Revista Revoluciones. Estudios en Ciencia Política, Humanidades y Sociales
Rev. Revoluciones. (2025). Vol. 7 Núm. 21
Editada por: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú
www.revistarevoluciones.com

ENSAYO

# Cibercrímenes de guerra: desafíos para la Corte Penal Internacional

## *Cyber War Crimes: Challenges for the International Criminal Court*

*Cibercrimes de Guerra: Desafios para o Tribunal Penal Internacional*

**María Márquez**[1]
UNIVERSIDAD CENTRAL DE VENEZUELA, CARACAS, VENEZUELA
mmarquezolmos@gmail.com
*https://orcid.org/0000-0001-7648-840X*

**DOI:** https://doi.org/10.35622/j.rr.2025.021.002
**Recibido:** 29-VII-2025 **/ Aceptado:** 26-VIII-2025 **/ Publicado:** 19-IX-2025

## Resumen

El presente ensayo tiene como objetivo analizar los cibercrímenes de guerra como un desafío para la Corte Penal Internacional. Para ello, se reflexiona sobre los ciberataques dirigidos contra infraestructuras críticas y se examina si este tipo de conductas puede ser comprendido dentro de los crímenes de guerra tipificados en el Estatuto de Roma. El trabajo se desarrolla a partir de un enfoque documental, utilizando artículos e investigaciones científicas que permiten interpretar y presentar información relevante sobre el tema abordado. Se sostiene que los cibercrímenes de guerra representan actualmente un desafío para la Corte Penal Internacional, en tanto los conflictos se ejecutan en un entorno complejo como el ciberespacio, lo que dificulta la identificación e individualización de los responsables, así como la obtención de medios probatorios que permitan acreditar su responsabilidad penal. No obstante, ello no excluye la posibilidad de que la Corte Penal Internacional recurra al apoyo de empresas tecnológicas para contar con herramientas técnicas que faciliten la investigación, persecución y captura de los responsables de este tipo de crímenes.

**Palabras clave:** ciberataques, ciberguerra, cibercrímenes de guerra, derecho internacional humanitario, infraestructuras críticas.

## Abstract

This essay aims to analyze cyber war crimes as a challenge for the International Criminal Court. To this end, it reflects on cyberattacks directed against critical infrastructures and examines whether this type of conduct can be understood within the war crimes typified in the Rome Statute. The work is developed from a documentary approach, using scientific articles and research that allow for the

[1] Docente en la Universidad Central de Venezuela.

ISSN: 2710-0499 ISSN-L: 2710-0480

interpretation and presentation of relevant information on the subject addressed. It is argued that cyber war crimes currently represent a challenge for the International Criminal Court, insofar as these conflicts take place in a complex environment such as cyberspace, which hinders the identification and individualization of those responsible, as well as the collection of evidentiary means to establish their criminal responsibility. Nevertheless, this does not preclude the possibility for the International Criminal Court to rely on the support of technology companies to obtain technical tools that facilitate the investigation, prosecution, and capture of those responsible for this type of crime.

**Keywords:** cyberattacks, cyber warfare, cyber war crimes, international humanitarian law, critical infrastructures.

## Resumo

Este ensaio tem como objetivo analisar os cibercrimes de guerra como um desafio para o Tribunal Penal Internacional. Para isso, reflete-se sobre os ciberataques dirigidos contra infraestruturas críticas e examina-se se esse tipo de conduta pode ser compreendido no âmbito dos crimes de guerra tipificados no Estatuto de Roma. O trabalho desenvolve-se a partir de uma abordagem documental, utilizando artigos e pesquisas científicas que permitem interpretar e apresentar informações relevantes sobre o tema abordado. Sustenta-se que os cibercrimes de guerra representam atualmente um desafio para o Tribunal Penal Internacional, uma vez que os conflitos ocorrem em um ambiente complexo como o ciberespaço, o que dificulta a identificação e individualização dos responsáveis, bem como a obtenção de meios probatórios que comprovem sua responsabilidade penal. No entanto, isso não exclui a possibilidade de o Tribunal Penal Internacional recorrer ao apoio de empresas tecnológicas para dispor de ferramentas técnicas que facilitem a investigação, persecução e captura dos responsáveis por esse tipo de crime.

**Palavras-chave:** ciberataques, ciberguerra, cibercrimes de guerra, direito internacional humanitário, infraestruturas críticas.

*"En la ciberguerra, el campo de batalla es el mundo entero, y el enemigo puede estar en cualquier parte".*
*Anónimo.*

## INTRODUCCIÓN

Con el transcurso del siglo XXI, las sociedades han experimentado una transformación progresiva debido a la incorporación de las tecnologías de información y comunicación (TIC), las cuales han proporcionado avances y beneficios no solo en la calidad de vida de los individuos, sino también en ámbitos como la ciencia, la educación, la economía, la medicina, la seguridad y la defensa, entre otros.

Las TIC, si bien han aportado innumerables beneficios a la sociedad actual, también pueden poner en riesgo la intimidad de las personas, generar pérdidas económicas significativas y comprometer la seguridad de un Estado mediante la ejecución de ciberataques. En este contexto, la intención del atacante consiste en robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos, a través del acceso no autorizado a una red, sistema informático o dispositivo digital. Por lo general, los ciberataques se producen conforme a tres (3) categorías: criminal, personal y política.

En el ciberataque por motivos criminales o delictivos, el ciberdelincuente procura obtener ganancias económicas, ya sea mediante el robo de dinero, la extorsión o la sustracción de datos, los cuales suelen emplearse para cometer robos de identidad, comercializarse en la Dark Web o mantenerse como mecanismo de presión para exigir un rescate. En lo que respecta al ciberataque por motivos personales, el atacante busca principalmente una retribución frente a algún descontento percibido en su entorno, ya sea laboral, familiar o educativo, pudiendo sustraer dinero, robar datos confidenciales o interrumpir los sistemas de una empresa. Por su parte, el ciberataque por motivos políticos se vincula con el hacktivismo, el ciberterrorismo o la ciberguerra; en este último supuesto, los actores de los Estados-Nación atacan agencias gubernamentales o infraestructuras estratégicas de sus adversarios (IBM, 2025a).

La ciberguerra no se desarrolla de manera abstracta; por el contrario, tiene un impacto profundo en la vida de las personas, ya que puede afectar infraestructuras críticas, como instalaciones médicas o sistemas de control para la generación de energía, desencadenando consecuencias inmediatas para amplios sectores de la población, en particular para los más vulnerables (Khan, 2023).

Ante un conflicto bélico ejecutado en el ciberespacio, la Corte Penal Internacional (CPI) debe interpretar el Estatuto de Roma de la misma forma en que se hace en el mundo físico, es decir, garantizando que la población civil y las infraestructuras críticas gocen del mismo nivel de protección. Para ello, resulta necesario que las armas cibernéticas cumplan con los límites establecidos para los medios y métodos tradicionales de guerra.

En definitiva, resulta urgente realizar una investigación detallada que analice los desafíos que enfrenta la Corte Penal Internacional (CPI) en esta materia, con el objeto de garantizar la ciberseguridad en contextos de conflicto armado, así como de asegurar que quienes cometan este tipo de cibercrímenes rindan cuentas ante la justicia penal internacional.

ISSN: 2710-0499 ISSN-L: 2710-0480

# METODOLOGÍA

Este ensayo optó por un análisis orientado a la reflexión crítica sobre los cibercrímenes de guerra y los desafíos que estos plantean para la Corte Penal Internacional (Marcelino Aranda et al., 2024).

Asimismo, el estudio adopta un enfoque de investigación documental, basado en la revisión, análisis e interpretación de fuentes secundarias pertinentes, tales como artículos científicos, instrumentos jurídicos internacionales, informes institucionales y referencias electrónicas confiables. Este enfoque permite integrar aportes doctrinales y normativos provenientes de distintas fuentes, ofreciendo una visión sistemática del fenómeno objeto de estudio y facilitando la construcción de argumentos jurídicos sustentados (Barraza, citado por Reyes-Ruiz y Carmona Alvarado, 2020).

# DESARROLLO

## Ciberespacio y la ciberseguridad en la era digital

A nivel internacional existe una creciente preocupación en torno al uso de las tecnologías de la información y la comunicación (TIC) y del ciberespacio como medios para la comisión de cibercrímenes. De acuerdo con el Manual de Tallin 2.0, el ciberespacio se define como un entorno conformado por componentes físicos y no físicos que permiten almacenar, modificar e intercambiar datos mediante el uso de redes computacionales (Organización de Estados Americanos [OEA], 2022).

El término *ciberespacio* proviene del griego *kybernetes*, que significa el arte de gobernar o manejar un navío. Dicho concepto fue posteriormente adaptado al campo de la cibernética y utilizado por primera vez en 1960 en el título *Atelier Cyberspace*, obra desarrollada por la artista Susanne Ussing y el arquitecto Carsten Hoff, quienes lo emplearon para denominar instalaciones sensoriales basadas en dispositivos de control remoto e imágenes, asociadas al estudio de la interacción tecnológica (Organización de Estados Americanos, 2022).

Con el auge de Internet durante la década de los noventa, el término ciberespacio adquirió una mayor relevancia conceptual, al asociarse inicialmente con la idea de que Internet constituía un dominio distinto del mundo real. Bajo esta concepción, se sostenía que dicho espacio se encontraba exento del control de los Estados y de la aplicación de sus normas jurídicas, quedando sujeto exclusivamente a la voluntad de sus usuarios. Esta postura dio lugar a un doble debate: por un lado, si el ciberespacio puede considerarse un dominio

independiente y, por otro, si debe o no regirse por normas jurídicas estatales e internacionales (Organización de Estados Americanos, 2022).

En términos generales, el ciberespacio comprende un conjunto de tecnologías digitales multidimensionales, estrechamente vinculadas a las actividades humanas, que se desarrollan en distintos dominios físicos del mundo real. Asimismo, puede entenderse como un medio artificial cuyo diseño y gobierno dependen tanto de soportes físicos (*hardware*) como virtuales (*software*), los cuales permiten modificar sus condiciones y capacidades. No obstante, estas modificaciones generan repercusiones directas en el mundo material, afectando de manera significativa la vida de los usuarios (García, 2021).

Debe advertirse que el ciberespacio enfrenta una problemática compleja, no solo debido a la ambigüedad que ofrece frente a la presencia de elementos hostiles, sino también por la amplitud de los efectos que produce, los cuales trascienden las fronteras físicas y los mecanismos institucionales tradicionales. Ante este escenario, la ciberseguridad se configura como una prioridad fundamental para la protección de los ciudadanos, las empresas y los Estados (García, 2021).

En este contexto, la ciberseguridad se refiere al conjunto de tecnologías, medidas y prácticas destinadas a prevenir los ciberataques o a mitigar su impacto. Su propósito principal es proteger sistemas, aplicaciones, dispositivos informáticos, datos confidenciales y activos financieros de personas, empresas y organizaciones gubernamentales frente a amenazas que van desde virus informáticos simples hasta ataques sofisticados como el *ransomware* (IBM, 2025b).

La tendencia en los últimos años evidencia un uso creciente de tecnologías de la información, tales como la computación en la nube, la inteligencia artificial, la creciente complejidad de las redes, el trabajo a distancia y la proliferación de dispositivos y sensores interconectados. Si bien estas innovaciones han generado importantes beneficios para la sociedad y el progreso humano, también han ampliado las oportunidades para que actores maliciosos ejecuten ciberataques de forma exponencial (IBM, 2025b).

Entre las amenazas más comunes en materia de ciberseguridad se encuentran el *malware*, el *ransomware*, el *phishing*, las amenazas internas y los ataques de denegación de servicio distribuido (*DDoS*). El *malware* se refiere a cualquier código o programa informático diseñado intencionalmente para dañar un sistema o afectar a sus usuarios. Por su parte, el *ransomware* constituye un tipo específico de *malware* que encripta los datos o dispositivos de la víctima con el objetivo de exigir un rescate a cambio de su liberación o de evitar un daño mayor.

ISSN: 2710-0499 ISSN-L: 2710-0480

En cuanto al *phishing*, este consiste en el envío de mensajes electrónicos, de texto o de voz destinados a engañar a los usuarios para que descarguen software malicioso, revelen información confidencial o realicen transferencias de fondos a terceros no autorizados (IBM, 2025b).

Seguidamente, se identifican las denominadas amenazas internas, las cuales se refieren a aquellas acciones realizadas por empleados de empresas privadas o entidades gubernamentales, contratistas o socios comerciales que, de manera premeditada o accidental, hacen un uso indebido de su acceso legítimo a sistemas o cuentas, los cuales pueden ser posteriormente aprovechados o secuestrados por ciberdelincuentes. Este tipo de amenazas resulta particularmente complejo de detectar, dado que presentan patrones de actividad autorizada y, en muchos casos, no son identificadas por soluciones tradicionales de seguridad como antivirus, *firewalls* u otros mecanismos diseñados principalmente para bloquear ataques externos.

Por su parte, los ataques de denegación de servicio distribuido (*DDoS*) tienen como objetivo bloquear el funcionamiento de un servidor, sitio web o red mediante la sobrecarga masiva de tráfico. Generalmente, estos ataques se ejecutan a través de *botnets*, es decir, redes de sistemas previamente comprometidos y controlados de forma remota por ciberdelincuentes mediante *malware*. En diversos escenarios, los ataques *DDoS* se combinan con estrategias de *ransomware* o se utilizan como mecanismo de extorsión, amenazando con su ejecución a cambio del pago de un rescate.

Para el diseño e implementación de una estrategia de ciberseguridad eficaz, resulta indispensable garantizar la protección integral de las distintas capas o dominios que conforman la infraestructura de las tecnologías de la información. En este sentido, la ciberseguridad abarca diversos ámbitos, entre los que destacan la seguridad de la infraestructura crítica, la seguridad de red, la seguridad de punto final, la seguridad de aplicaciones, la seguridad en la nube, la seguridad de la información y la seguridad móvil.

La seguridad de la infraestructura crítica se orienta a la protección de sistemas informáticos, redes, datos y activos digitales esenciales para el funcionamiento de sectores clave como la seguridad pública, la salud, la economía y la seguridad nacional. Complementariamente, la seguridad de red tiene como finalidad detectar y prevenir ataques cibernéticos y accesos no autorizados, garantizando que los usuarios legítimos puedan interactuar de forma segura con los recursos de red disponibles.

ISSN: 2710-0499 ISSN-L: 2710-0480

En cuanto a la seguridad de punto final, esta se enfoca en la protección de dispositivos como servidores, ordenadores de escritorio, portátiles y dispositivos móviles frente a posibles ciberataques. De manera paralela, la seguridad de aplicaciones busca resguardar tanto las aplicaciones instaladas localmente como aquellas que operan en entornos en la nube, evitando la explotación de vulnerabilidades que puedan ser utilizadas por actores maliciosos para comprometer sistemas o información.

Es importante tener en cuenta que *seguridad en la nube* se refiere a la protección de los servicios, datos, aplicaciones e infraestructuras alojadas en entornos *cloud*, bajo un modelo de responsabilidad compartida. En dicho modelo, el proveedor del servicio asume la protección de la infraestructura y los servicios ofrecidos, mientras que el usuario es responsable de salvaguardar los datos, el código y los activos digitales que almacena o ejecuta en la nube (IBM, 2025b).

Seguidamente, corresponde hacer referencia a la seguridad de la información, entendida como la protección de toda la información relevante de una organización, incluyendo archivos y datos digitales, documentos en formato físico, medios de almacenamiento e incluso la expresión humana, frente al acceso, divulgación, uso o alteración no autorizados. De manera complementaria, la seguridad móvil comprende un conjunto de disciplinas y tecnologías orientadas a la protección de teléfonos inteligentes y dispositivos móviles, incorporando herramientas como la gestión de aplicaciones móviles (*Mobile Application Management – MAM*) y la gestión de la movilidad empresarial (*Enterprise Mobility Management – EMM*) (IBM, 2025b).

En este contexto, la ciberseguridad es vital para proteger el funcionamiento de las sociedades contemporáneas, sus datos y sus infraestructuras críticas frente a ciberataques maliciosos, lo cual demanda una cultura de prevención, concienciación y prácticas responsables por parte de usuarios, organizaciones y Estados

**La ciberguerra como táctica ofensiva en los conflictos armados**

De acuerdo con el Comité Internacional de la Cruz Roja (CICR), la ciberguerra constituye un fenómeno relativamente reciente en el contexto de los conflictos armados. Este organismo la define como un conjunto de operaciones dirigidas contra computadoras o sistemas informáticos mediante flujos de datos, empleadas como método de guerra en el marco de un conflicto armado. Asimismo, la ciberguerra comprende aquellas medidas hostiles orientadas a descubrir, alterar, destruir, interrumpir o transferir datos almacenados,

ISSN: 2710-0499 ISSN-L: 2710-0480

procesados o transmitidos por sistemas informáticos pertenecientes al adversario (Comité Internacional de la Cruz Roja, 2021).

La ciberguerra presenta una serie de características distintivas, entre las que destacan su complejidad y asimetría, la delimitación específica de objetivos, su corta duración y la reducción de daños físicos directos sobre los combatientes. No obstante, amplía el espacio de combate, reduce la densidad de tropas, intensifica la disputa por la superioridad de la información y exige una capacidad de reacción rápida por parte de los mandos militares. A pesar de estas particularidades, sus consecuencias pueden resultar tan devastadoras como las generadas por los conflictos armados convencionales (Leiva, 2018).

En cuanto a los objetivos perseguidos mediante la ciberguerra, estos incluyen dañar sistemas o entidades hasta impedir su reconstrucción o funcionamiento, interrumpir o quebrantar el flujo de información, destruir datos del adversario, reducir la eficacia de los sistemas de comunicación enemigos, atacar infraestructuras críticas, engañar a los oponentes, acceder ilícitamente a sistemas informáticos y sustraer información sensible, entre otros fines estratégicos (Leiva, 2018).

La ciberguerra se vale de las capacidades tecnológicas y de red de un Estado para interrumpir, denegar, degradar, manipular o destruir información contenida en los sistemas informáticos de otro Estado, generalmente mediante la actuación de *hackers* que operan en favor del Estado atacante. En este sentido, se identifican tres tipos de ciberguerra: 1) *Personal Information Warfare*; 2) *Corporate/Organizational Level Information Warfare*; y 3) *Open/Global Scope Information Warfare* (Leiva, 2018).

El *Personal Information Warfare* se encuentra directamente vinculado con la seguridad personal, la privacidad de los datos y el acceso a las redes de información. Por su parte, el *Corporate/Organizational Level Information Warfare* se relaciona con prácticas de espionaje entre organizaciones de distinto nivel, ya sea de empresas hacia Estados o entre Estados. Finalmente, el *Open/Global Scope Information Warfare* abarca fenómenos asociados al ciberterrorismo, tales como ataques dirigidos a centros tecnológicos, el uso de propaganda digital para amplificar el impacto de los ataques, así como la planificación logística de atentados tradicionales, biológicos o tecnológicos mediante el uso de plataformas digitales (Leiva, 2018).

Ahora bien, debe precisarse que en el contexto de la ciberguerra existe una amplia variedad de posibles vectores de ataque. No obstante, sus operaciones suelen concentrarse en determinados métodos recurrentes, entre los que destacan

el *malware*, el *ransomware*, los ataques de denegación de servicio distribuido (*DDoS*), el espionaje, la subversión y las infiltraciones. En lo que respecta al *malware*, este comprende la creación de virus y gusanos informáticos destinados a atacar infraestructuras críticas del Estado afectado, provocando, por ejemplo, la interrupción de las comunicaciones, cortes en el suministro eléctrico o la paralización de servicios públicos esenciales (Buxton, 2023).

El *ransomware*, como una modalidad específica de *malware*, genera desequilibrios significativos en el país atacado al secuestrar redes o datos estratégicos, los cuales pueden ser utilizados como mecanismo de presión o como fuente de financiamiento para futuras operaciones de ciberguerra. En cuanto a los ataques de denegación de servicio distribuido (*DDoS*), estos emplean redes de dispositivos comprometidos (*botnets*) para saturar sistemas informáticos mediante el envío masivo de solicitudes falsas, con el objetivo de inutilizar servicios y afectar el normal funcionamiento de operaciones fundamentales del Estado atacado (Buxton, 2023).

El espionaje cibernético se utiliza con la finalidad de obtener información sensible, para lo cual se emplean técnicas como el *spear-phishing*, los ataques de fuerza bruta, el descifrado de contraseñas y el uso de programas espía (*spyware*), los cuales facilitan el acceso no autorizado a redes y la filtración de datos estratégicos. Por su parte, la subversión se orienta a la difusión de propaganda digital, incluyendo noticias falsas (*fake news*) y otras formas de desinformación, con el propósito de alterar el ecosistema mediático del país afectado, minar la confianza pública en las instituciones y autoridades, y generar discordia social. Estas acciones suelen ejecutarse de manera complementaria a otros ataques cibernéticos, potenciando su impacto político y social (Buxton, 2023).

Finalmente, las infiltraciones pueden ser llevadas a cabo por *hacktivistas*, confidentes u otros actores internos o externos que, de forma voluntaria o involuntaria, divulgan información confidencial de manera anónima, generalmente a través de la *dark web*. Estas filtraciones pueden contribuir, directa o indirectamente, al debilitamiento de la seguridad nacional del Estado afectado y facilitar la ejecución de ataques externos de mayor alcance (Buxton, 2023).

Al respecto, resulta pertinente señalar que uno de los primeros casos emblemáticos de ciberguerra tuvo lugar durante el conflicto con Estonia en el año 2007, mediante ataques de denegación de servicio distribuido (*DDoS*). Como respuesta a estos acontecimientos, en 2008 se creó el Centro de Defensa Cibernética de la Organización del Tratado del Atlántico Norte (OTAN), con sede en Tallin, Estonia. Dicho ciberataque ha sido considerado de gran magnitud, al

ISSN: 2710-0499 ISSN-L: 2710-0480

afectar a más de un millón de computadoras y comprometer infraestructuras críticas vinculadas con las comunicaciones, el comercio y la economía del país.

Igualmente, resulta pertinente hacer referencia a dos de los casos más recientes y representativos de ciberguerra en el contexto internacional. El primero corresponde al conflicto entre Rusia y Ucrania (2022–actualidad), en el cual se ha evidenciado una escalada sin precedentes de ciberataques. El mismo día del inicio de la invasión rusa se produjo un ataque cibernético dirigido contra el satélite de comunicaciones KA-SAT, lo que provocó la interrupción de las comunicaciones militares de Ucrania. Este ataque trascendió las fronteras del país afectado, dejando sin acceso a Internet a decenas de miles de personas en distintos Estados europeos, desde Francia hasta Ucrania. Incluso, un mes después del incidente, alrededor de 2 000 turbinas eólicas en Alemania continuaban fuera de funcionamiento, lo que evidencia el impacto transnacional de este tipo de operaciones cibernéticas (Burkhalter, 2022).

El segundo caso corresponde al conflicto entre Israel y Hamas (2023–2025). Según el informe *Tool of First Resort: Israel–Hamas War in Cyber*, elaborado por Google, se han registrado múltiples ciberataques entre Israel e Irán, así como actividades sostenidas de espionaje cibernético vinculadas con Hamas. El informe detalla agresiones reiteradas por parte de Irán contra Israel y entidades estadounidenses, con resultados variables en términos de efectividad y alcance (Adrados, 2024).

Asimismo, dicho informe revela hallazgos relevantes, como el uso recurrente de *malware* móvil en campañas de espionaje dirigidas contra Israel. De igual forma, se documenta que Hamas llevó a cabo operaciones cibernéticas que incluyeron campañas masivas de *phishing* en Palestina y países vecinos, ataques con *malware* contra entidades israelíes y acciones dirigidas contra infraestructuras críticas, como la inutilización de estaciones de gas en Irán, atribuida al grupo Gonjeshke Darande y vinculada a advertencias públicas asociadas a Israel. Además, se han identificado campañas de desinformación que incorporan el uso de inteligencia artificial, lo que incrementa la complejidad y el alcance de los ataques en el ciberespacio (Adrados, 2024).

En este escenario, el uso hostil del ciberespacio genera una preocupación creciente en materia de seguridad para los gobiernos, los particulares, las empresas y los medios de comunicación. Por tal motivo, el Comité Internacional de la Cruz Roja ha manifestado de manera reiterada su inquietud respecto al desarrollo de capacidades cibernéticas militares y su empleo en conflictos armados, al considerar que estas prácticas incrementan la sensación de inseguridad entre los Estados y otros actores internacionales.

**Cibercrímenes de guerra y el Estatuto de Roma de la Corte Penal Internacional**

Desde hace más de una década, el Comité Internacional de la Cruz Roja ha sostenido que el uso de capacidades cibernéticas en los conflictos armados debe someterse plenamente a los principios y normas del Derecho Internacional Humanitario (DIH), del mismo modo que cualquier otra arma, medio o método de guerra, ya sea nuevo o tradicional. No obstante, también ha señalado la necesidad de profundizar el debate entre los Estados acerca de la forma en que dichas normas deben interpretarse y aplicarse específicamente en el ciberespacio (Comité Internacional de la Cruz Roja, 2021).

Asimismo, el Comité Internacional de la Cruz Roja ha enfatizado que no existe una diferencia sustancial entre la guerra desarrollada en el ciberespacio y aquella que se ejecuta en los dominios terrestre, aéreo, marítimo o espacial. En este sentido, retoma lo establecido por la Corte Internacional de Justicia, la cual ha señalado que los principios y normas del Derecho Internacional Humanitario aplicables a los conflictos armados rigen para todas las formas de guerra y para todo tipo de armas, incluidas aquellas que puedan desarrollarse en el futuro (Comité Internacional de la Cruz Roja, 2021).

El Derecho Internacional Humanitario cuenta con un conjunto de instrumentos jurídicos fundamentales destinados a regular la conducción de los conflictos armados y a proteger a las personas que no participan directamente en las hostilidades. Entre estos instrumentos destacan los Convenios de Ginebra de 1949, los cuales han sido adoptados, hasta agosto de 2006, por 194 Estados. Dichos Convenios establecen normas específicas orientadas a la protección de los miembros de las fuerzas armadas —combatientes— que resulten heridos, enfermos o náufragos, así como de los prisioneros de guerra y la población civil. Asimismo, contemplan la protección del personal médico, los capellanes militares y el personal civil de apoyo a las fuerzas armadas, siendo complementados por los Protocolos Adicionales, que amplían y refuerzan las normas humanitarias aplicables en los conflictos armados (Cruz Roja Americana, 2006).

Los Convenios de Ginebra constituyen la piedra angular del Derecho Internacional Humanitario moderno y se estructuran actualmente en cuatro convenios y dos protocolos adicionales. Estos instrumentos reflejan los esfuerzos de la comunidad internacional por garantizar la protección de las personas afectadas por los conflictos armados. En particular, el Primer Convenio de Ginebra protege a los heridos y enfermos de las fuerzas armadas en campaña y se encuentra conformado por 64 artículos. El Segundo Convenio de Ginebra tiene

ISSN: 2710-0499 ISSN-L: 2710-0480

por objeto aliviar la suerte de los heridos, enfermos y náufragos de las fuerzas armadas en el mar y consta de 63 artículos. Por su parte, el Tercer Convenio de Ginebra garantiza el trato debido a los prisioneros de guerra y está compuesto por 143 artículos. Finalmente, el Cuarto Convenio de Ginebra se refiere a la protección de las personas civiles en tiempo de guerra y se encuentra integrado por 159 artículos (Cruz Roja Americana, 2006).

Debe señalarse que el Estatuto de Roma de la Corte Penal Internacional tipifica los crímenes de guerra en su artículo 8, el cual contiene un listado detallado de conductas que vulneran el derecho y las costumbres aplicables en los conflictos armados, generando responsabilidad penal individual. Dicho artículo define los crímenes de guerra como aquellas infracciones graves de los Convenios de Ginebra de 1949 cometidas en el marco de un conflicto armado (art. 8, Estatuto de Roma).

En este contexto, la Corte Penal Internacional solo puede ejercer su jurisdicción respecto de conductas que, por su gravedad, han sido calificadas como crímenes internacionales. Al analizar el artículo 8 del Estatuto de Roma, se advierte que en el literal b se contemplan las denominadas "otras violaciones graves de las leyes y usos aplicables en los conflictos armados internacionales", entre las cuales se incluyen los ataques dirigidos contra bienes de carácter civil e infraestructuras civiles esenciales o infraestructuras críticas. Este supuesto resulta particularmente relevante para el análisis de los ciberataques que, por su naturaleza y efectos, puedan afectar directamente a la población civil o a servicios indispensables para su supervivencia (art. 8.2.b.ix, Estatuto de Roma).

El Estatuto de Roma no establece ninguna disposición referente a los cibercrímenes y la ciberguerra, sin embargo, esa conducta desplegada puede encuadrar en los elementos de los crímenes internacionales básicos, como en el caso de los crímenes de guerra (Khan, 2023). Cuando un conflicto armado se desarrolla en el ciberespacio y desestabiliza mediante ciberataques el funcionamiento de las denominadas infraestructuras críticas, con el fin de impedir la prestación de servicios fundamentales a la población, se estaría frente a lo que se denomina cibercrímenes de guerra, es decir, se refiere aquellos crímenes que se cometen por medios digitales (Pascual, 2023).

Por lo general, muchos ejércitos cuando recurren a este tipo de herramientas digitales y las complementan con operaciones bélicas usuales, realizan lo que se denomina guerras híbridas, es decir, guerras que se mueven en un terreno gris, situado entre la paz y la guerra, entre la legalidad e ilegalidad (Pascual, 2023).

En definitiva, la ciberguerra puede impactar en las personas que hacen vida en el país atacado, ya que la mayoría de los ciberataques se dirigen contra las infraestructuras críticas, como en el caso de los hospitales, sistemas de control para la generación de energía, estaciones de gas, sistemas de comunicaciones, plantas nucleares, entre otros, dicha situación puede traer terribles consecuencias a la población, de allí que si estos ciberataques encuadran como crímenes de guerra, tal como lo establece el Estatuto de Roma, entonces la Corte Penal Internacional (CPI) tiene competencia para investigarlos y juzgarlos.

**Desafíos probatorios y de atribución para la Corte Penal Internacional**

El marco legal se enfrenta a obstáculos tecnológicos y procesales complejos. El ciberespacio, por su naturaleza intangible, transfronterizo y anónimo, dificulta enormemente la individualización del autor material y, más aún, la atribución jurídica a un Estado, un elemento esencial para configurar un crimen de guerra en un conflicto armado internacional. A diferencia de un bombardeo convencional, un ataque digital puede ser enmascarado mediante servidores intermedios, ejecutado por grupos de hackers con vínculos ambiguos con gobiernos, y dejar un rastro digital fragmentado y fácilmente alterable. Esta opacidad permite que ataques que causan sufrimiento humano significativo, como la interrupción de sistemas hospitalarios o de suministro eléctrico, queden en la impunidad por la mera dificultad de probar su origen.

Frente a este escenario, se comparte la visión de que la Corte Penal Internacional no debe ni puede renunciar a su mandato de proteger a las víctimas de los conflictos armados, independientemente del medio empleado. Para superar estos desafíos, resulta indispensable una cooperación multinivel: por un lado, la colaboración estrecha con Estados y empresas tecnológicas que puedan aportar capacidades forenses digitales, inteligencia sobre atribución y acceso a evidencias técnicas. Por otro, se requiere una actualización urgente de las capacidades internas de la CPI en materia de investigación digital, incluyendo la formación de equipos especializados y la adopción de protocolos para la preservación de pruebas digitales. En última instancia, si se aspira a que el Derecho Internacional Humanitario sea una realidad también en el ciberespacio, la comunidad internacional debe dotar a la CPI de las herramientas (técnicas, jurídicas y cooperativas) necesarias para que la justicia no se detenga donde comienza lo digital.

## CONCLUSIÓN

ISSN: 2710-0499 ISSN-L: 2710-0480

Los ciberataques contra infraestructuras críticas (como sistemas de salud, comunicación, energía o transporte) representan una amenaza grave en conflictos contemporáneos, con potencial de causar víctimas civiles y pérdidas económicas considerables. Tanto en la ciberguerra como en la guerra convencional, el objetivo sigue siendo desestabilizar al adversario, aunque los medios digitales permiten operar de manera remota y anónima, dificultando la atribución de responsabilidades.

El Estatuto de Roma, aunque no tipifica expresamente los cibercrímenes, permite interpretar que los ciberataques dirigidos contra infraestructuras civiles esenciales pueden encuadrarse como crímenes de guerra según su artículo 8(2)(b)(ix). Por tanto, la Corte Penal Internacional posee competencia para investigar estos actos, a pesar de los desafíos técnicos y probatorios que plantea el ciberespacio.

La investigación de cibercrímenes de guerra constituye un reto para la CPI debido a la naturaleza intangible y transfronteriza del ciberespacio, que obstaculiza la identificación de autores y la recolección de pruebas. No obstante, la colaboración con empresas tecnológicas y la cooperación internacional pueden facilitar medios técnicos y apoyos necesarios para avanzar en estos procesos.

Por lo tanto, se requiere una actualización normativa del Estatuto de Roma que refleje los desafíos de la era digital, así como un esfuerzo coordinado entre Estados, sector privado y organizaciones internacionales para asegurar que el Derecho Internacional Humanitario se aplique con efectividad también en el ciberespacio.

**Conflicto de intereses / Competing interests:**

La autora declara que no existe ningún conflicto de interés con algún autor o institución.

**Rol de los autores / Authors Roles:**

María Márquez: Conceptualización, metodología, validación, análisis formal, investigación, recursos, escritura – borrador original, visualización.

**Fuentes de financiamiento / Funding:**

La autora declara que no recibió un fondo específico para esta investigación.

**Aspectos éticos / legales; Ethics / legals:**

La autora declara no haber incurrido en aspectos antiéticos, ni haber omitido aspectos legales en la realización de la investigación.

## REFERENCIAS

Adrados, A. (2024). *Ciberguerra 2024: Israel, Irán y Hamás*. Silicon Technology Powering Business. https://www.silicon.es/ciberguerra-2024-israel-iran-y-hamas-2494615

Burkhalter, D. (2022). *¿Cuándo un ciberataque es un crimen de guerra?* SWI swissinfo.ch. https://www.swissinfo.ch/spa/politica/cu%C3%A1ndo-un-ciberataque-es-un-crimen-de-guerra/47567504

Buxton, O. (2023). *Ciberguerra: Tipos, ejemplos y cómo protegerse*. Avast Academy. https://www.avast.com/es-es/c-cyber-warfare

Comité Internacional de la Cruz Roja. (2021). *En el ciberespacio las guerras también tienen límites*. https://www.icrc.org/es/document/en-el-ciberespacio-las-guerras-tambien-tienen-limites

Cruz Roja Americana. (2006). *Los Convenios de Ginebra de 1949 y sus Protocolos adicionales*. https://www.redcross.org/content/dam/redcross/enterprise-assets/cruz-roja/cruz-roja-pdfs/Resumen-de-los-Convenios-de-Ginebra-de-1949-y-sus-Protocolos-Adicionales.pdf

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

IBM. (2025a, 20 de febrero). *¿Qué es un ciberataque?* https://www.ibm.com/es-es/topics/cyber-attack

IBM. (2025b, 15 de marzo). *¿Qué es la ciberseguridad?* https://www.ibm.com/es-es/topics/cybersecurity

Khan, K. (2023, 20 de agosto). *Technology will not exceed our humanity*. Digital Front Lines. https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

Leiva, R. (2018). *Aparece la ciberguerra*. En *La ciberguerra: Sus impactos y desafíos*. Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. https://www.ceeag.cl/wp-content/uploads/2020/06/LA-CIBERGUERRA-SUS-IMPACTOS-Y-DESAFIOS.pdf

Marcelino Aranda, M., Martínez Cuevas, M., & Camacho Vera, A. (2024). Análisis documental: Un proceso de apropiación del conocimiento. *Revista Digital Universitaria, 25*(6), 1–11. https://doi.org/10.22201/ceide.16076079e.2024.25.6.1

Medina, M., Rojas, R., Bustamante, W., Loaiza, R., Martel, C., & Castillo, R. (2023). *Metodología de la investigación: Técnicas e instrumentos de investigación*. Instituto Universitario de Innovación, Ciencia y Tecnología INUDI Perú. https://doi.org/10.35622/inudi.b.080

Organización de los Estados Americanos. (2022). *Segundo informe: El derecho internacional aplicable al ciberespacio*. http://www.oas.org/es/sla/cji/docs/CJI-doc_671-22_rev2_corr1_ESP.pdf

Pascual, M. (2023, 1 de octubre). *La Corte Penal Internacional perseguirá los cibercrímenes de guerra*. *El País*. https://elpais.com/tecnologia/2023-10-01/la-corte-penal-internacional-perseguira-los-cibercrimenes-de-guerra.html

Reyes-Ruiz, L., & Carmona Alvarado, F. (2020). *La investigación documental para la comprensión ontológica del objeto de estudio*. Universidad Simón Bolívar. https://bonga.unisimon.edu.co/server/api/core/bitstreams/2af35a4b-2abf-4f78-a550-0a4e4764e674/content