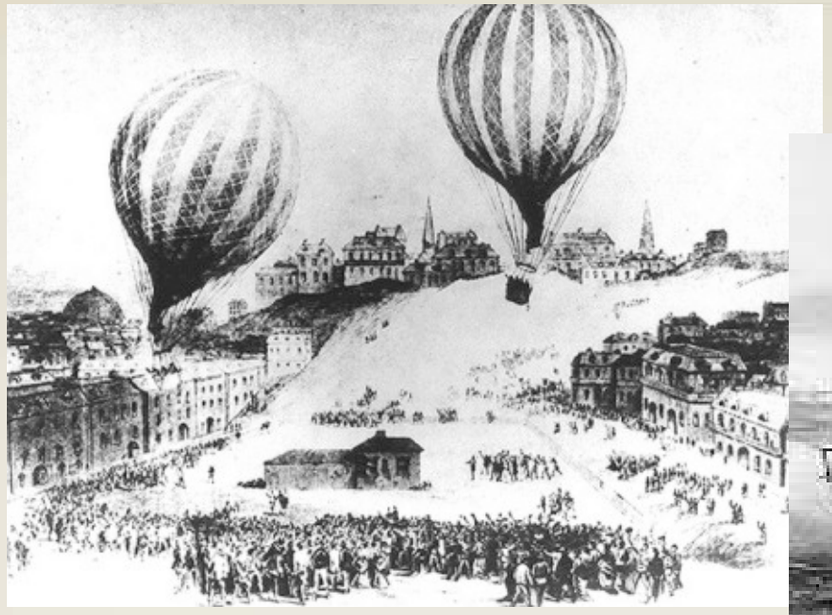
Las armas nuevas. Operaciones en el ciberespacio y ciberguerra. Manual de Tallinn 2.0

Jerónimo Domínguez Bascoy

Armas nuevas

- El derecho de los Estados a elegir los medios y métodos de guerra **no es ilimitado.**
- El Derecho internacional contiene reglas que prohíben o restringen determinados efectos, tipos de armas o medios y métodos de guerra en los conflictos armados.
- Avances tecnológicos: siempre, a lo largo de la historia, utilizados para fines militares, surgiendo en algunos casos debates acerca de su conformidad o no con las reglas vigentes sobre la conducción de las hostilidades.

Armas nuevas



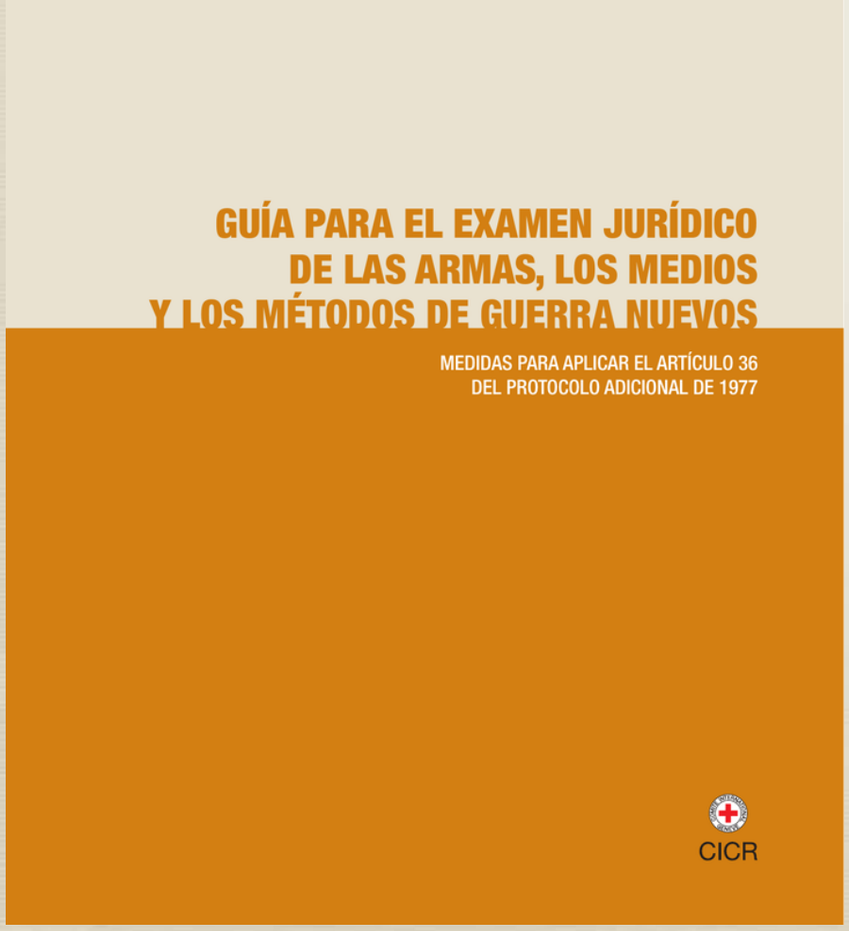
Armas nuevas

ARTÍCULO 36
PROTOCOLO ADICIONAL I

Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante.

Armas nuevas

Guía del CICR para el examen jurídico de las armas, los medios y los métodos de guerra nuevos (enero 2006)



https://www.icrc.org/es/doc/assets/files/other/icrc_003_0902.pdf

Comentarios del CICR al PA I: El artículo 36 implica obligatoriamente el establecimiento de procedimentos internos que permitan dilucidar la licitud de las armas, los medios y los métodos de guerra.

Armas nuevas

Guía del CICR 2006

Armas que deben someterse a examen jurídico

- Las palabras “métodos o medios” incluyen las armas en sentido amplio y la manera de utlizarlas.

- Un arma o un medio de guerra no pueden evaluarse en forma separada del método de guerra con que prevén utilizarse.

- No se exige analizar todas las formas posibles de empleo indebido de un arma, sino solo su uso normal o previsto.

Armas nuevas

Guía del CICR 2006

Prohibiciones o restricciones sobre armas específicas

- Ejemplos: gases axfisiantes (1925); armas bacteriológicas y toxínicas (1972); técnicas de modificación ambiental con fines militares u hostiles (1976); ciertas armas convencionales excesivamente nocivas o de efectos indiscriminados (1980) [con sus Protocolos como, p.e., el de 1995 sobre armas láser cegadoras]; armas químicas (1993); minas antipersonal (1997)

Armas nuevas

Guía del CICR 2006

Prohibiciones o restricciones generales en el DIH

- Armas, medios y métodos que causen males supérfluos o sufrimientos innecesarios.
- Métodos o medios concebidos para causar, o que sea previsible causen, daños extensos, duraderos y graves al medio ambiente.
- Métodos o medios no discriminatorios, esto es, que no puedan dirigirse contra un objetivo militar concreto.
- Métodos o medios cuyos efectos no sea posible limitar, de modo que puedan alcanzar indistintamente a objetivos militares y personas y bienes civiles.
- Ataques por bombardeo que traten como objetivo militar único varios objetivos militares precisos y separados dentro de una población.
- Ataques desproporcionados (excesivo daño incidental).

Armas nuevas

Desafíos que presentan los actuales avances tecnólogicos y científicos

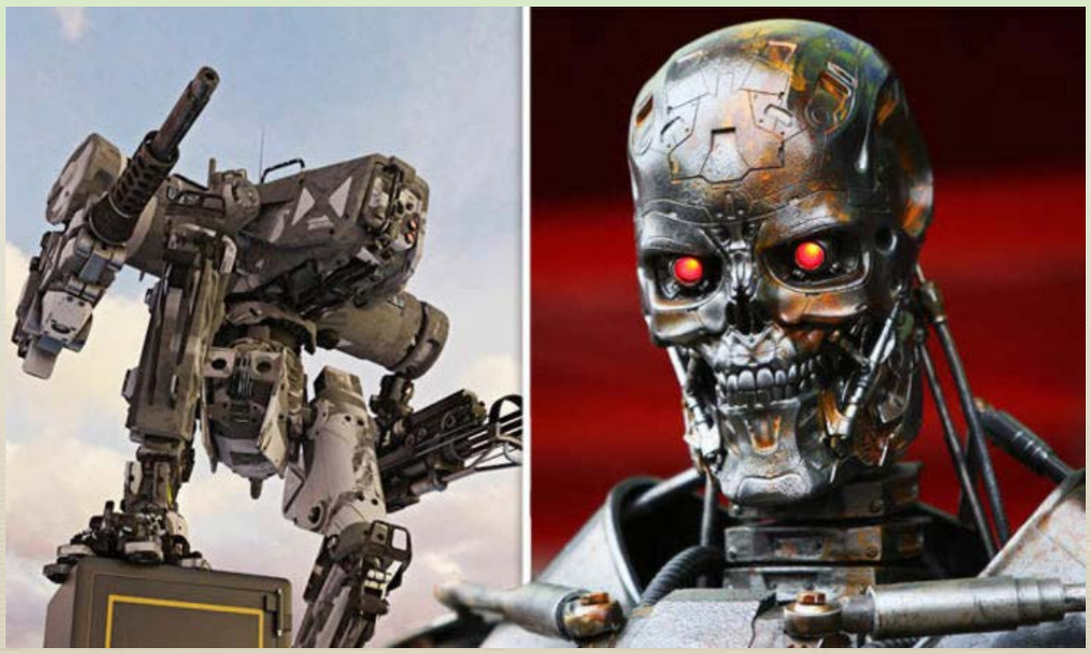
Los avances en la ciencia y en la tecnología pueden traducirse en armas y desarrollos que transformen radicalmente la forma de conducir la guerra. Tales avances someten la revisión del artículo 36 del PA I a retos muy complejos.

Armas nuevas

Sistemas de armas autónomos letales

- "Autonomía": capacidad de una máquina para realizar tareas sin intervención humana, interactuando con el entorno mediante una programación informática (algoritmos de percepción y control).

- LAWS: sistemas de armas que pueden seleccionar, detectar y atacar blancos con escasa o nula intervención del hombre. Pueden ser semiautónomos, autónomos bajo supervisión o completamente autónomos



Armas nuevas

Sistemas de armas autónomos letales

- Revisión conforme al artículo 36 PAI:

- Uso normal: daños supérfluos o sufrimientos innecesarios; dañar indiscriminadamente objetivos legítimos y personas y bienes protegidos; daños al medio ambiente.
- Capacidad de actuar conforme a los principios de distinción, proporcionalidad y precauciones en los ataques.
- Armas capaces de seleccionar y atacar blancos autónomamente: derechos humanos (vida y dignidad); principio de humanidad y dictados conciencia pública; vacío de responsabilidad en caso de violaciones del DIH.

- GEG Convención Armas Convencionales: https://www.unog.ch/80256EE600585943/(httpPages)/5C00FF8E35B6466DC125839B003B62A1?OpenDocument

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

¿Qué es el ciberespacio?

Dominio interactivo formado por redes digitales, que es utilizado para almacenar, modificar y comunicar información, que incluye a internet junto a otros sistemas de información utilizados para el funcionamiento de las infraestructuras, los negovios y otros servicios

(UK Cyber Security Strategy 2011)

Entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos utilizano redes informáticas.

(Tallinn Manual 2.0 2017)

Dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones.

(Estrategia de Ciberseguridad Nacional de España 2013)

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

Ciberoperaciones

Empleo de capacidades cibernéticas para alcanzar objetivos en o a través del ciberespacio

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

Ciberoperaciones

Disponibilidad	Confidencialidad	Integridad
Impedir el acceso o el uso de los sistemas o al información que contienen, sin causar daños personales o materiales. Ataques DoS o DDoS (a través de *botnets*).	Sustraer información del sistema o posibilitar futuras operaciones contra la disponibilidad o integridad del sistema, de los datos o de infraestructuras conectdas. Troyanos/RAT/Backdoor.	Manipular o alterar datos en los sistemas atacados para provocar daños o destrucción en los datos, el sistema u otros sistemas conectados, e incluso muerte o lesiones de personas.
Ataques de DoS sufridos por Estonia en 2007.	US OPM (2014-2015) Sony Pictures Entertainment (2014) DNC Hacks (2016)	Stuxnet 2010 (Irán). Bl. Energy Ucrania (2015-2016) WannaCry/ NotPetya (2017)

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

Harold H. Koh, Legal Adviser, U.S. Department of State, on September 18, 2012, at the USCYBERCOM at Fort Meade, Maryland.

El ciberespacio no es una zona *"law-free"* donde cualquiera pueda realizar actividades hostiles sin reglas o restricciones.

Jeremy Wright, UK Attorney General, on May 23, 2018, at the Chatham House, London.

La cuestión no es si el Derecho internacional se aplica o no en el ciberespacio, sino cómo se aplica.

OTAN: Declaración oficial tras la cumbre de Gales (Sept. 2014)

Nuestra política es reconocer que el Derecho Internacional, incluyendo el DIH y la Carta de las NU, se aplican en el ciberespacio.

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

Informes 2013 y 2015 de los Grupos de Expertos Gubernamentales sobre "Avances en la información y las telecomunicaciones en el contexto de la seguridad internacional"

GENERAL ASSEMBLY

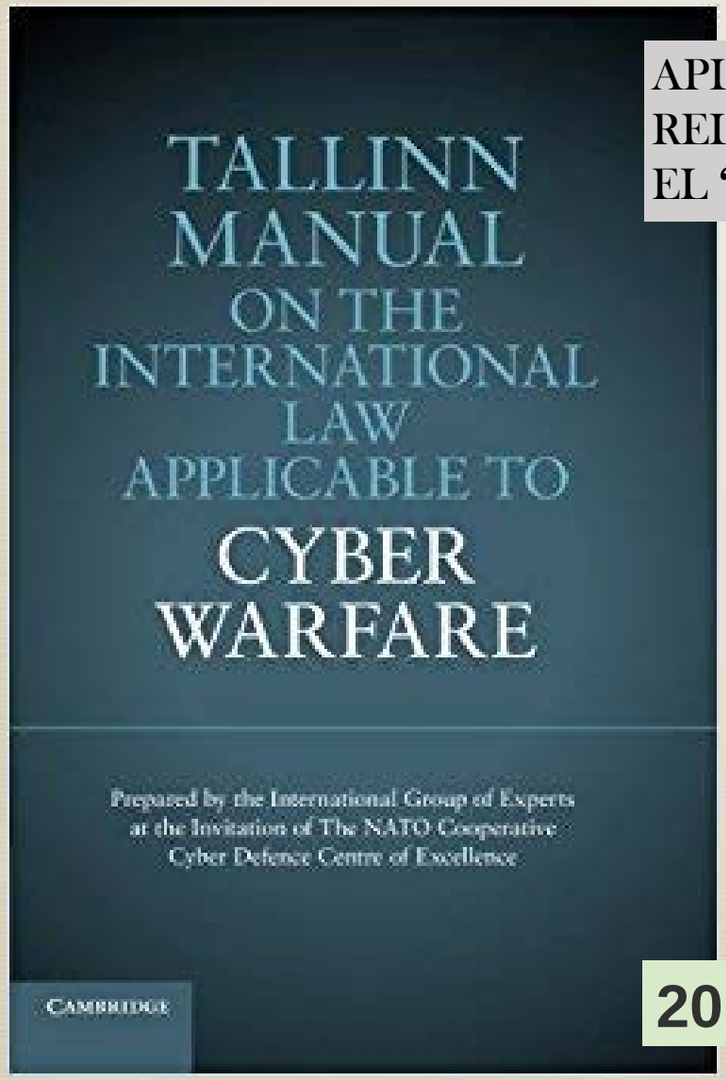
- El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías.

- El derecho internacional se aplica al uso de las TIC por los Estados, existiendo principios jurídicos internacionales establecidos, incluidos, si procede, los principios de humanidad, necesidad, proporcionalidad y distinción.

Armas nuevas

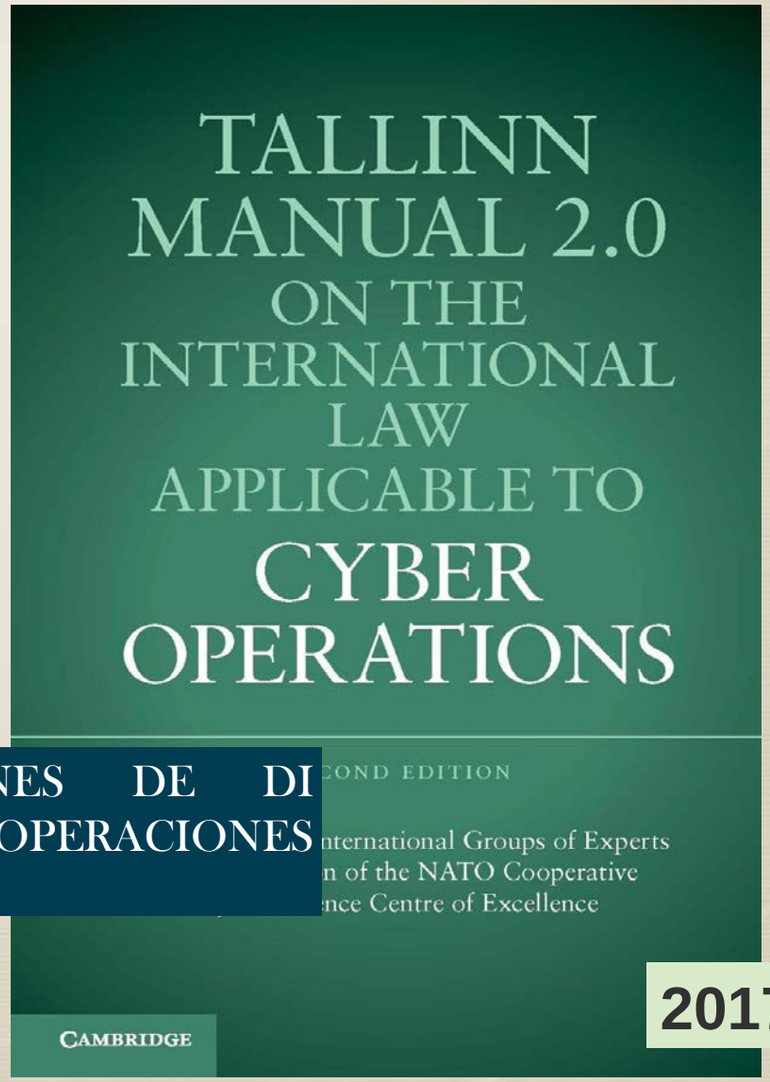
Aplicación del DIH a las operaciones en el ciberespacio

¿CÓMO SE APLICA EL DERECHO INTERNACIONAL EN EL CIBERESPACIO?



APLICACIÓN EN EL CIBERESPACIO DEL DI
RELATIVO A SITUACIONES QUE IMPLICAN
EL **"USO DE LA FUERZA"**

2013



AMPLIACIÓN A LOS REGÍMENES DE DI
APLICABLES A LAS CIBEROPERACIONES
EJECUTADAS EN **TIEMPO DE PAZ**

2017

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

CIBERCONFLICTOS ARMADOS INTERNACIONALES

Hostilidades –que incluyen ciberoperaciones o bien se limitan a éstas– **entre dos o más Estados.**

Control por un Estado de un grupo organizado de hackers que penetran en ciber-infraestructuras de otro Estado causando daños físicos significativos.

Mero **apoyo** a actores estales (p.e., proporcionando herramientas para llevar a cabo ciber-operaciones) no basta para internacionalizar un previo conflicto no internacional. Otra cosa sería que les proporcionara **inteligencia específica** sobre ciber-vulnerabilidades para un ataque concreto.

El carácter **"armado"** del conflicto, ¿cómo se evalúa en el contexto ciberespacial?. ¿Sería suficiente un único ciber-incidente con resultado de daños físicos?. El **STUXNET,** ¿dio lugar a un conflicto armado internacional?

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

CIBERCONFLICTOS ARMADOS NO INTERNACIONALES

Situaciones de **violencia armada prolongada** –que incluya o se limite a ciberoperaciones– **entre fuerzas armadas gubernamentales y grupos armados organizados**, o entre tales grupos. La confrontación debe alcanzar un nivel mínimo de **intensidad** y la parte no estatal en el conflicto debe contar con un grado mínimo de **organización.**

Alcance geográfico del conflicto: ¿El tránsito de datos durante una ciberoperación a través de ciber-infraestructuras situadas fuera del territorio del Estado en el que se desarrolla el CANI no internacionaliza el conflicto?.

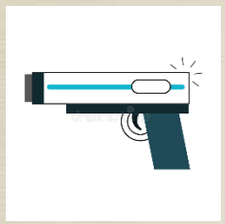
Umbral de **intensidad**: No basta con meras intrusiones, borrado, destrucción o robo de datos, DoS, CNE o "defacement" de webs oficiales. Serían precisos ciberataques altamente destructivos o letales.

Umbral de **organización**: grupos organizados virtualmente. No basta con una actuación colectiva simultanea, sin ninguna coordinación, sino que es precisa una actuación colaborativa.

Armas nuevas

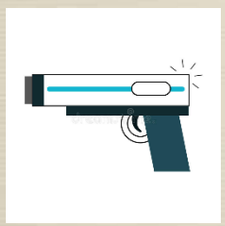
Aplicación del DIH a las operaciones en el ciberespacio

CIBERARMAS



Medios de combate cibernético usados, diseñados o pensados para ser utilizados con la finalidad de herir o causar la muerte a personas o dañar o destruir objetos

Obligación de revisar su **conformidad con el DIH** (art. 36 PA I) en el proceso de estudio, desarrollo, adquisición o adopción.



Ilegalidad de las ciberarmas diseñadas para causar **daños superfluos o sufrimientos innecesarios**. Difícil de imaginar.

Más probable: ilegalidad de ciberarmas **no discriminatorias** o cuyos efectos no pueden ser controlados. Ejemplo: malware concebido para introducirse en redes programado para explotar vulnerabilidades tanto de sistemas civiles como militares, cuando hubiera sido posible limitarlo a estos últimos.

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

CIBEROPERACIONES COMO "ATAQUES"

Reglas sobre conducción de hostilidades formuladas en términos de "ataques"

"Ataque" en el *ius in bello* y "ataque armado" en el *ius ad bellum*. Definición art. 49.1 PA I: actos de violencia contra el adversario. Ciberoperaciones: no hay violencia en el acto en sí, hay que atender a sus efectos.

Ciberoperaciones que hieren, matan, dañan o destruyen = ataques. Debate: ¿La interferencia por medios cibernéticos con la funcionalidad de un objeto (una infraestructura cibernética queda inutilizada o precisa de una importante reparación) puede equipararse a daño o destrucción?.

Ciberoperación contra una ciber-infraestructura que no daña el sistema en sí mismo = ataque cuando es razonablemente previsible que indirectamente causará daños, muerte o destrucción. Ejemplo: Ciberataque contra un sistema SCADA que regula el funcionamiento de una presa.

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

CIBER TARGETING: OBJETIVOS MILITARES

Principio de **distinción:** aplicable a los ciberataques. Obligación de distinguir en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigir las operaciones únicamente contra objetivos militares.

Objetos: los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida (art. 52.2 PA I). Cuestiones principales: dada su intangibilidad, ¿pueden atacarse **datos civiles** sin violar el DIH?; ¿Qué pasa con los bienes de **"doble uso"**?

Personas: pueden atacarse (por medios cinéticos o cibernéticos) combatientes, miembros de grupos armados organizados y civiles que participan directamente en las hostilidades, sean éstas cinéticas o cibernéticas. Requisitos para que un **hacker aislado o múltiples hackers** actuando de forma no colaborativa puedan ser considerados participantes directos: umbral de daño, causalidad directa y nexo de beligerancia.

Armas nuevas

Aplicación del DIH a las operaciones en el ciberespacio

CIBER TARGETING: PROPORCIONALIDAD

Prohibición de los ciberataques cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista.

Supuesto: ciberataque sobre un objetivo militar del que, además, resultarán dañados bienes civiles como ordenadores, redes informáticas o ciber-infraestructuras.

La regla solo juega con respecto a daños físicos, por lo que, p.e., un ataque DoS contra un objetivo militar que interfiriera con servicios de email civiles no se tendría en cuenta en el cálculo.

El daño colateral puede ser tanto directo (provocado inicialmente como efecto del ciberataque) como indirecto (daños a personas u objetos por efecto del ataque contra la ciber-infraestructura de la que dependen). Ejemplo: interferencia con un sistema de comunicaciones dual (militar-civil) en una gran área metropolitana que pudiera perturbar el funcionamiento de los servicios de emergencia.