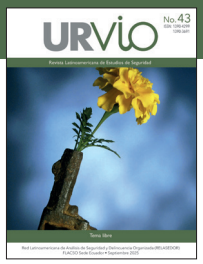
Misceláneos



doi.org/10.17141/urvio.43.2025.6332

URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 43, septiembre-diciembre 2025
pp.70-88 • RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Emblemas digitales en conflictos armados: solución técnica y jurídica para la protección de entidades humanitarias

Digital Emblems in Armed Conflicts: Technical and Legal Solution for Protecting Humanitarian Entities

Jersain-Zadamig Llamas-Covarrubias[1]

Recibido: 8 de agosto de 2024
Aceptado: 30 de enero de 2025
Publicado: 1 de septiembre de 2025

Resumen

Introducción: en un mundo cada vez más digitalizado, los conflictos armados se han extendido al ciberespacio, donde las ciberoperaciones amenazan a entidades protegidas por el derecho internacional humanitario (DIH), como hospitales y organizaciones humanitarias. Este estudio propone un emblema digital como solución técnica y jurídica para identificar y proteger estas entidades en el entorno digital. En este sentido, se analizan los desafíos técnicos, jurídicos y operativos de su implementación. **Objetivo**: el objetivo es evaluar la viabilidad del emblema digital como herramienta de protección en conflictos armados. Se revisan el marco jurídico del DIH, los beneficios y riesgos de implementarlo, y se proponen recomendaciones para su adopción internacional. **Metodología**: se empleó un enfoque analítico-descriptivo basado en revisión documental de tratados internacionales, documentos del CICR y manuales como el *Tallinn Manual 2.0*; se complementó con análisis teórico de conceptos como la *cyber kill chain* y se evaluaron casos prácticos de ciberataques. **Conclusiones**: el estudio concluye que el emblema digital es una solución innovadora para proteger entidades humanitarias, aunque enfrenta desafíos como la exposición de activos y el uso indebido. Se recomienda un marco jurídico internacional específico, tecnologías avanzadas de autenticación y cooperación entre Estados, organizaciones humanitarias y actores tecnológicos para garantizar su efectividad.

Palabras clave: cibernética; conflicto armado; digitalización; emblema; solidaridad internacional

Abstract

Introduction: in an increasingly digitalized world, armed conflicts have extended into cyberspace, where cyber operations threaten entities protected by International Humanitarian Law (IHL), such as hospitals and humanitarian organizations. This study proposes a digital emblem as a technical and legal solution to identify and protect these entities in the digital environment, analyzing the technical, legal, and operational challenges of its implementation. **Objective**: the aim is to evaluate the feasibility of the digital emblem as a protection tool in armed conflicts, analyzing the IHL legal framework, the benefits and risks of its implementation, and proposing recommendations for its international adoption. **Methodology**: an analytical-descriptive approach was used, based on a document review of international treaties, ICRC documents, and manuals such as the Tallinn Manual 2.0, complemented by theoretical analysis of concepts like the Cyber Kill Chain and evaluation of practical cases of cyberattacks. **Conclusions**: the study concludes that the digital emblem is an innovative solution to protect humanitarian entities, although it faces challenges such as asset exposure and misuse. A specific international legal framework, advanced authentication technologies, and cooperation among states, humanitarian organizations, and technological actors are recommended to ensure its effectiveness.

Keywords: armed conflicts; cybernetics; digitization; emblems; international solidarity

1 Universidad de Guadalajara (UdeG), México, jersain.llamas@academicos.udg.mx, orcid.org/0000-0003- 1965-2415.

Introducción

En un mundo cada vez más digitalizado, los conflictos armados se han extendido al ciberespacio, donde las ciberoperaciones se han convertido en una herramienta estratégica para actores estatales y no estatales. Estas operaciones, definidas como acciones realizadas a través de tecnologías de la información y la comunicación para infiltrarse, manipular o interrumpir sistemas informáticos (Gisel y Olejnik 2018), han puesto en riesgo a entidades protegidas por el derecho internacional humanitario (DIH), como hospitales y organizaciones humanitarias (CICR 2019). Este fenómeno evidencia la vulnerabilidad de las infraestructuras en conflictos y plantea desafíos sin precedentes para proteger a la población civil. En este contexto, surge la necesidad de desarrollar mecanismos innovadores, como un emblema digital, para reforzar la protección de estas entidades en el entorno digital.

Este estudio se centra en la propuesta de un emblema digital como solución técnica y jurídica para identificar y proteger a entidades humanitarias en el ciberespacio durante conflictos armados. Inspirado en símbolos tradicionales como la Cruz Roja, el emblema digital busca trasladar su función protectora al ámbito digital, y permitir a los operadores cibernéticos reconocer de inmediato los activos amparados por el DIH (CICR, 2022). Sin embargo, implementarlo implica desafíos técnicos, jurídicos y operativos que deben abordarse para garantizar su eficacia. La pregunta central es: ¿cómo puede un emblema digital contribuir a proteger a entidades humanitarias en el ciberespacio durante conflictos armados, y cuáles son los principales desafíos para implementarlo?

La relevancia de esta investigación radica en su contribución a un campo emergente donde convergen el DIH y la ciberseguridad. Aunque existen estudios sobre la aplicación del DIH en el ciberespacio (Schmitt 2017; Mačák y Rodenhäuser 2023), pocos han explorado soluciones específicas como el emblema digital. Este estudio busca llenar este vacío académico y ofrecer una herramienta práctica para organizaciones humanitarias y Estados, y abordar temas globales como la protección de la población civil y la adaptación del DIH a las nuevas realidades tecnológicas.

Los objetivos del estudio son: (1) analizar el marco jurídico actual del DIH y su aplicabilidad a las ciberoperaciones; (2) evaluar la viabilidad técnica y operativa del emblema digital; (3) identificar beneficios, riesgos y desafíos asociados a su implementación, y (4) proponer recomendaciones para su adopción internacional. Mediante un enfoque interdisciplinario, este estudio contribuye al debate académico y práctico sobre la protección de entidades humanitarias en un entorno digitalizado y conflictivo.

Finalmente, esta investigación es relevante para académicos, profesionales del DIH y la ciberseguridad, organizaciones humanitarias, gobiernos y actores tecnológicos. En un mundo donde los ciberataques contra hospitales y organizaciones humanitarias son cada vez más frecuentes (Tidy 2023), el desarrollo de un emblema digital representa un paso decisivo hacia la protección de la vida y la dignidad humana en el ciberespacio. Al abordar los desafíos técnicos y jurídicos, este estudio aspira a sentar las bases para una herramienta que marque la diferencia en futuros conflictos armados.

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 43 • septiembre-diciembre 2025 • pp.70-88
ISSN 1390-4299 (en línea) y 1390-3691

Marco teórico

El análisis de los emblemas digitales como herramienta de protección en conflictos armados se basa en teorías y conceptos interdisciplinarios que abarcan el DIH, la cibernética, la comunicación simbólica y la ciberseguridad. El DIH, que regula los conflictos armados protegiendo a civiles y limitando los medios y métodos de guerra, es aplicable al ciberespacio a través de principios como la distinción, la proporcionalidad y la precaución (CICR 2019; Mačák y Rodenhäuser 2023). Estos principios exigen que las ciberoperaciones respeten las normas internacionales, incluso si no están explícitamente mencionadas en tratados como los Convenios de Ginebra o el Protocolo Adicional I (1977). Además, el *Tallinn Manual 2.0* (Schmitt 2017) ofrece directrices específicas sobre cómo el DIH se aplica a las ciberoperaciones e incluye la protección de emblemas humanitarios en el entorno digital.

La cibernética aporta el modelo de la *cyber kill chain* (Hutchins, Cloppert y Amin 2011), que describe las fases de un ciberataque, desde el reconocimiento hasta las acciones sobre el objetivo. Este modelo es clave para entender cómo un emblema digital puede disuadir a los atacantes al identificarlos en la fase de reconocimiento e interrumpir así la cadena de ataque. Por otro lado, la comunicación simbólica (Goodrich 2014) explica cómo los emblemas, como la Cruz Roja o la Media Luna Roja, trascienden barreras lingüísticas y culturales para transmitir protección y neutralidad. En el ámbito digital, este enfoque se adapta a través de un diseño que combina elementos visuales y técnicos para garantizar que el emblema sea claramente identificable y comprensible para los operadores cibernéticos.

La ciberseguridad complementa este marco al abordar la protección de infraestructuras, como hospitales y organizaciones humanitarias, frente a ciberataques. El emblema digital se concibe como una herramienta complementaria a las medidas de ciberseguridad, pero implementarlo plantea desafíos técnicos, como la necesidad de autenticación robusta y la integración en sistemas heterogéneos (Linker y Basin 2023). Finalmente, la disuasión y la atribución son conceptos clave para entender cómo el emblema digital puede aumentar el costo percibido de atacar una entidad protegida, ya sea mediante la amenaza de represalias legales o la posibilidad de ser identificado y sancionado (Bodeau y Graubart 2013), obligando al operador a reconsiderar sus acciones debido al alto costo y a la posibilidad de ser perseguido judicialmente por crímenes de guerra (Morello y Vignati 2024). En conjunto, estas teorías y conceptos proporcionan un marco sólido para analizar la viabilidad y el impacto de los emblemas digitales en la protección de entidades humanitarias en el ciberespacio.

Metodología

Este estudio adopta un enfoque analítico-descriptivo basado en revisión documental y análisis teórico para examinar la viabilidad y los desafíos de implementar un emblema digital como herramienta de protección para entidades humanitarias en conflictos armados. La metodología se estructura en tres fases principales: (1) revisión de fuentes primarias y

URVIO, Revista Latinoamericana de Estudios de Seguridad No. 43 • septiembre-diciembre 2025 • pp.70-88
ISSN 1390-4299 (en línea) y 1390-3691

secundarias; (2) análisis conceptual de principios jurídicos y técnicos, y (3) evaluación de casos prácticos y propuestas técnicas.

En la primera fase, se realizó una revisión documental exhaustiva de tratados internacionales, como los Convenios de Ginebra (1949) y el Protocolo Adicional I (1977), así como de documentos clave del Comité Internacional de la Cruz Roja (CICR), incluyendo informes y resoluciones recientes (CICR 2019; CICR 2022). También se consultaron manuales especializados, como el *Tallinn Manual 2.0* (Schmitt 2017) y el *Woomera Manual* (Beard y Stephens 2024), que ofrecen directrices sobre cómo aplicar el DIH en el ciberespacio. Estas fuentes permitieron identificar los principios jurídicos aplicables, como la distinción, la proporcionalidad y la precaución, y su relevancia para las ciberoperaciones.

En la segunda fase, se llevó a cabo un análisis teórico de conceptos clave, como la *cyber kill chain* (Hutchins, Cloppert y Amin 2011), que describe las fases de un ciberataque, y la comunicación simbólica (Goodrich 2014), que explica el papel de los emblemas como herramientas de protección y disuasión. Este análisis permitió evaluar cómo un emblema digital podría integrarse en estrategias de ciberseguridad y cumplir con los principios del DIH. Además, se examinaron propuestas técnicas, como el emblema digital autenticado (ADEM, por su acrónimo en inglés), que utiliza métodos criptográficos para garantizar la autenticidad de la señal (Linker y Basin 2023).

En la tercera fase, se evaluaron casos prácticos y noticias recientes que ilustran la vulnerabilidad de entidades humanitarias frente a ciberataques, como los ataques a hospitales durante conflictos armados o la adopción de códigos de ética por parte de grupos de *hacktivistas* (Tidy 2023; Lyons 2023). Estos ejemplos proporcionaron un contexto real para analizar la efectividad potencial del emblema digital y los riesgos asociados con implementarlo, como la posible exposición de activos protegidos o el uso indebido del emblema por actores maliciosos.

En resumen, la metodología empleada en este estudio combina revisión documental, análisis teórico y evaluación de casos prácticos para abordar de manera integral los aspectos jurídicos, técnicos y operativos del emblema digital. Este enfoque permite garantizar que las conclusiones estén respaldadas por evidencia sólida y un marco conceptual bien definido, para contribuir al debate académico y práctico sobre la protección de entidades humanitarias en el ciberespacio.

Resultados y discusión

Ciberoperaciones y derecho internacional humanitario (DIH)

El notable avance de la digitalización ha traído consigo una proliferación de ciberataques dirigidos contra entidades protegidas por el DIH, como hospitales, centros médicos y organizaciones humanitarias (CICR 2019, 4-5). Este incremento no solo evidencia la vulnerabilidad de infraestructuras en tiempos de conflicto, sino que también plantea desafíos

sin precedentes en la protección de la vida y la integridad de la población, al transformar el ciberespacio en un nuevo campo de batalla.

Las ciberoperaciones son acciones ejecutadas mediante tecnologías de la información y la comunicación, destinadas a infiltrar, manipular, interrumpir o extraer datos de sistemas informáticos (Gisel y Olejnik 2018, 5-8). Estas pueden ser ofensivas, defensivas, de espionaje o híbridas, y ajustarse a las estrategias y tácticas de los actores involucrados (9-10). Su diversidad y complejidad dificultan el análisis y la regulación internacional, ya que cada caso requiere enfoques específicos y adaptados, lo cual obstaculiza crear normativas universales.

Para desentrañar la dinámica de estas operaciones, es necesario recurrir al modelo de la *cyber kill chain*,[2] el cual desglosa el proceso en fases que abarcan desde el reconocimiento y el armamento, hasta la entrega, explotación, instalación, establecimiento de canales de comando y control, y la ejecución final de acciones sobre el objetivo (Hutchins, Cloppert y Amin 2011, 4-5). Aunque estas etapas pueden solaparse o reiterarse según las circunstancias, su estudio permite identificar puntos críticos donde intervenir para prevenir o mitigar daños, y es fundamental para desarrollar estrategias de defensa y respuesta.

A pesar de la alta interconectividad y la complejidad del entorno digital, el ciberespacio no es un espacio sin ley. Por el contrario, se rige por los principios y preceptos del DIH, que exigen limitar el uso de la fuerza y proteger a la población civil (Morello 2024). Entre estos principios se destacan el de humanidad y necesidad, que impone evaluar el costo humano de las operaciones; el de distinción, que obliga a diferenciar entre objetivos militares y civiles, y el de proporcionalidad, que impone que el daño ocasionado no sea excesivo en relación con la ventaja militar obtenida (Mačák y Rodenhäuser 2023). Asimismo, se garantiza la protección de instalaciones médicas y de las operaciones humanitarias, salvaguardando a quienes prestan servicios esenciales en situaciones de conflicto.

El marco jurídico vigente, que incluye los Convenios de Ginebra de 1949, sus Protocolos Adicionales (especialmente el artículo 36 del Protocolo Adicional I de 1977) y el derecho internacional consuetudinario, establece normas aplicables a las ciberoperaciones en conflictos armados, aunque no las mencione explícitamente (CICR 2019, 7-8). El DIH incorpora principios como distinción, proporcionalidad y precaución, y prohíbe capacidades cibernéticas consideradas armas con efectos indiscriminados (CICR 2005, norma 71), ataques contra personas y bienes civiles (Protocolo Adicional I 1977, arts. 48, 51 y 52; CICR 2005, normas 1 y 7), y actos o amenazas destinados a aterrorizar a la población (Protocolo Adicional I 1977, art. 51(2); CICR 2005, norma 2). También se prohíben los ataques indiscriminados

2 *Reconnaissance* (reconocimiento): el adversario recopila información sobre el objetivo, identificando posibles vulnerabilidades. *Weaponization* (armamento): se desarrollan o configuran herramientas o *exploits* personalizados para atacar las vulnerabilidades que se identifican. *Delivery* (entrega): el adversario transmite la carga maliciosa al sistema objetivo, generalmente a través de correos electrónicos, enlaces, o dispositivos comprometidos. *Exploitation* (explotación): una vez entregada, la carga maliciosa explota una vulnerabilidad para ganar acceso al sistema. *Installation* (instalación): se instalan herramientas adicionales, como *backdoors* o *rootkits*, para mantener el acceso persistente. *Command and control* (C2): el adversario establece un canal de comunicación con el sistema comprometido para dirigir sus acciones. *Actions on objectives* (acciones sobre el objetivo): finalmente, el adversario ejecuta sus objetivos, como el robo de datos, destrucción de sistemas o espionaje.

(Protocolo Adicional I 1977, art. 51(4); CICR 2005, normas 11 y 12) y los ataques desproporcionados, que causen daños excesivos en relación con la ventaja militar concreta esperada (Protocolo Adicional I 1977, arts. 51(5)(b) y 57; CICR 2005, norma 14).

Además, existe la obligación de tomar todas las precauciones factibles para proteger a la población y los bienes civiles en operaciones militares, incluyendo las ciberoperaciones (Protocolo Adicional I 1977, art. 57; CICR 2005, normas 15-21). Esto implica prohibir ataques contra bienes esenciales para la supervivencia civil (Protocolo Adicional I 1977, art. 54; Protocolo Adicional II 1977, art. 14; CICR 2005, norma 54) y garantizar la protección de servicios médicos (Convenio I 1949, art. 19; Convenio II 1949, art. 12; Convenio IV 1949, art. 18; CICR 2005, normas 25, 28 y 29). En tiempos de paz, estas medidas incluyen separar redes cibernéticas militares y civiles, desconectar sistemas críticos de internet e identificar infraestructuras con protección especial, como hospitales (Protocolo Adicional I 1977, art. 58; CICR 2005, normas 22-24).

Por otra parte, algunos instrumentos indicativos o de *soft law*, como el *Tallinn Manual 2.0* y el *Woomera Manual*, ofrecen directrices que pudieran ayudar a integrar un emblema digital en el derecho internacional.

El *Tallinn Manual 2.0* establece directrices para proteger emblemas en conflictos armados en el ámbito digital. La Regla 106 prohíbe trampas cibernéticas con emblemas protegidos, personas vulnerables o sitios humanitarios (Schmitt 2017, 457-459). La Regla 124 restringe el uso indebido de emblemas como la Cruz Roja y la Media Luna Roja en el entorno digital (Schmitt 2017, 496-498). La Regla 125 veta el uso no autorizado del emblema de la ONU en ciberoperaciones (Schmitt 2017, 499), y la Regla 126 prohíbe simular autoría enemiga con emblemas ajenos (Schmitt 2017, 499-503). La Regla 127 impide usar emblemas de Estados neutrales en ciberataques (Schmitt 2017, 503-504). Además, la Regla 133 exige identificar claramente unidades médicas con marcadores electrónicos (Schmitt 2017, 515-517), y la Regla 142 protege la propiedad cultural mediante convenciones de archivos y etiquetado de datos (Schmitt 2017, 534-536).

Complementariamente, el *Woomera Manual* aborda aspectos relacionados con emblemas en el contexto espacial, aunque con una aplicación limitada en conflictos armados. La Regla 35 protege unidades médicas y personal religioso, mientras que la Regla 45 prohíbe el uso indebido de marcas nacionales, militares y protectoras, incluido el emblema de la ONU, salvo autorización expresa (Beard y Stephens 2024, 324-328; 384-388).

En paralelo a las formas de regulación antes mencionadas, se ha propuesto un conjunto de ocho reglas para los *hackers civiles* durante la guerra, conocidas también como el *Código de Ginebra de la ciberguerra*, que establecen lo siguiente: (1) no dirigir ataques contra objetivos civiles; (2) evitar usar *malware* de propagación automática que cause daños indiscriminados; (3) planificar las operaciones de modo que se minimicen los efectos colaterales sobre la población; (4) abstenerse de atacar instalaciones médicas y humanitarias; (5) no atacar infraestructuras esenciales para la supervivencia civil; (6) prohibir amenazas cuya finalidad sea atemorizar a la población; (7) no incitar a violar el DIH, y (8) cumplir estas normas, incluso

si el adversario no lo hace (Rodenhäuser y Vignati 2023). Además, se establecen cuatro obligaciones para los Estados orientadas a restringir y controlar la participación de estos actores en conflictos cibernéticos.

Recientemente, varios operadores cibernéticos y *hacktivistas* han adoptado las ocho reglas para *hackers* civiles durante la guerra. Grupos como el IT Army of Ukraine han expresado públicamente su compromiso con estas normas (Tidy 2023), lo cual marca un avance hacia la autorregulación en conflictos armados. Este compromiso refleja una mayor conciencia sobre el respeto al DIH e infiere que los actores cibernéticos pueden responder a señales de protección. Ejemplos similares incluyen grupos de *ransomware* que detuvieron ataques contra organizaciones de salud durante la pandemia de COVID-19 (Abrams 2020) o el grupo LockBit, que ofreció un descifrador gratuito tras atacar el Hospital for Sick Children de Toronto (Lyons 2023).

No obstante, a pesar de los avances en la aplicación de los principios del DIH y la adopción de códigos éticos por operadores cibernéticos, el entorno digital requiere mecanismos de protección específicos y robustos. Es clave desarrollar un emblema digital que sirva como señal inequívoca de protección bajo el DIH. Este emblema no solo identificaría y resguardaría infraestructuras críticas y entidades humanitarias en el ciberespacio, sino que también impulsaría soluciones técnicas y jurídicas para fortalecer su protección frente a los riesgos de las ciberoperaciones en conflictos armados.

Análisis de un emblema digital como herramienta de protección

El concepto de emblema en el DIH está tradicionalmente asociado a símbolos como la Cruz Roja, la Media Luna Roja o el Cristal Rojo, que identifican y protegen entidades médicas y humanitarias durante conflictos armados (CICR 2022, 13). Estos símbolos, regulados a nivel internacional y nacional, señalan que quienes los exhiben gozan de protección especial y están exentos de ataques. Históricamente, los emblemas han sido cruciales para representar y difundir el derecho, combinando imagen, lema y explicación para facilitar la comprensión de normas jurídicas y reforzar su transmisión en la memoria colectiva (Goodrich 2014, 1-22). Al consolidarse el entorno digital como principal medio de comunicación, los emblemas han evolucionado para adaptarse a las nuevas dinámicas digitales, y han redefinido su percepción e interpretación (Manor y Pamment 2024, 54-58).

Sin embargo, la digitalización plantea desafíos para la tradición emblemática, ya que la inmediatez, interactividad y fluidez del ciberespacio cuestionan las nociones convencionales de autoridad, decisión y temporalidad (Tranter 2017, 515-532). Los emblemas digitales representan una evolución de estos símbolos, y generan preguntas sobre su efectividad en el entorno digital y su potencial para revitalizar la comunicación jurídica y humanitaria (Sanz 2011, 385-391). La propuesta de un emblema digital se basa en su función histórica como herramienta pedagógica que vincula lo visual con la normatividad jurídica, y facilitan comprender principios legales (Goodrich 2014, 1-22). En respuesta, la CICR y el movimiento

han propuesto crear un emblema digital, un marcador integrado en activos, servicios y datos cibernéticos que traslade la función protectora de los emblemas físicos al ámbito digital (Morello y Vignati 2024).

El objetivo fundamental del emblema digital es facilitar la identificación de infraestructuras críticas e información sensible perteneciente a entidades humanitarias y médicas, y permitir a los operadores cibernéticos reconocer de manera inmediata que esos activos están amparados por el DIH (Forsythe 2024, 287-290). En medio de la niebla de la guerra digital, esta señalización se proyecta como un complemento a las medidas tradicionales de ciberseguridad, refuerza la protección legal de los sistemas y reduce el riesgo de ciberataques que pueden acarrear elevados costos humanos (CICR 2020, 481-492; CICR 2022, 17).

Diversas propuestas clasifican los emblemas digitales en categorías que incluyen soluciones basadas en archivos, sistemas DNS, direcciones IP y modelos avanzados como el emblema digital autenticado (ADEM), que emplea métodos criptográficos para asegurar su autenticidad (CICR 2022, 27-30; Linker y Basin 2023, 2815-2829). Actualmente, la iniciativa está en fase experimental, con el desarrollo de especificaciones técnicas y pruebas de seguridad, aunque requiere una validación más exhaustiva para su implementación a gran escala (IETF s. f.).

Paralelamente, la resolución del CoD 2022 instó al Comité Internacional de la Cruz Roja (CICR) a investigar la viabilidad técnica del emblema digital y a coordinar esfuerzos con la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (IFRC), las Sociedades Nacionales (SN) y los Estados (Morello y Vignati 2024). En ese marco se planteó desarrollar prototipos; consultar de manera directa con los Estados, y colaborar con el movimiento a través de encuentros regionales y la formación de un grupo informal.

La recomendación final se presentó en la 34ª Conferencia Internacional, con el objetivo de promover la adopción del emblema digital en el DIH, y fue adoptada mediante resolución en octubre de 2024 (Conferencia Internacional de la Cruz Roja y de la Media Luna Roja 2024); orientada a proteger a la población civil y a otros bienes en contextos de conflictos armados, reafirma el valor jurídico y protector de los emblemas y signos distintivos. Esta resolución reconoce las investigaciones llevadas a cabo por el CICR, en colaboración con instituciones académicas y otros actores del movimiento, para definir el propósito, los parámetros y la factibilidad del emblema digital. Además, alienta al CICR a mantener un diálogo activo con los Estados y los componentes del movimiento para evaluar la viabilidad técnica, fortalecer las capacidades de los interesados, y explorar las posibilidades jurídicas y diplomáticas para aplicarlo en conflictos armados.

En este contexto, la resolución de octubre de 2024 representa un avance sustancial, ya que, tras décadas de debates en foros multilaterales sobre desarme, seguridad y temas humanitarios, existe un consenso creciente sobre los riesgos que actividades vinculadas a las TIC, como la interrupción de servicios esenciales y el obstáculo a operaciones humanitarias, representan para la población civil (Gisel y Rodenhäuser 2025). La resolución no solo establece criterios comunes para limitar el costo humano de las ciberoperaciones en conflictos

armados, sino que también sienta bases para futuros acuerdos y medidas que refuercen la protección de civiles en un entorno cada vez más digitalizado.

Lo expuesto hasta aquí indica que el ciberespacio no es un espacio sin ley, y que los conflictos armados en este ámbito también tienen límites. Aunque no está prohibido realizar ciberoperaciones bajo el DIH, es necesario establecer obligaciones que todos deban respetar. La pregunta clave es: ¿cómo se logra esto? La respuesta es mediante un emblema digital, cuyo fin sea la disuasión. A continuación, se explica esta afirmación.

Analizar la *cyber kill chain* resulta esencial para comprender la aplicación práctica de un emblema digital. Durante la fase de reconocimiento, en la que el adversario recopila información sobre posibles objetivos (Hutchins, Cloppert y Amin 2011, 4-5), la presencia de un emblema digital actuaría como una señal temprana que indica que el activo marcado está protegido por el DIH. Esto permitiría romper la cadena de ataque desde sus inicios, obligando al adversario a replantear sus intenciones antes de proceder con las etapas de armado y entrega.

En este contexto, aunque existen diversas actividades para combatir a los ciberoperadores,[3] el emblema digital se concibe como una herramienta disuasoria (Bodeau y Graubart 2013, 7-12). Su presencia advierte al operador cibernético que atacar una infraestructura, entidad o datos protegidos por el DIH constituye un crimen de guerra, lo cual conlleva perseguir a sus responsables. Así, el núcleo del escudo digital no depende solo del buen comportamiento del ciberoperador, sino de disuadirlo, infundiendo temor ante la posibilidad de atribución, represalias o la incertidumbre de lograr los efectos deseados, lo que lo lleva a cesar o suspender sus actividades.

Aunque algunos operadores cibernéticos han adoptado códigos de ética y han evitado atacar entidades protegidas por el DIH, estas medidas voluntarias no aseguran una protección uniforme ni efectiva en el ciberespacio. Por ello, un emblema digital robusto se presenta como una solución sistemática. Su función principal sería redirigir al operador cibernético mediante un efecto disuasorio: al marcar claramente los activos protegidos, el emblema aumenta la percepción del riesgo asociado a su ataque, y obliga al agresor a reconsiderar sus acciones debido al alto costo y la posibilidad de ser perseguido judicialmente por crímenes de guerra (Morello y Vignati 2024).

En conjunto, adoptar un emblema digital representa una evolución lógica y necesaria en la protección de entidades humanitarias en el ciberespacio, pues traslada los beneficios y la tradición de los emblemas físicos al entorno digital. La integración de tecnologías avanzadas, la robusta autenticación y el efecto disuasorio que se logra al redirigir a los operadores cibernéticos constituyen elementos fundamentales para preservar la vida y la integridad en tiempos de conflicto.

3 Redirigir: abarca disuadir (desalentar al adversario), desviar (dirigir esfuerzos hacia objetivos falsos) y engañar (proporcionar información falsa). Evitar: basada en prevenir (tomar medidas anticipadas) y adelantarse (anticipar acciones del adversario). Impedir: comprende degradar (reducir la efectividad del adversario), retrasar (prolongar el ataque) y detectar (identificar actividades maliciosas). Limitar: orientada a contener (restringir actividades), reducir (minimizar el impacto), recuperar (restaurar sistemas) y eliminar (borrar amenazas). Exponer: que incluye analizar (estudiar las tácticas del adversario) y publicitar (dar a conocer vulnerabilidades para aumentar la conciencia).

Beneficios, riesgos y desafíos de implementar un emblema digital

En este apartado se analizan de manera integral los beneficios, riesgos y desafíos asociados a implementar un emblema digital, concebido como una herramienta para identificar y proteger, en el entorno cibernético, los activos, servicios, y datos de actores médicos y humanitarios en situaciones de conflicto armado.

El objetivo principal del emblema digital es señalar claramente que la entidad marcada goza de protección legal bajo el DIH, y complementa las medidas de ciberseguridad existentes sin reemplazarlas. Aunque no es una solución técnica definitiva para todos los desafíos del ciberespacio, desarrollarlo es valioso, ya que podría reducir, aunque sea parcialmente, el daño directo o incidental derivado de ciberoperaciones hostiles. Además, facilitaría que los operadores comprometidos con el DIH identifiquen con precisión los componentes digitales de entidades protegidas, y reduzcan el riesgo de errores y ataques a infraestructuras críticas (CICR 2022, 17-18).

Sin embargo, el aumento de visibilidad que ofrece el emblema digital conlleva riesgos. Entre ellos, se destaca la posible exposición de activos y servicios protegidos, lo que podría facilitar la creación de listas de objetivos fáciles y ataques a gran escala por parte de actores maliciosos desde cualquier lugar del mundo. Además, el emblema podría ser mal utilizado por actores no autorizados para simular protección o encubrir operaciones ofensivas, lo cual socavaría su credibilidad, y expondría a entidades médicas y humanitarias a mayores riesgos. También podría generar una falsa sensación de seguridad y llevar a que se descuiden medidas esenciales de ciberseguridad o a malinterpretar la ausencia del emblema como falta de protección, a pesar de que el DIH garantiza protección independientemente de su uso (CICR 2022, 18-20).

A pesar de los riesgos asociados a implementar el emblema digital, estos pueden reducirse considerablemente con una aplicación rigurosa y protocolos avanzados de ciberseguridad. Un diseño basado en estándares internacionales y tecnologías de código abierto, junto con auditorías y regulaciones estrictas, puede asegurar que la visibilidad del emblema actúe como un elemento disuasorio y facilitador para identificar y proteger activos, en lugar de convertirlos en blancos vulnerables. Además, un marco legal robusto refuerza que el emblema complementa, pero no reemplaza, las medidas esenciales de seguridad, con lo cual evita una falsa sensación de protección. Los riesgos de uso indebido o malinterpretación pueden mitigarse mediante gestión transparente, monitoreo constante y campañas de concientización sobre su correcto uso. Así, el emblema digital se convierte en una herramienta efectiva y confiable para proteger entidades humanitarias y médicas en el ciberespacio, sin comprometer su seguridad ni credibilidad.

En cuanto a los desafíos para operacionalizarlo, se identifican varios aspectos técnicos y jurídicos. En primer lugar, los componentes digitales y el almacenamiento de datos de las entidades protegidas suelen estar interrelacionados con redes o espacios de datos no protegidos, sobre todo en entornos basados en la nube. Por ello, la solución ideal debe ser capaz de marcar

solo los datos y aplicaciones correspondientes a las entidades médicas o humanitarias, sin abarcar servidores o nubes enteras que puedan alojar información de carácter militar u otros datos sensibles. Otro desafío reside en generar confianza y credibilidad en el emblema digital, lo que exige un desarrollo neutral y transparente, posiblemente a partir de tecnología de código abierto, junto con una regulación legal que sancione el uso indebido (CICR 2022, 20-21).

Además, implementarlo implica dificultades, debido a la imposibilidad de modificar los sistemas operativos de ciertos dispositivos médicos por razones técnicas, regulatorias o de seguridad. Esto limita la aplicación directa del emblema, y exige alternativas como señalización a nivel de red, o colaboración con fabricantes y organismos de estandarización para integrarlo. Por último, la solución debe adaptarse no solo a la tecnología actual, sino también a futuras infraestructuras, dada la expansión de dispositivos internet de las cosas (IoT, por sus siglas en inglés) y la transición de IPv4 a IPv6. Asimismo, es importante que el emblema digital esté respaldado por una solución técnica que permita a los operadores programar sus sistemas para evitar dañar activos marcados, y asegurar su valor protector frente a operaciones maliciosas o incidentales (CICR 2022, 21).

Para abordar los desafíos técnicos y jurídicos de implementar el emblema digital, resulta esencial establecer requisitos regulatorios claros y robustos que garanticen su efectividad y credibilidad. En este sentido, instrumentos como el Cybersecurity Act, el Cyber Resilience Act y el Cyber Solidarity Act, de la Unión Europea, ofrecen modelos útiles que, aunque no forman parte del DIH, pueden servir de referencia para desarrollar un marco normativo adaptado al emblema digital.

El Cybersecurity Act (European Parliament and Council 2019) ofrece un sistema de certificación que podría asegurar la integración segura del emblema en entornos compartidos y en la nube, lo que evitaría marcar infraestructuras sensibles no destinadas a protección humanitaria. Por otro lado, el Cyber Resilience Act (European Parliament and Council 2024), al establecer requisitos de ciberseguridad desde la fase de diseño de dispositivos, proporciona un marco para abordar la limitación de sistemas operativos no modificables en dispositivos médicos. Este enfoque podría inspirar estándares que faciliten la señalización a nivel de red, o la colaboración con fabricantes y organismos de estandarización; esto permitiría integrar el emblema sin alterar sistemas operativos existentes. Además, su énfasis en la resiliencia de productos conectados, como los dispositivos IoT, ofrece una base para adaptar el emblema digital a futuras infraestructuras tecnológicas.

Finalmente, el Cyber Solidarity Act (European Parliament and Council 2025), con su enfoque en la cooperación y el intercambio de información, resalta la importancia de mecanismos de supervisión y control para prevenir el uso indebido del escudo digital y fortalecer su credibilidad como herramienta de protección en el ciberespacio. En conjunto, estos instrumentos demuestran que un marco regulatorio uniforme y coordinado es indispensable para complementar la protección que otorga el DIH en el entorno cibernético, y asegura que el emblema digital cumpla su propósito sin comprometer la seguridad ni la integridad de las entidades protegidas.

En síntesis, implementar un emblema digital constituye una herramienta complementaria indispensable para salvaguardar a las entidades humanitarias y médicas en conflictos armados, al posibilitar una identificación precisa y un resguardo efectivo de sus activos en el entorno cibernético. No obstante, su éxito dependerá de una integración sinérgica entre innovaciones tecnológicas, protocolos de ciberseguridad avanzados y un marco jurídico internacional actualizado, capaz de responder a las exigencias de un ciberespacio en constante transformación. Solo mediante un enfoque estratégico que equilibre de manera rigurosa los beneficios potenciales, los riesgos inherentes y los desafíos técnicos y jurídicos, se podrá consolidar el emblema digital como un elemento disuasorio y protector, garantizando su eficacia y credibilidad en un contexto tan dinámico como el actual.

Requisitos operativos, técnicos y legales para desarrollar un emblema digital

En este apartado se analizan de forma integral de los beneficios, riesgos y desafíos asociados a implementar un emblema digital, diseñado como una herramienta para identificar y proteger, en el entorno cibernético, los activos, servicios y datos de actores médicos y humanitarios en situaciones de conflicto armado.

Desde el punto de vista operativo, es necesario que el emblema sea fácil de desplegar, eliminar y mantener a gran escala. Dado que las operaciones en conflictos suelen desarrollarse en condiciones de infraestructura limitada, con recursos escasos y personal con niveles dispares de experiencia en tecnologías de la información, la solución debe ser de bajo costo y no requerir procedimientos complejos. Esta facilidad operativa permite que solo entidades autorizadas, como hospitales y organizaciones humanitarias, puedan usar el emblema de manera eficiente, incluso si su uso previo deja rastros digitales que no comprometen la protección en tiempo real (CICR 2022, 22).

Es fundamental coordinar con organismos especializados, como la Internet Assigned Numbers Authority (IANA) o la Internet Corporation for Assigned Names and Numbers (ICANN), para asignar recursos digitales específicos, junto con programas de difusión y capacitación (CICR 2022, 26). En este contexto, el respaldo de Cybersecurity Tech Accord al Red Cross Digital Emblem Pledge marca un gran avance, al reunir a actores clave de la industria tecnológica para apoyar que se cree y operacionalice el emblema digital. Este compromiso no solo facilita desarrollar soluciones técnicas viables, sino que también promueve estándares globales que garantizan interoperabilidad y eficacia en entornos de conflicto; de esta manera, refuerza la necesidad de mecanismos de bajo costo y fácil implementación, alineados con las demandas operativas de entidades humanitarias y médicas en zonas de guerra (Cybersecurity Tech Accord 2023).

En el ámbito técnico, el emblema debe diseñarse para ser claramente identificable, visible y comprensible por los operadores cibernéticos, quienes deben detectarlo sin esfuerzos adicionales. Es fundamental que se integre naturalmente tanto en el perímetro de las redes (para alertar en la fase de reconocimiento) como en los puntos finales de los sistemas, para

garantizar su eficacia en diversos escenarios de ataque. Además, debe incluir mecanismos automáticos o certificados digitales que permitan verificar su autenticidad sin exponer a los operadores a riesgos, asegurando que la señal de protección sea reconocida universalmente, sin importar el contexto cultural o lingüístico (CICR 2022, 23-24).

Desde el punto de vista legal, es imperativo integrar el emblema digital en el DIH y regularlo mediante instrumentos jurídicos adecuados, de acuerdo con el precedente de los emblemas físicos, cuya forma, función y protección están claramente definidas y respaldadas por el derecho internacional y nacional. Para lograrlo, existen varias vías, como crear un nuevo Protocolo adicional a los Convenios de Ginebra, revisar el Anexo I del Protocolo Adicional I o firmar acuerdos *ad hoc* entre las partes en conflicto. Sin embargo, el éxito del emblema digital dependerá de cómo se integre en los sistemas legales nacionales e internacionales, junto con una amplia difusión de conocimiento y capacitación entre entidades protegidas y operadores cibernéticos, para asegurar que su uso esté regulado, su mal uso sea prevenido y sancionado, y su protección sea respetada en conflictos armados (CICR 2022, 26).

Sobre este último punto, es determinante destacar que el requisito legal es un elemento *sine qua non* del emblema digital. Si no se consagra en instrumentos internacionales y nacionales, carecerá de la fuerza necesaria para ser reconocido y respetado. Si el emblema no está normado, su eficacia disuasoria se verá comprometida, ya que la ausencia de un respaldo jurídico explícito permitiría interpretaciones ambiguas y usos indebidos, lo cual debilitará su capacidad para proteger a entidades humanitarias y médicas en conflictos armados.

Para lograr una disuasión efectiva, no basta con la implementación tecnológica o la resiliencia operativa. Es esencial contar con un marco jurídico robusto que permita identificar, perseguir y sancionar a quienes intenten vulnerar la integridad del emblema digital. Combatir eficazmente las ciberoperaciones hostiles es crucial para la ciberseguridad, ya que la disuasión no se alcanza solo con resistencia pasiva, sino que requiere mecanismos legales que aseguren una respuesta inmediata y coordinada frente a actos subversivos (European Commission 2020, 15; 2025, 11). Solo así se generará un efecto disuasorio real que refuerce tanto la protección como el valor simbólico del emblema digital.

La experiencia en el ciberespacio, especialmente en ciberdiplomacia, ilustra este principio. Por ejemplo, el anuncio de la OTAN en 2014 de que un ciberataque podría invocar el artículo 5, su cláusula de defensa colectiva (NATO 2014), y la decisión en 2016 de designar el ciberespacio como un dominio operativo (NATO 2016) muestran cómo una norma claramente definida fortalece la credibilidad y eficacia de las respuestas disuasorias en un entorno complejo y dinámico (Hiller 2025, 82-84). Aunque el ejemplo de la OTAN tiene un enfoque ofensivo y el emblema digital es defensivo, ambos comparten la necesidad de un marco legal preciso que garantice efectos tangibles y reconocidos.

Un régimen normativo que regule el emblema digital no solo legitima su uso, sino que establece mecanismos esenciales de control: identificación de actores maliciosos, persecución judicial y coordinación de respuestas entre entidades de ciberseguridad, diplomáticos cibernéticos y organismos de justicia. Este enfoque es importante para generar un efecto

disuasorio real en el ciberespacio, donde la cooperación internacional y el intercambio de información son fundamentales para contrarrestar amenazas y responder efectivamente a campañas de desinformación y agresiones híbridas.

En definitiva, es indispensable integrar el emblema digital en un marco jurídico sólido para que este instrumento alcance su máximo potencial en la protección de entidades humanitarias y médicas en conflictos armados. Solo al armonizar normas y aplicar mecanismos legales de control se podrá garantizar que el emblema no solo sea un símbolo de protección, sino también un elemento disuasorio con fuerza real ante quienes intenten vulnerarlo.

Limitaciones e investigaciones futuras

El emblema digital es una herramienta prometedora para proteger activos humanitarios y médicos en conflictos armados, pero, como ya se ha mencionado, también enfrenta desafíos. Su alta visibilidad, clave para la disuasión, también puede convertir a los activos protegidos en objetivos atractivos para actores maliciosos. Además, integrar el emblema digital en infraestructuras tecnológicamente heterogéneas, como dispositivos médicos no modificables o sistemas legados, presenta desafíos técnicos importantes. Por otro lado, usar el emblema también podría generar falsas expectativas de seguridad o facilitar usos indebidos si no se establecen mecanismos robustos de autenticación y validación (CICR 2022, 16).

El marco normativo actual, basado en el DIH, no se ha adaptado plenamente a las dinámicas del ciberespacio. Tecnologías emergentes como la inteligencia artificial (IA) y el IoT complican la atribución de responsabilidades y aumentan el riesgo de daño colateral. Según Pete Renals (2021), la automatización en operaciones cibernéticas, aunque dependiente de decisiones humanas, introduce márgenes de error en contextos de alta presión. Noëlle van der Waag-Cowling (2021) advierte que la militarización del ciberespacio crea un espacio gris donde las normas tradicionales son insuficientes.

La interoperabilidad del emblema digital requiere técnicas avanzadas de autenticación, como métodos criptográficos, que aseguren su integridad sin afectar al rendimiento de los sistemas. Sin embargo, en países con recursos limitados, la falta de capacidades tecnológicas dificulta adoptarlo, lo cual aumenta la vulnerabilidad. Además, los principios del DIH, como la proporcionalidad y la necesidad militar, plantean desafíos prácticos. Incluso si el emblema es respetado, no garantiza protección contra todos los daños, como los colaterales en ataques a objetivos militares cercanos o la vulnerabilidad de infraestructuras esenciales no marcables, como el suministro de agua o electricidad (CICR 2022, 16).

La investigación futura debe enfocarse en perfeccionar el emblema digital y abordar nuevas amenazas, especialmente aquellas que involucran IA, como la manipulación de señales digitales o campañas de desinformación. Es vital desarrollar mecanismos de autenticación avanzados que refuercen la integridad del emblema y mitiguen intentos de falsificación.

La cooperación internacional es esencial para armonizar marcos normativos que aborden el uso indebido de IA en ciberoperaciones y extiendan los principios del DIH a estos nuevos

escenarios. Yasmin Afina y Giacomo Persi Paoli (2024 28) destacan que técnicas como el *watermarking* podrían mejorar la atribución de responsabilidades, mientras que identificar factores disuasorios y adoptar mecanismos de verificación robustos podrían reducir riesgos tanto de actores estatales como no estatales.

En resumen, aunque el emblema digital enfrenta limitaciones técnicas, normativas y operativas, su potencial para proteger entidades humanitarias es considerable. Avances en investigación técnica, empírica y normativa, junto con una mayor cooperación internacional, serán esenciales para que esta herramienta sea efectiva para proteger a la población amparada por el DIH durante conflictos armados.

Conclusiones

En este estudio se ha explorado la viabilidad y los desafíos asociados a implementar un emblema digital como herramienta de protección para entidades humanitarias y médicas en el ciberespacio durante conflictos armados. A través de un análisis interdisciplinario que combina aspectos jurídicos, técnicos y operativos, se ha demostrado que el emblema digital representa una solución innovadora y necesaria para adaptar los principios del DIH a las realidades del entorno digital. Sin embargo, su éxito dependerá de que se superen desafíos y se adopte un enfoque integral que equilibre sus beneficios potenciales con los riesgos inherentes.

En primer lugar, el emblema digital tiene el potencial de fortalecer la protección de entidades humanitarias al facilitar su identificación en el ciberespacio, reduciendo así el riesgo de ataques cibernéticos contra infraestructuras como hospitales y organizaciones de ayuda. Su capacidad para disuadir a los operadores cibernéticos, al señalar que los activos marcados están protegidos por el DIH, lo convierte en una herramienta complementaria a las medidas tradicionales de ciberseguridad. No obstante, su implementación debe ir acompañada de protocolos técnicos robustos, como métodos de cifrado avanzados y sistemas de autenticación, para garantizar su integridad y evitar su uso indebido. En este sentido, se recomienda fomentar la colaboración con la industria tecnológica para desarrollar y estandarizar las tecnologías necesarias, y promover que se creen consorcios internacionales que trabajen en la interoperabilidad y seguridad del emblema.

En segundo lugar, la efectividad del emblema digital depende en gran medida de su integración en el marco jurídico internacional. Es esencial que este mecanismo sea reconocido y regulado a través de instrumentos legales específicos, como un nuevo Protocolo Adicional a los Convenios de Ginebra o acuerdos *ad hoc* entre las partes en conflicto. Este protocolo debería incluir disposiciones claras sobre el diseño, autenticación y sanciones por uso indebido del emblema, otorgándole la misma fuerza legal que los emblemas físicos tradicionales. Además, su adopción debe estar respaldada por un marco normativo que sancione el uso indebido del emblema y garantice que se lo respete en los conflictos armados. La experiencia de instrumentos como el Cybersecurity Act, el Cyber Resilience Act y el Cyber Solidarity Act

de la Unión Europea ofrece modelos útiles para desarrollar un marco regulatorio adaptado a las necesidades del emblema digital.

En tercer lugar, implementar el emblema digital implicar desafíos técnicos y operativos que deben ser abordados de manera sistemática. La interoperabilidad con sistemas heterogéneos, la protección de dispositivos médicos no modificables y la adaptación a futuras infraestructuras tecnológicas, como el IoT, son aspectos críticos que requieren soluciones de vanguardia. Para ello, es crucial coordinar con organismos internacionales como la IANA y la ICANN, así como con actores clave de la industria tecnológica, para garantizar la viabilidad y adopción global del emblema. Asimismo, se recomienda implementar programas de capacitación y concientización dirigidos a operadores cibernéticos, entidades humanitarias y gobiernos, enfocados en la importancia del emblema digital, su correcto uso y las consecuencias legales de su violación.

Finalmente, el emblema digital no debe ser visto como una solución definitiva, sino como un componente más dentro de una estrategia integral de protección en el ciberespacio. Su implementación debe ir acompañada de campañas de concientización, capacitación y cooperación internacional para asegurar que todas las partes involucradas comprendan su propósito y lo respeten. Además, es esencial continuar investigando y desarrollando mecanismos complementarios, como técnicas avanzadas de atribución y verificación, para contrarrestar las amenazas emergentes asociadas a la IA y la automatización de ciberataques. La realización de pruebas piloto en diferentes contextos regionales y la promoción de ejercicios de simulación conjunta permitirían afinar los procedimientos de marcación y respuesta, y asegurarán que el emblema digital sea efectivo en escenarios reales.

En conclusión, el emblema digital representa un notable avance en la protección de entidades humanitarias en el ciberespacio, pero su éxito dependerá de la sinergia entre innovación tecnológica, regulación jurídica y cooperación internacional. Solo a través de un enfoque coordinado y riguroso se podrá garantizar que esta herramienta cumpla su objetivo de proteger la vida y la dignidad humana en los conflictos armados del siglo XXI.

Bibliografía

Abrams, Lawrence. 2020. "Ransomware Gangs to Stop Attacking Health Orgs During Pandemic". *Bleeping Computer*, 18 de marzo. https://bit.ly/4cjZsNs

Afina, Yasmin, y Giacomo Persi Paoli. 2024. *Governance of Artificial Intelligence in the Military Domain: A Multi-stakeholder Perspective on Priority Areas*. UNIDIR - RAISE. https://bit.ly/4kusfEx

Beard, Jack, y Dale Stephens. 2024. *The Woomera Manual on the International Law of Military Space Activities and Operations*. Reino Unido: Oxford University Press.

Bodeau, Deborah, y Richard Graubart. 2013. *Characterizing effects on the cyber adversary: A vocabulary for analysis and assessment*. Bedford: The MITRE Corporation.

CICR. 2005. *Estudio sobre el derecho internacional humanitario consuetudinario*. https://bit.ly/4kBk2yv

CICR. 2019. *Derecho internacional humanitario y ciberoperaciones durante conflictos armados*. Documento de posición del CICR. https://bit.ly/3FA9mzZ

CICR. 2020. "International Humanitarian Law and Cyber Operations During Armed Conflicts: ICRC Position Paper Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security". *International Review of the Red Cross* 102(913): 481-492. https://doi.org/10.1017/S1816383120000478

CICR. 2022. "Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions", https://bit.ly/3AdwstG

Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. 2024. "Protección de la población civil y de otras personas y bienes protegidos ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante conflictos armados". Resolución 34IC/24/R2, aprobada en octubre de 2024. https://bit.ly/4bUFxpP

Convenios de Ginebra de 1949: Convenios de Ginebra. 1949. Convenios de Ginebra para la protección de las víctimas de la guerra. https://bit.ly/3FAxd2D

Cybersecurity Tech Accord. 2023. "Cybersecurity Tech Accord Signs Red Cross Digital Emblem Pledge". https://bit.ly/4kPOLrv

European Commission. 2020. *The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission. https://bit.ly/3FwzMmd

European Commission. 2025. *Cyber Blueprint - Draft Council Recommendation*. COM(2025) 66 final, 2025/0036 (NLE). Brussels: European Commission. https://bit.ly/4kvjjyK

European Parliament and Council. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union L 151 (7 June 2019): 15-69. https://bit.ly/4kVc6In

European Parliament and Council. 2024. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union L 2847 (20 November 2024): 1-2. https://bit.ly/41V0IDx

European Parliament and Council. 2025. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). Official Journal of the European Union L 38 (15 January 2025): 1-3. https://bit.ly/4kWecrm

Forsythe, David P. 2024. *The Contemporary International Committee of the Red Cross: Challenges, Changes, Controversies*. Reino Unido: Cambridge University Press.

Gisel, Laurent, y Lukasz Olejnik. 2018. *The Potential Human Cost of Cyber Operations*. ICRC. https://bit.ly/4iV6ZpI

Gisel, Laurent, y Tilman Rodenhäuser. 2025. "¿Primer paso de otros muchos? Un avance para proteger a las poblaciones civiles contra el uso de tecnologías de la información y las comunicaciones durante conflictos armados". *ICRC Law and Policy Blog*, 11 de marzo. https://bit.ly/4iP5fyi

Goodrich, Peter. 2014. *Legal Emblems and the Art of Law*. Nueva York: Cambridge University Press.

Hiller, Ben. 2025 "From Deterrence to Initiative Persistence in Cyberspace: NATO's Changing Role in Cyber Diplomacy". En *A Handbook for the Practice of Cyber Diplomacy*, editado por Andrea Salvi, Heli Tiirmaa-Klaar y James Andrew Lewis, 82-85. Luxemburgo: Publications Office of the European Union.

Hutchins, Eric, Michael J. Cloppert, y Rohan M. Amin. 2011. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". https://bit.ly/4bUFNVP

IETF. s. f. DIEM Working Group – About. https://datatracker.ietf.org/group/diem/about/

Linker, Felix, y David Basin. 2023. "ADEM: An authentic digital emblem". Ponencia presentada en Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Dinamarca, 21 de noviembre.

Lyons, Jessica. 2023. "LockBit: Sorry about the SickKids ransomware, not sorry about the rest". *The Register*, 4 de enero. https://bit.ly/3SGMQJw

Mačák, Kubo, y Tilman Rodenhäuser. 2023. "Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations". *ICRC Law and Policy Blog*, 7 de marzo. https://bit.ly/41zvkuo

Manor, Ilan, y James Pamment. 2024. "From Micro to Macro Digital Disruptions: A New Prism for Investigating Digital Diplomacy". En *The Oxford Handbook of Digital Diplomacy*, editado por Corneliu Bjola, e Ilan Manor, 45-62. Reino Unido: Oxford University Press.

Morello, Romina. 2024. "Aplicación del DIH en ciberoperaciones". Ponencia presentada en el Cybersecurity Summer Bootcamp 2024, Universidad de León, España, 18 de julio.

Morello, Romina, y Mauro Vignati. 2024. "Digitalizando los Emblemas Cruz Roja / Media Luna Roja / Cristal Rojo". Ponencia presentada en el Cybersecurity Summer Bootcamp 2024, Universidad de León, España, 18 de julio.

NATO. 2014. Wales Summit Declaration. Press Release (2014) 120, 5 de septiembre. https://bit.ly/3XRJHck

NATO. 2016. Warsaw Summit Communiqué. Press Release (2016) 100, 9 de julio. https://bit.ly/4iPS548

Protocolo Adicional I a los Convenios de Ginebra de 1949: Protocolo Adicional I. 1977. Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la

protección de las víctimas de los conflictos armados internacionales. https://bit.ly/4igfV9y

Protocolo Adicional II a los Convenios de Ginebra de 1949: Protocolo Adicional II. 1977. Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados no internacionales. https://bit.ly/4igfV9y

Renals, Pete. 2021. "Future Developments in Military Cyber Operations and Their Impact on the Risk of Civilian Harm". *Palo Alto Networks*. https://bit.ly/3FwwVtn

Rodenhäuser, Tilman, y Mauro Vignati. 2023. "8 Rules for 'Civilian Hackers' During War, and 4 Obligations for States to Restrain Them". *ICRC Law and Policy Blog*, 4 de octubre. https://bit.ly/3DObUtR

Sanz, Álvaro. 2011. "Shifting our vision: reading early modern emblems in the 21st century". *eHumanista: Journal of Iberian Studies* (18): 385-391.

Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Reino Unido: Cambridge University Press.

Tidy, Joe. 2023. "Ukraine Cyber-Conflict: Hacking Gangs Vow to De-Escalate". *BBC News*, 6 de octubre. https://bit.ly/41W7DfO

Tranter, Kieran. 2017. "Law, the digital and time: The legal emblems of Doctor Who". *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique* 30: 515-532.

Van der Waag-Cowling, Noëlle. 2021. *Stepping into the Breach: Military Responses to Global Cyber Insecurity*. Departamento de Estudios Estratégicos, Universidad de Stellenbosch. https://bit.ly/4iae8CM