%20de%20la%20fuerza

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

Porche, I. (2020). *Ciberguerra: Introducción a los conflictos en la era de la información.* https://dokumen-pub.translate.goog/cyberwarfare-an-introduction-to-information-age-conflict-1st-edition-1630815764-9781630815769-1630815780-9781630815783.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc.