MARÍA CAMILA MEDINA GARCÍA

LA CIBERGUERRA: UNA NUEVA DIMENSIÓN DEL CONFLICTO. RETOS PARA EL DERECHO INTERNACIONAL HUMANITARIO

(Tesis de Grado)

Bogotá D.C, Colombia

2018

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

TESIS DE GRADO

Rector:	**Dr. Juan Carlos Henao Pérez**
Secretaria General:	**Dra. Martha Hinestrosa Rey**
Directora Departamento Derecho Constitucional:	**Dra. Magdalena Inés Correa Henao**
Director de Tesis:	**Dr. Edgar Solano González**
Presidente de Tesis:	**Dra. Magdalena Inés Correa Henao**
Examinadores:	**Dra. Natalia Castro Niño** **Dr. Bernardo Vela Orbegozo** **T.C David Rodríguez Camacho**

A Elena, mi madre.

AGRADECIMIENTOS

A mi director, Edgar Solano González, por su constante guía, no solo en la elaboración de esta investigación, sino a lo largo de mi paso por el Externado de Colombia, por su confianza en mis ideas y por su amistad.

A la doctora Magdalena Correa Henao, por abrirme las puertas del Departamento de Derecho Constitucional, por apostar a mi formación e incentivar a la búsqueda de nuevo conocimiento.

A los profesores Jorge Roa, Carolina Rico y Carlos López por su apoyo en este proceso.

A Josefa Buitrago de Posada, por sus consejos sabios, y su aliento constante para avanzar con optimismo, paciencia y perseverancia.

A Laura Sofía Medina García, por su amor e incondicionalidad a lo largo de la elaboración de estas páginas: “haz la pinche tesis”.

A mi padre, por enseñarme la importancia de la disciplina, e infundir siempre en mí ganas de aprender.

A Camilo Rodríguez, por su paciencia, cariño y apoyo en estos meses de trabajo, y por leer estas páginas.

A mis amigos, en particular a Carolina Téllez, Angie Sánchez y Marcelo Lozada, por escucharme y animarme en estos meses.

Por último, pero de la manera más sentida y especial, a mi madre. Espero que este trabajo haga algo de honor a tu amor, dedicación e incondicionalidad. Gracias por darme tus mejores años y lo mejor de ti para crecer.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

ABREVIATURAS Y SIGLAS

ASEAN: Asociación de Naciones del Sudeste Asiático.

CCD COE: Cooperative Cyber Defence Centre of Excellence

CIJ: Corte Internacional de Justicia.

DDoS: Denegación de servicios.

DIH: Derecho Internacional Humanitario.

FDI: Fuerzas de Defensa de Israel.

Fig: figura.

HRW: Human Rights Watch.

ICMP: Internet Message Protocol.

IL- CERT: Israel's Computer Emergency Response Team- Equipo de Respuesta a Emergencias Informáticas de Israel.

INCB: Oficina Cibernética Nacional.

MI5: Security Service of United Kingdom.

NISA: Autoridad Nacional de Seguridad de la Información (Israel).

OEA: Organización de Estados Americanos.

ONU: Organización de las Naciones Unidas.

OSCE: Organización para la Seguridad y la Cooperación en Europa.

OTAN: Organización del Tratado del Atlántico Norte

PA I: Protocolo Adicional I a los Convenios de Ginebra de 1997.

PLC: Controladores lógicos programables.

TIC: Tecnologías de la Información y las Telecomunicaciones.

TPY: Tribunal Penal para la Ex Yugoslavia.

UE: Unión Europea.

UIT: Unión Internacional de Telecomunicaciones.

UNIDIR: Instituto de las Naciones Unidas de Investigación sobre el Desarme.

INTRODUCCIÓN

La aparición de nuevas tecnologías dio lugar a la Tercera y Cuarta Revolución Industrial[1]. Los avances que eran quimeras hace algunos años, se tornaron en realidad y hoy en día afectan distintos ámbitos de la vida social, como la estabilidad de la democracia, la paz y la seguridad de los individuos y los Estados, e incluso el goce de derechos como la privacidad[2].

Por ejemplo, en 2011, durante la primavera árabe, el gobierno de Hosni Mubarak bloqueó el acceso a internet a los ciudadanos de Egipto[3]. Asimismo, se he hecho famoso el escándalo de Cambridge Analytica y su influencia en el comportamiento de los electores en la contienda que ganó Donald Trump[4].

Debido a que la guerra y los conflictos no escapan de este cambio de paradigma, es necesario plantear las reflexiones que se han suscitado en el régimen jurídico llamado a regular este tipo de situaciones: el Derecho

[1] SCHWAB, Klaus. El reto de dar forma a la Cuarta Revolución Industrial. En: Project Syndicate [En línea]. Enero 11 de 2016. Disponible en: https://www.project-syndicate.org/commentary/fourth-industrial-revolution-human-development-by-klaus-schwab-2016-01/spanish?barrier=accessreg. Consultado el 20 de abril de 2018; SCHWAB, Klaus .Cuatro principios de liderazgo de la Cuarta Revolución Industrial. World Economic Forum [En línea]. 12 de octubre de 2016. Disponible en: https://www.weforum.org/es/agenda/2016/10/cuatro-principios-de-liderazgo-de-la-cuarta-revolucion-industrial/. Consultado el 19 de abril de 2018.

[2] Al respecto consultar Comisión Interamericana de Derechos Humanos. Estándares para una internet libre, abierta e incluyente. Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II CIDH/RELE/INF.17/17 15 de marzo 2017. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

[3] WILLIAMS, Christopher. How Egypt shut down the internet. The Telegraph [En línea]. Enero 28 de 2011 Disponible en: https://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html. Consultado el 20 de abril de 2018.

[4] ROSENBERG, Matthew, CONFESSORE, Nicholas and CADWALLADR, Carole. How Trump Consultants Exploited the Facebook Data of Millions [En línea]. The New York Times, 17 de marzo de 2018. Disponible en: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Consultado el 25 de abril de 2018.

Internacional Humanitario (en adelante DIH o derecho de los conflictos armados).

En ese orden de ideas, el objetivo de este trabajo no será analizar todas las normas de derecho internacional que se podrían aplicar al ciberespacio, sino que se circunscribirá a la aplicación del DIH a este nuevo entorno, para demostrar que a pesar de su indeterminación y su falta de estudio, no es una zona libre donde se pueden llevar a cabo ataques sin limitaciones.

En particular, se pretende determinar si las normas de DIH existentes son suficientes para responder a nuevos supuestos de hecho, como los ciberataques. Así las cosas, surgen varios escenarios ¿se debe reinterpretar el DIH o además se deben crear nuevo derecho convencional?

Para responder a estos interrogantes, se definirá el ámbito de aplicación de las normas jurídicas en cuestión, es decir el ciberespacio. En este punto también se abordarán sus elementos característicos y algunas de las vicisitudes que lo rodean, para resaltar su naturaleza dinámica y su relación con algunas nociones jurídicas.

A su vez, se realizará una aproximación a la relación que existe entre el ciberespacio y los conflictos. Para esto, se explicarán el contenido de figuras relevantes para la comprensión de la conflictividad cibernética, verbigracia, ciberoperaciones, ciberarmas, ciberataques y ciberhostilidades.

Tras delimitar estos conceptos, se expondrá la relevancia jurídica de los ciberconflictos, y su incidencia en las políticas internas de seguridad y defensa, así como la relación de estas con posiciones de las organizaciones internacionales de carácter regional y universal.

Lo anterior es antesala del eje central de la presente investigación: la creciente relación entre el DIH y el ciberespacio. Para entrar en esta discusión, se presentarán posiciones a favor y en contra de la aplicación de este régimen jurídico a este nuevo entorno, y se analizarán los siguientes puntos:

En primer lugar, se explicará por qué algunas ciberoperaciones se pueden considerar ataques violentos y se determinará cuáles integran esta categoría objeto de análisis del DIH, teniendo en cuenta factores como el tipo de infraestructura sobre el cual recaen los ataques, y las posibles afectaciones que pueden causar a la población civil y sus bienes.

En segundo lugar, se establecerá la relación entre las ciberarmas y el concepto de medios y métodos de guerra, para justificar por qué los avances tecnológicos pueden considerarse armas, y en este sentido, se abordarán posibilidades para la limitación en su uso y alcance.

Debido a que los medios y métodos de guerra deben respetar los principios de distinción, proporcionalidad y precaución, se determinará si estas normas se pueden o no interpretar en el contexto del ciberespacio, y qué particularidades presentan en este entorno.

En la segunda parte de este documento, se hablará de ejemplos concretos de ciberataques. La metodología para trabajar estos casos será una descripción fáctica, que permitirá tener elementos para determinar si las normas que se estudiaron a lo largo del primer capítulo resultan o no aplicables, y hasta qué medida. Esto permitirá ver las diferentes aristas que existen en la aplicación del DIH a casos concretos, así como permite reflexionar sobre soluciones para futuros cibereventos.

A pesar de que existen muchos casos de usos de la tecnología, se escogieron dos, pues el contexto en el que se desarrollan son lo más cercano a un conflicto armado, presupuesto *sine qua non* para la aplicación del DIH: el conflicto Georgia- Rusia del año 2008, y los ciberataques que tuvieron lugar en la central nuclear de Natanz, Irán, en 2010.

Para finalizar este acápite introductorio, es necesario precisar en qué consisten algunos términos que se utilizarán a lo largo de este escrito, con el fin de facilitar su compresión.

Con frecuencia, se hará alusión al Manual de Tallin sobre Derecho Internacional aplicable a la Ciberguerra[5] (en adelante Manual de Tallin). Por esta razón es importante que el lector conozca de antemano la naturaleza de este texto.

El Manual de Tallin es una adaptación de distintas normas de derecho internacional consuetudinario, promovido por el *Cooperative Cyber Defence Centre of Excellence* (CCD COE) de la Organización del Tratado del Atlántico Norte (en adelante OTAN) y publicado por *Cambridge University Press*[6].

Esta interpretación involucró a un Grupo de Expertos Internacionales (que incluyó reputados académicos, profesionales involucrados en la práctica y un equipo técnico), que trabajó durante de 3 años. Este equipo realizó comentarios a cada una de las 95 reglas a través de las cuales se pretende

[5] SCHMITT, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013.
[6] Gobierno de España. Publicación del Manual de Tallín sobre "Ley Internacional en la Ciberguerra". Portal de Tecnología e Innovación del Ministerio de Defensa, 22 de enero de 2013. Disponible en: https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59. Consultado el 18 de abril de 2018.

aplicar el derecho existente a la ciberguerra[7]. Dentro de estas normas, se hace referencia al cuerpo del DIH.

Además de la aclaración sobre el Manual de Tallin, también es menester aclarar algunos términos no jurídicos, debido a la interdisciplinariedad del tema. Por tal razón, se procederá a realizar un pequeño glosario que permita la comprensión de algunos temas relacionados con las tecnologías de la información y las telecomunicaciones (en adelante TIC).

Software: son programas que se utilizan para operar los computadores y los dispositivos relacionados[8].

Malware: es un software malicioso. Se utiliza para robar, encriptar o borrar datos, alterar o hackear funciones básicas de los computadores. También sirve para monitorear la actividad de los usuarios de un computador sin autorización[9].

Virus: es una clase de malware que "inserta parte de su código interno dentro de programas legítimos. De este modo, un usuario podría estar ejecutando un software genuino y a la vez el virus si dicho archivo está infectado."[10]

Proxy: se refiere a "un ordenador que sirve de intermediario entre un navegador web e Internet"[11]. También puede entenderse como una técnica de

---

[7] SCHMITT, Michael N. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed [En línea]. En: Harvard International Law Journal. Vol 54, 2012. Disponible en: http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf. P. 14.

[8] Techtarget. Software. Definition. Disponible en: https://searchmicroservices.techtarget.com/definition/software. Traducción propia.

[9] Techtarget. Malware. Definition. Disponible en: https://searchsecurity.techtarget.com/definition/malware. Traducción propia.

[10] Revista Semana. ¿Qué es un Malware y cómo se puede prevenir?. Disponible en: https://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3. Consultado el 20 de abril de 2018.

[11] CCM. ¿Qué es un proxy?. Disponible en: https://es.ccm.net/faq/2755-que-es-un-proxy

ataque diseñada para suplantar una página web auténtica en sus motores de búsqueda y en las páginas de búsqueda de resultados[12].

Gusano: "código malicioso diseñado para propagarse automáticamente a través de cualquier medio como dispositivos de almacenamiento USB, discos duros, redes corporativas, redes sociales, etc."[13]

Botnet: "grupo de PC infectados y controlados por un atacante de forma remota."[14]

Sin más preámbulo, se invita al lector a analizar nuevos paradigmas que trae la evolución para dar respuestas humanas y justas, haciendo uso de las herramientas que ofrece el derecho.

[12] Techtarget. Proxy hacking. Definition. Disponible en: https://searchmicroservices.techtarget.com/definition/software. Traducción propia.
[13] Revista Semana. ¿Qué es un Malware y cómo se puede prevenir?. Disponible en: https://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3. Consultado el 20 de abril de 2018.
[14] Kapersky lab daily. ¿Qué es un botnet? Disponible en: https://www.kaspersky.es/blog/que-es-un-botnet/755/

CAPÍTULO I. EL CIBERESPACIO

Si bien el ciberespacio es un elemento de naturaleza variable debido al avance de nuevas tecnologías, es importante conocer su naturaleza a través de los elementos que lo componen. Al delimitar este objeto de estudio, será posible hablar de regímenes jurídicos que podrían aplicarse sobre este nuevo entorno de actividades de la humanidad.

1.1 NATURALEZA JURÍDICA DEL CIBERESPACIO

Desde un punto de vista tradicional, los Estados tienen como límite espacial de sus competencias sus territorios, compuestos de cuatro dimensiones: terrestre, marítima, aérea y electromagnética[15]. Estos espacios se pueden delimitar por "un entorno físico, natural o artificial, con dimensiones y fronteras"[16].Sin embargo, el desarrollo de nuevas tecnologías por parte del ser humano ha llevado a hablar de nuevos dominios, como el ciberespacio.

Este término apareció por primera vez a manera de ciencia ficción en 1984, cuando William Gibson lo utilizó en su novela *Nueronmancer* para referirse a un entorno virtual donde se hacía uso de datos[17*], pero poco a poco fue

[15] Cfr. ROBAYO GALVIS, Wilfredo, Elementos del Estado: el territorio. En: CORREA HENAO, Magdalena, RAMÍREZ CLEVES, Gonzalo Andrés y OSUNA PATIÑO, Néstor (editores). Lecciones de Derecho Constitucional: tomo I. Bogotá: Universidad Externado de Colombia, 2017.

[16] LÓPEZ DE TURISO Y SÁNCHEZ, Javier. El ciberespacio como escenario de conflicto. Identificación de amenazas. En: Ministerio de Defensa de España. El ciberespacio. Nuevo escenario de confrontación. Monografías del CESEDEN no. 126, 2012. P. 128.

[17] RABOIN, Bradley. Corresponding evolution: international law and the emergence of cyberwarfare. En: Journal of the National Association of Administrative Law Judiciary, 2011. Vol. 31, 602. P. 607.

[*] Texto original en inglés. Traducción propia.

convirtiéndose en una realidad que preocupa a los individuos, a diversas organizaciones internacionales[18], empresas y a los Estados[19].

Este campo es tan novedoso, que ni siquiera los expertos en nuevas tecnologías logran llegar a un consenso sobre el alcance de este dominio. Por un lado, la Unión Internacional de Telecomunicaciones[20] (en adelante UIT) sostiene que el ciberespacio es "el lugar creado a través de la interconexión de sistemas de ordenador mediante Internet"[21].

Por su parte, el MI5 (*Security Service of United Kingdom*) sostiene que es un conjunto de "medios electrónicos de las redes digitales utilizados para almacenar, modificar y comunicar información. Incluye no solamente Internet, sino también otros sistemas de información que soportan las empresas, infraestructura y servicios"[22]. En el mismo sentido, el Reino de España considera que el ciberespacio es un "dominio global y dinámico compuesto por

[18] Distintas organizaciones regionales, como la OEA y la UE han empezado a mostrar su preocupación en torno a la regulación jurídica del ciberespacio. Sobre el particular, han invitado a sus Estados miembro a regular esta materia en su derecho interno, no solo desde el punto de vista penal o del ciberdelito, sino también a través de mecanismos de ciberseguridad y ciberdefensa. Sobre el particular, consultar:
OEA/Ser.K/XXXVIII CES/dec.1/03 rev. Organización de Estados Americanos. Declaración Sobre Seguridad en Las Américas, 28 octubre 2003. Disponible en: www.oas.org/csh/spanish/documentos/cp12364s04.doc; Comisión Europea. Comunicado de prensa: Estado de la Unión 2017 – Ciberseguridad: la Comisión intensifica la respuesta de la UE a los ciberataques. Bruselas, 2017.

[19] Como se observará en páginas posteriores, varios Estados alrededor del mundo han adoptado políticas de ciberseguridad para asegurar su estabilidad y la de sus ciudadanos en el ciberespacio.

[20] Organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC. https://www.itu.int/es/about/Pages/default.aspx

[21] UIT, Rec UIT- T X. 1205. Sector de Normalización de las Telecomunicaciones de la UIT (04/2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Seguridad en el ciberespacio-ciberseguridad. Aspectos generales de la ciberseguridad, abril de 2008.

[22] MI5. Security Service, United Kingdom. Disponible en: https://www.mi5.gov.uk/cyber. Traducción propia.

las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones"[23]

Este concepto también encuentra recibo en la doctrina, que considera que el ciberespacio es "mucho más que internet, más que los mismos sistemas y equipos, el *hardware* y el *software* […], es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio"[24].

Así pues, se puede concluir que hay dos posturas frente al alcance del ciberespacio. Para efectos de este estudio, se acogerá una posición intermedia, como lo ha hecho, por ejemplo, el Estado colombiano a través de su Comisión de Regulación de Telecomunicaciones[25], según la cual el ciberespacio es un dominio conformado por un vasto conjunto de redes, cuya manifestación más notoria es el internet, sin que sea la única.

Tras llegar a una definición del ciberespacio, interesa resaltar aspectos generales de este nuevo dominio de actividades del ser humano, que escapa de lo convencional y plantea nuevos retos a diversas disciplinas, entre ellas, el derecho. En este orden de ideas, es preciso explicar sus principales características, así como su incidencia directa en categorías jurídicas como el ejercicio de la soberanía, la jurisdicción y la responsabilidad, especialmente en materia de conflictos armados[26].

---

[23] Gobierno de España. Estrategia de ciberseguridad nacional [En línea]. Madrid, 2013 Disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf. Consultada el 16 de marzo de 2018.
[24] FELIU ORTEGA, Luis. La ciberseguridad y la ciberdefensa. En: Monografías del CESEDEN, No. 126. Madrid: Centro Superior de Estudios de la Defensa, 2012. Pp. 42-43.
[25] REPÚBLICA DE COLOMBIA. Comisión de Regulación de Telecomunicaciones. Resolución 2058 de 2009, art. 1.9.
[26] Manual de Tallin. P. 13.

En primer lugar, el ciberespacio es un espacio ***artificial***, contrario a los dominios terrestre, marítimo, aéreo y espacial, en la medida que no surge en la naturaleza, sino que es creado por el hombre[27], lo cual implica que su diseño y posteriores imperfecciones dependen exclusivamente de este[28].

En segundo lugar, es un espacio ***inestable.*** Esta característica tiene una estrecha relación con la primera, puesto que siempre estará sujeto a cambios según los avances de las nuevas tecnologías[29].

En tercer lugar, es un espacio con doble condición: ***virtual*** y ***físico***[30]. Este aspecto encuentra recibo en autores como Gómez de Agreda o Robles, que afirman que el nuevo dominio va desde los ordenadores, hasta "servidores en otros países, cables submarinos o satélites por los que se mueve la información"[31], conectados por cables o de manera inalámbrica[32], lo cual implica una proyección en el mundo no virtual[33].

En este orden de ideas, cabe realizar algunas precisiones sobre el alcance de estas dos características. La parte virtual del ciberespacio es ***ilimitada*** porque trasciende las limitaciones geográficas y físicas[34]. Esto tiene una incidencia

---

[27] ROBLES CARRILLO, Margarita. El ciberespacio: presupuestos jurídicos para su ordenación [En línea]. En: Revista Chilena de Derecho y Ciencia Política. Enero- abril, 2016. Vol. 7, no 1. Disponible en: http://portalrevistas.uct.cl/index.php/RDCP/article/view/1025. P. 17; GÓMEZ DE AGREDA, Ángel. El ciberespacio como escenario de conflicto. Identificación de amenazas. En: El ciberespacio. Nuevo escenario de confrontación, Monografías del CESEDEN no. 126, febrero de 2012, p. 117.

[28] Ibíd. GÓMEZ DE AGREDA, Ángel. El ciberespacio como escenario de conflicto. P. 117.

[29] CHOUCRI, Nazli. Cyberpolitics in international relations. Cambridge: The MIT Press, 2012. P.4.

30 Ibíd.

[31] GÓMEZ DE AGREDA, Ángel. El ciberespacio como escenario de conflicto. Identificación de amenazas. Op. Cit., p. 173.

[32] Ibíd.

[33] ROBLES CARRILLO, Margarita. El ciberespacio: presupuestos jurídicos para su ordenación. Op. Cit., p. 17.

[34] CHOUCRI, Nazli. Op. Cit., p. 4.

directa en materia de fronteras y jurisdicciones[35], pues permite abrir el debate de la categorización del ciberespacio como un espacio común – *global common*- es decir, un espacio que no forma parte de ningún Estado y, en consecuencia, ninguno de ellos puede ejercer soberanía[36].

Por su parte, el componente físico del ciberespacio, es decir, las "comunicaciones, almacenamiento y recursos de computación sobre los que funcionan sistemas de información"[37], se ha denominado ***ciberinfraestructura***. Esto significa que el ciberespacio es una fusión entre zonas del espectro electromagnético y una infraestructura física especial.

Teniendo en cuenta esta naturaleza dual, los Estados estarían obligados a ejercer soberanía sobre las ciberinfraestructuras, así como sobre las actividades que se desarrollen en torno de estas[38], pero ninguno de ellos podría hacer el intento de apropiarse del ciberespacio – entendido como elemento virtual-.

Además de lo anterior, en el ciberespacio también confluyen dos elementos, que implican a los sujetos (o ciberactores) que en él actúan: el ***anonimato*** y

[35] CHOUCRI, Nazli. Op. Cit., p. 4.
[36] KUTT NEBRERA, Alexander. La importancia de dominar los *global commons* en el siglo XXI [En línea]. Documento marco. Instituto Español de Estudios Estratégicos, 2015. Disponible en: http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf. P. 4.
[37] Manual de Tallin, p. 15. States and cyberspace. De acuerdo con *World Economic Forum,* actualmente hay 293 cables submarinos que hacen posible la conexión mundial a internet; a través de los mismos, también pasan llamadas de voz WORLD ECONOMIC FORUM. El fascinante mapa donde puedes ver el recorrido oculto de los cables marinos que nos conectan a internet [En línea]. 17 de mayo de 2017. Disponible en: https://www.weforum.org/es/agenda/2017/05/el-fascinante-mapa-donde-puedes-ver-el-recorrido-oculto-de-los-cables-marinos-que-nos-conectan-a-internet/?utm_content=buffer59801&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer. Consultado el 15 de febrero de 2018.
[38] Manual de Tallin, regla 1. Traducción propia.

la ***neutralidad***[39]. Estos tienen una base técnica y humana, cuya relación intrínseca se explicará a continuación.

Los ciberactores se valen de herramientas técnicas, verbigracia *proxies,* para ocultar su autoría y los métodos de ataque utilizados en la operación que se ejecuta, lo cual, en términos de estrategia, termina por generar una ventaja inicial[40]. Este fenómeno causaría tensiones que podrían derivar en conflictos, pues a través del uso indebido de las tecnologías de la información y las comunicaciones (en adelante TIC) es posible atribuir falsas responsabilidades a otros Estados u organizaciones[41].

Ahora bien, ¿quiénes son los denominados cibersujetos y/o ciberactores? Para efectos de este trabajo son dos: los grupos y los Estados.

Los primeros, consisten en un conjunto de personas que se "agrupan para conseguir de forma colectiva sus objetivos"[42]; en esta categoría caben grupos terroristas[43], grupos de extremismo político, grupos de delincuencia organizada y atacantes de bajo perfil[44], por mencionar algunos ejemplos. Los

---

[39] ROBLES CARRILLO, Margarita. El ciberespacio: presupuestos jurídicos para su ordenación. Op. Cit., p. 17.

[40] LEJARZA ILLARO, Eguskiñe. Ciberguerra, los escenarios de confrontación [En línea]. Documento de opinión. Instituto Español de Estudios Estratégicos, 2014. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO182014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf. P.5.

[41] TORRES SORIANO, Manuel R. El dilema de interpretación del ciberespacio [En línea]. Instituto Español de Estudios Estratégicos. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO03-2018_Dilema_Ciberespacio_ManuelRTorres.pdf. P. 7.

[42] LÓPEZ DE TURISO Y SÁNCHEZ, Javier. Óp. Cit., p. 122.

[43] **Ciberterrorista:** personas que actuarían tanto para financiarse como para fines de propaganda o causar pérdidas en las instituciones e infraestructuras críticas de los países que consideran sus enemigos**; Ciberactivistas:** se tratarían de grupos antisistema, y la finalidad de las acciones sería desacreditar a aquellas instituciones contra las que actúan, con el fin último de modificar su comportamiento; **Ciberejércitos:** con "una capacidad financiera muy superior a los atacantes habituales" así como "una sofisticación máxima". Tomado de: LEJARZA ILLARO, Eguskiñe. Óp. Cit., p. 5 y 16.

[44] CARO BEJARANO, María José. Alcance y ámbito de la seguridad nacional en el ciberespacio. En: JOYANES AGUILAR, Luis. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Madrid: Instituto español de estudios

segundos, son un sujeto clásico de derecho internacional, que importan en la medida que tengan responsabilidad al dirigir acciones que promuevan la defensa de los intereses frente a otros Estados[45].

Los diferentes actores pueden realizar actividades en el ciberespacio con un amplio margen de libertad, pues este dominio está en constante avance y permite desarrollar y aplicar diversas herramientas, que van desde ciberdelitos o cibercrimen[46] como la piratería de software y las transacciones fraudulentas[47], hasta fenómenos más complejos como el ciberterrorismo[48] y la ciberguerra[49].

Tras presentar las vicisitudes del ciberespacio, sus características principales y algunos de los fenómenos que en el acontecen, está claro que es un complejo entorno digital cuyo principal referente es el internet, lo cual no es

---

estratégicos e Instituto Universitario "General Gutiérrez Mellado, 2010. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. P. 72.

[45] Ibíd.

[46] El cibercrimen corresponde a actividades en las que los computadores y los sistemas de información son utilizados como herramienta u objetivo principal. Este concepto incluye delitos "tradicionales" como el fraude o la sustitución de identidad, pasando por la distribución de pornografía infantil o la apología a la xenofobia, hasta ataques sobre sistemas de información. Cfr. EUROPEAN COMMISSION. Joint communication to the European Parliament, the council, the European economic and social committee and the committee of the regions. Cybersecurity Strategy of the European union: an open, safe and secure cyberspace [En línea]. Disponible en: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. P. 3. Consultado el 18 de marzo de 2018. Traducción propia.

[47] REGUERA SÁNCHEZ, Jesús. Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario [En línea]. Grupo de Estudios en Seguridad Internacional, Universidad de Granada. Marzo 18 de 2015. Disponible en: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario. Consultado el 19 de enero de 2018.

[48] Cfr. CANDAU ROMERO, Javier. Estrategias nacionales de ciberseguridad. Ciberterrorismo. En: JOYANES AGUILAR, Luis. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Madrid: Instituto español de estudios estratégicos e Instituto Universitario "General Gutiérrez Mellado, 2010. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf. P. 265- 268.

[49] Entiéndase por ciberguerra "el uso de un código de computadora –unos y ceros– para causar la muerte, lesiones, destrucción o daños durante los conflictos armados". Cfr. COMITÉ INTERNACIONAL DE LA CRUZ ROJA. Colombia: tres expertos discuten los desafíos del DIH. 11 de septiembre de 2015. Disponible en: https://www.icrc.org/es/document/colombia-tres-expertos-discuten-los-desafios-actuales-del-dih. Consultado el 19 de marzo de 2018.

óbice para que no existan o puedan existir sistemas de redes más efectivos y poderosos y que generen más interés a los actores de este entorno, especialmente a los que ya han empezado una pugna por su dominio.

A modo de conclusión, debe tenerse presente la naturaleza volátil del ciberespacio, su asequibilidad a todo tipo de personas u organizaciones, y su constante evolución conforme a los avances de la tecnología al momento de desarrollar normas jurídicas para su regulación.

1.2 CIBERESPACIO, CONFLICTOS Y NORMATIVIDAD

A) Relación del ciberespacio y los conflictos

El ciberespacio ha empezado a reconocerse como el quinto dominio de los conflictos[50]. Las características del ciberespacio permiten que permee con facilidad elementos como el mar, el aire, y la tierra, y asimismo, se convierte en un campo de batalla para distintos actores (estatales o no estatales, como se explicó con anterioridad) [51].

En este nuevo entorno se llevan a cabo actividades que reciben el nombre de ***ciberoperaciones***. En palabras del Manual de Tallin, estas hacen referencia a "el empleo de capacidades con el propósito principal de lograr objetivos a través del uso del ciberespacio"[52]. Este término comprende actividades como

[50] JOYANES AGUILAR, Luis. Introducción. Estado del arte de la ciberseguridad en Ciberseguridad. En: Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Madrid: Instituto español de estudios estratégicos e Instituto Universitario "General Gutiérrez Mellado, 2010. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf.

[51] CARO BEJARANO, María José. Op. Cit., p. 53.

[52] Manual de Tallín, p. 15. Sobre el particular, los expertos que participaron en la elaboración de este manual consideran que los Estados tienen responsabilidad sobre las ciberoperaciones que conduzcan sus organismos internos, o que en su defecto, les sean atribuibles en virtud del derecho de la responsabilidad de los Estados; así pues, se puede atribuir responsabilidad por ciberactividades que realicen terceros o actores no estatales. Dentro de las ciberoperaciones, existe la categoría de ciberataques (Manual de Tallín, regla 20 y 30).

“ataques a redes y sistemas, alteración de datos o software, interrupción de comunicaciones”[53]; hasta ataques de gran magnitud, que incluso comprometerían vidas humanas, como manipulación o destrucción de infraestructura estratégica y crítica, por ejemplo, plantas de electricidad, aeropuertos, entre otros[54].

El juego de poderes entre distintos actores, sean estatales o no estatales, también se manifiesta en el ciberespacio a través de ***ciberconflictos***. Este término se puede entender como “un enfrentamiento de dos o más posiciones (estatales o no estatales) por poder, dinero y control de activos o recursos estratégicos ubicados en el ciberespacio (con unos actores), donde los adversarios son desconocidos e inciertos, así como sus capacidades e intenciones para debilitar o dominar a su contraparte”[55].

Estos elementos representan ventajas militares para los Estados tradicionalmente débiles, pues las tecnologías pueden resultarles más baratas y asequibles, de modo que pueden causar daños a estados superiores

---

[53] CERVELL HORTAL, María José. La legítima defensa en el derecho internacional contemporáneo. Valencia: Tirant lo Blanch, 2017. P. 300.

[54] Ibíd. El contenido del concepto “infraestructura crítica” se ha desarrollado en el derecho interno de países como Colombia y España. Cfr. República de Colombia. Departamento Nacional de Planeación. Política Nacional de Seguridad Digital, documento CONPES 3854 de 2016. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf: Infraestructura crítica cibernética nacional: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

Cfr. Reino de España. Ley 8 de 2011, Art. 1 (d) y (e): **d) Infraestructuras estratégicas:** las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. **e) Infraestructuras críticas:** las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

[55] KELLO, Lucas. The virtual weapon and international order. New Heaven [CT]: Yale University Press, 2017.

militarmente[56]. Lo anterior tiene implicaciones en materia de seguridad, pues se convierte en un atractivo "escenario estratégico, táctico y operativo"[57].

Para llevar a cabo las operaciones en mención, se utilizan ***ciberarmas***, o en otras palabras, códigos dañinos[58]. Durante los últimos años, algunas empresas han creado programas capaces de tener consecuencias tan perversas en el mundo físico, que expertos en materia de ciencia y tecnología han expresado que, en términos de potencial destructivo, "las ciberarmas no son inferiores a las armas nucleares, biológicas o químicas, aunque a diferencia de estas armas de destrucción masiva, las primeras no están sujetas a ningún tipo de control y tienen el 'glamour' de ser invisibles, omnipresentes y precisas"[59].

Las ciberarmas no utilizan fuerza cinética, como las armas tradicionalmente conocidas. Existen sectores que las clasifican como armas defensivas y armas ofensivas. Las primeras están compuestas por "dispositivos de análisis y control de tráfico de red, hardware y software de seguridad, configuraciones correctas, procedimientos, y por la formación y concienciación de técnicos y usuarios"[60], mientras que las armas ofensivas se construyen a través de "la investigación, generación de código, unos conocimientos adecuados y unas tácticas y técnicas especializadas"[61].

---

[56] ROSCINI, Marco. World Wide Fare – Jus ad bellum and the Use of CyberForce. En: Max Planck Yearbook of United Nations Law, 2010. Volume 14. PP. 88-89.
[57] ROBLES CARRILLO, Margarita. El ciberespacio: presupuestos para su ordenación jurídico-internacional. Op. Cit., pp. 17-18
[58] SOLCE, Natasha. The Battlefield Of Cyberspace: The Inevitable New Military Branch—The Cyber Force. En: Albany Law Journal od Science & Technology, 2008. Vol. 18, No. 293. P. 305.
[59] KASPERSKY, Eugene. The Flame That Changed the World [En línea]. 14 de junio de 2012. Disponible en http://eugene.kaspersky.com/2012/06/14/the-flame-that-changed-theworld/#more-2717. Consultado el 3 de febrero de 2018. Traducción propia.
[60] LÓPEZ DE TURISO, Javier. El ciberespacio como escenario de conflicto. Identificación de amenazas. Op. Cit., p. 138.
[61] Ibíd., p. 139.

A través de ciberarmas, se pueden realizar ciberoperaciones que pueden llegar a ser una amenaza para la estabilidad de la paz entre los Estados. Dichas operaciones en forma de ***ciberataques*** pueden alcanzar el carácter de ***ciberhostilidades.*** Las últimas son operaciones militares que se dirigen en el ciberespacio, en las cuales las partes de un conflicto utilizan el flujo de datos con finalidades que pueden ir desde la infiltración de un sistema hasta la manipulación de infraestructuras industriales[62]. Las hostilidades también pueden ser una combinación entre operaciones en las que exista fuerza cinética y cibernética[63].

Fig. 1. Las matryoshkas sirven como ejemplo para entender la relación de estos términos, pues el concepto ciberoperaciones es el más general y contiene a los demás. Imagen tomada de: https://www.vectorstock.com/royalty-free-vector/russian-tradition-matryoshka-dolls-vector-1057195

[62] DOMÍNGUEZ VASCOY, Jerónimo. Aplicación del Derecho Internacional Humanitario a las operaciones en el ciberespacio. En: RODRÍGUEZ-VILLASANTE Y PRIETO, José Luis, LÓPEZ SÁNCHEZ, Joaquín. Derecho Internacional Humanitario. 3 ed. Valencia: Tirant lo Blanch, 2017. P. 624. ISBN: 978-84-9119-871-0.
[63] Manual de Tallin, regla 41.

Para ahondar en esta materia, primero es conveniente traer a colación la acertada distinción que plantea Robles sobre el uso de los ciberataques a través de cuatro categorías: i) uso clandestino del arma cibernética, ii) uso paralelo del ciberataque y el armamento tradicional, iii) uso combinado de ciberataques y armamento tradicional y, por último, iv) ciberataques de carácter autónomo.

En primer lugar, la autora hace referencia al uso clandestino del arma cibernética[64]. En este supuesto, los distintos sujetos o actores utilizan el arma cibernética para atacar a sus objetivos de manera sigilosa, sin dejar huella, con el fin de dar otra apariencia a una provocación o conflicto[65].

En segundo lugar, Robles sostiene que otra opción consiste en el uso paralelo del ciberataque y del armamento tradicional[66]. Esto consiste en el uso del ciberataque de manera concomitante con un conflicto o acción militar en desarrollo; sin embargo esta "no tiene incidencia directa en el teatro de operaciones o dispositivo militar, sino que se concreta en la realización de ciberataques que favorecen a alguna de las partes por el impacto psicológico que conlleva en el desarrollo del conflicto[67].

Como tercera opción está el uso combinado de ciberataques y armamento tradicional[68]. Este evento resulta muy interesante, pues implica todas las formas de lucha desde el punto de vista militar, pues contrario a la opción anterior, en este caso la operación militar integra a sus medios tradicionales

[64] ROBLES CARRILLO, Margarita. El ciberespacio: presupuestos jurídicos para su ordenación. Op. Cit., p. 37.
[65] Ibíd.
[66] Ibíd., p. 38.
[67] Ibíd.
[68] Ibíd., p. 39.

acciones ciberespaciales que coadyuvan a su éxito, varían el riesgo y aumentan la efectividad[69].

Por último, los ciberataques también pueden alcanzar un carácter autónomo o alternativo a las operaciones militares clásicas[70]. Esta opción abre un abanico de preguntas frente a los corolarios clásicos, los medios y métodos de guerra, y el uso de la fuerza en el derecho internacional, pues justo aquí es donde se cambia completamente la acción armada al incorporar las nuevas tecnologías como único medio de ataque. Piénsese, por ejemplo, en la combinación de recursos cibernéticos y nucleares que podrían implicar una ventaja sobre el oponente al privarlo del "control sobre sus mecanismos de represalia"[71].

Estos escenarios de ciberoperaciones dan cuenta del nuevo panorama al que se enfrentan los Estados del mundo. Según el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNDIR), más de 100 países de distintos continentes han mostrado su preocupación por asuntos de ciberseguridad, así como por fortalecer sus mecanismos de ciberdefensa[72].

Incluso, algunos de estos Estados, por ejemplo, España[73], Estonia[74] y Colombia[75], han creado unidades en el seno de sus Fuerzas Armadas con el

---

[69] Ibíd., p. 40.
[70] Ibíd., p. 41.
[71] Cfr TORRES SORIANO, Manuel R. El dilema de interpretación del ciberespacio. Op. Cit., p. 10.
[72] Cfr. LEWIS, James A., TIMLIN, Katrina. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. Center for Strategic and International Studies. UNDIR Resources, 2011. Disponible en: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf, p. 3. El estudio menciona las estrategias que se adoptaron en países como Albania, Australia, Argentina, Colombia, Brasil, Corea del Sur, entre otros.
[73] Cfr. Gobierno de España. Estrategia de Ciberseguridad Nacional, 2013. Disponible en: www.dsn.gob.es/es/file/146/download?token=Kl839vHG
[74] Cfr. Ministry of Economic Affairs and Communication, Estonia. Cyber Security Strategy 2014-2017, 2014. Disponible en: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.
[75] Cfr. Comando General de las Fuerzas Militares de Colombia. Plan Estratégico Militar -PEM-2030., 2015. Disponible en: https://cdn.fac.mil.co/sites/default/files/plan_estrategico_mil

fin de hacer frente a los posibles ataques que se den en el ciberespacio, como puede observarse en las estructuras que se presentan a continuación:

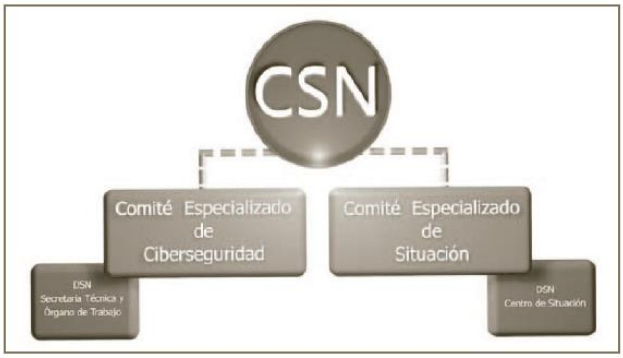

Fig. 2. Estructura del sistema de ciberseguridad español. Tomado de la Estrategia de Ciberseguridad Nacional, España, 2013. Disponible en: www.dsn.gob.es/es/file/146/download?token=Kl839vHG

Fig. 3. Estructura del sistema de ciberseguridad de Estonia. Tomado de: KASKA, Kadri, OSULA, Anna-Maria, STINISSEN, LTC Jan. The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013. P. 10.

itar_2030.pdf, p. 24. Las FF.MM colombianas consideran que un buen dominio del ciberespacio les permite mantener ventaja estratégica frente a las amenazas.

Fig. 4. Propuesta de Comisión Intersectorial para la ciberseguridad y la ciberdefensa. Tomada de: República de Colombia. Departamento Nacional de Planeación. Documento CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa, 14 de julio de 2011. P. 21. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Un aspecto interesante de las políticas estudiadas es que no solo involucran al sector defensa en su implementación, sino que además integran a otras entidades de los gobiernos como los ministerios de relaciones exteriores y los de telecomunicaciones o tecnologías para abordar la problemática del ciberespacio.

Por otra parte, los Estados manifiestan su preocupación no solo en su ámbito interno, sino que además han llevado el asunto a organizaciones regionales de las cuales son parte.

Por ejemplo, en 2003, la Organización de Estados Americanos (en adelante OEA) celebró la Conferencia Especial sobre Seguridad, en Ciudad de México.

En esta ocasión puso de presente que la seguridad de la región se ve afectada por distintas amenazas, entre las que destaca los ataques a la seguridad cibernética[76]. En este sentido, los Estados miembro consideraron importante adoptar una cultura cibernética en la región, con el fin de "prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas"[77].

Asimismo, en 2013, la Comisión Europea publicó una estrategia de ciberseguridad para la Unión Europea (o UE)[78]. Dentro de los objetivos estratégicos, la organización trazó como metas mejorar la resiliencia cibernética[79], reducir el cibercrimen[80], desarrollar una política de ciberdefensa y capacidades que correspondan a una Política Común de Defensa[81], desarrollar recursos tecnológicos e industriales para la ciberdefensa[82] y establecer una política internacional para el ciberespacio[83].

Tal vez este último punto es el más interesante, pues habla sobre la sinergia entre los ámbitos civil y militar para la protección de infraestructuras críticas, e incluso habla de un trabajo conjunto entre la UE y la OTAN para mejorar la ciberdefensa. Además, la UE sostuvo que buscaría cooperación con la ONU, la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Asociación de Naciones del Sudeste Asiático (ASEAN) y con la OEA[84]. Tal

[76] OEA, Declaración de México. Óp. Cit., párr. 4.
[77] OEA, Declaración de México. Óp. Cit., párr. 26.
[78] Cfr. EUROPEAN COMMISSION. Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace. Op. Cit.
[79] Ibíd., p. 4.
[80] Ibíd., p. 4.
[81] Ibíd., p. 5
[82] Ibíd., p. 5.
[83] Ibid, p. 5.
[84] EUROPEAN COMMISSION. Op. Cit. p. 15.

como sucede en el caso americano, la UE hace un llamado a sus Estados para que adopten políticas de ciberseguridad en su derecho interno[85].

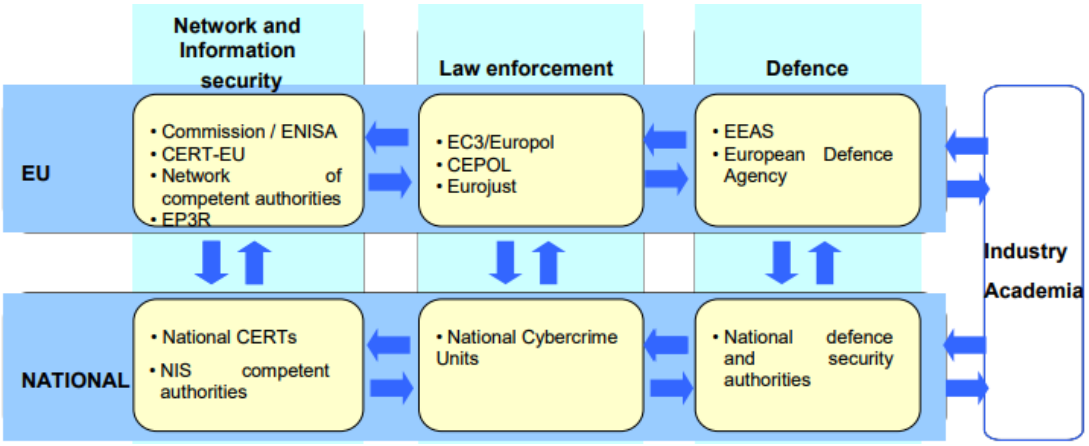

Fig. 5. Distribución de competencias entre la UE y los Estados miembro. Tomada de EUROPEAN COMMISSION. Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace. Joint communication to the European Parliament, the council, the European economic and social committee and the committee of the regions. Disponible en: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

Conforme a estos ejemplos, no está en discusión que los Estados del mundo deben hacer esfuerzos individuales y colectivos para mejorar sus índices de ciberseguridad y ciberdefensa, en el que involucren un tratamiento interdisciplinar que aborde conocimientos científicos y sociales, como el derecho. En este orden de ideas, resulta interesante la propuesta de Modelo de Madurez de la Capacidad Cibernética propuesto por la Universidad de Oxford y aplicado en estudios del Banco Interamericano de Desarrollo[86] .

Dicho modelo integra las siguientes variables para evaluar los avances de los países en materia de ciberseguridad y ciberdefensa: (i) Políticas y estrategia

[85] EUROPEAN COMMISSION. Op. Cit., p. 7.
[86] Cfr. ANDREW LEWIS, James. Estrategias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos. Banco Interamericano de Desarrollo, 2016; GLOBAL CYBER SECURITY CAPACITY CENTRE. Cybersecurity Capacity Maturirty Model for Nations (CMM). University of Oxford, 2016. Disponible en: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

nacional de seguridad cibernética; (ii) Cultura cibernética y sociedad; (iii) Educación, formación y competencias en seguridad cibernética; (iv) Marco jurídico y reglamentario, y (v) Normas, organizaciones y tecnologías.

Todo lo anterior demuestra que los Estados se están preparando para eventuales situaciones de conflicto a través del diseño de políticas como las observadas. Por ende, es necesario analizar las discusiones sobre la aplicación del DIH en este contexto.

B) Ciberguerra y Derecho Internacional Humanitario: reinterpretación de normas jurídicas para un nuevo dominio

Conforme a los ejemplos estudiados, los Estados se están preparando para poder actuar en el ciberespacio. Por tal razón, la Asamblea General de la ONU ha expresado su preocupación sobre el correcto uso del ciberespacio desde 1997[87]. Este organismo internacional sostiene que el uso de nuevas tecnologías tiene incidencia directa en la paz y la seguridad mundial[88], puesto que las nuevas tecnologías se pueden poner al servicio de fines que son incompatibles con la estabilidad y la seguridad internacionales, de modo que pueden generar un efecto negativo en ámbitos civiles y militares[89].

Las alarmas se encienden aún más cuando ya se tiene noticia de ataques que causan un potencial daño a la población civil – aunque aún no alcanzan un nivel de lesiones, daños o pérdidas de vidas humanas- y abren la puerta a nuevos escenarios para hacer la guerra.

---

[87] Cfr. Asamblea General de Naciones Unidas. Función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme. 23 de diciembre de 1997. A/RES/52/33.
[88] Cfr. Ibíd.; Asamblea General de Naciones Unidas. Función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme. 4 de enero de 1999. A/RES/53/73.
[89] Verbigracia, Asamblea General de Naciones Unidas. Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. 20 de noviembre de 2000. A/RES/55/28.

Por ejemplo, en 2007 la República Estonia sufrió ciberataques -presuntamente provenientes de Rusia -. La causa de estos hechos se atribuye al traslado de un monumento a los soldados soviéticos que cayeron en la Segunda Guerra Mundial ubicado en el centro de Tallin- capital de Estonia- hacia un cementerio militar con poca visibilidad[90].

Los ciberataques conllevaron a la inutilización temporal de infraestructuras críticas y la paralización de sectores de la administración estatal, del sistema bancario, de la policía y de medios de comunicación[91].

Estos bloqueos son particularmente graves para la población estonia, pues existe un gran desarrollo en materia de gobierno cibernético; verbigracia, los ciudadanos cuentan con una tarjeta de identificación electrónica que les permite acceder a múltiples servicios como el sistema de voto por internet, la realización de declaraciones de impuestos por vía electrónica, historiales médicos en línea, entre otros[92].

Otro referente importante, y tal vez el más interesante para la posible aplicación del DIH es el ataque que sufrió la República Islámica de Irán en 2010, cuando terceros lograron atacar el sistema que controla la infraestructura del programa de enriquecimiento nuclear– que a todas luces es una infraestructura estratégica-, mediante un virus llamado *Stuxnet*. Las consecuencias fueron dramáticas para el Estado iraní, pues los perpetradores lograron la destrucción de mil centrifugadoras de uranio[93].

---

[90] REGUERA SÁNCHEZ, Jesús. Op. Cit., p. 6.
[91] GUTIÉRREZ ESPADA, Cesáreo. La ciberguerra y el derecho internacional. En: MARTÍNEZ PÉREZ, Enrique. Las amenazas a la seguridad internacional hoy. Valencia: Tirant lo Blanch, 2017, p. 210. Estos hechos se atribuyen al traslado de un monumento a los soldados soviéticos que cayeron en la Segunda Guerra Mundial ubicado en el centro de Tallín- capital de Estonia- hacia un cementerio militar con poca visibilidad. Sobre el último hecho, consultar: REGUERA SÁNCHEZ, Jesús. Óp. Cit., p. 6.
[92] ANDREW LEWIS, James. Op. Cit., pp. 13-14.
[93] Cfr. GUTIÉRREZ ESPADA, Cesáreo. Óp. Cit., p. 211.

A partir de lo anterior se puede establecer una relación directa entre las nuevas tecnologías y el desarrollo de los conflictos. Así pues, las primeras deben tener unos límites de aplicación[94], señalados por reglas[95].

En este orden de ideas, es válido decir que la paz es una excepción en el desarrollo de la humanidad. Por tal razón, desde el derecho internacional se habla del *ius in bello*[96]*,* que no es más que admitir la existencia de conflictos armados con limitaciones que buscan en todo momento la protección del ser humano. Así las cosas, los Estados llegaron a consensos frente a usos y costumbres de guerra, que se materializaron en cuerpos normativos que hoy conocemos como Derecho Internacional Humanitario[97].

Desde una perspectiva clásica, existen tres grandes ramas que conforman esta disciplina del derecho internacional público: i) el Derecho de La Haya, que busca proteger a combatientes y no combatientes en los conflictos a través de la limitación de los medios y métodos de combate[98]; ii) el Derecho de Ginebra, que tiene por objeto dar protección a las víctimas no combatientes de conflictos

[94] VAN CREVELD, Martin. From 2000 BC to the present, revised ed., The Free Press, New York, 1991. PP. 1-3. En: LIIVOJA, Rain. Technological change and the evolution of the law of war. En: International Review of the Red Cross, 2015. No. 900. Disponible en: https://www.icrc.org/es/international-review/article/los-cambios-tecnologicos-y-la-evolucion-del-derecho-de-la-guerra, p. 1169.

[95] International Committee of the Red Cross. Cyber warfare and international humanitarian law: The ICRC's position. Disponible en: https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf, p. 1.

[96] Cfr. PÉREZ GONZÁLEZ, Manuel. El derecho internacional humanitario frente a la violencia bélica. En: RODRÍGUEZ-VILLASANTE Y PRIETO, José Luis, LÓPEZ SÁNCHEZ, Joaquín. Derecho Internacional Humanitario. 3 ed. Valencia: Tirant lo Blanch, 2017. ISBN: 978-84-9119-871-0. P. 31; VELA ORBEGOZO, Bernardo. Lecciones de derecho internacional. Tomo I. Bogotá: Universidad Externado de Colombia, 2012. pp. 47- 75.

[97] RODRÍGUEZ- VILLASANTE Y PRIETO, José Luis. Fuentes del Derecho Internacional Humanitario. En: RODRÍGUEZ-VILLASANTE Y PRIETO, José Luis, LÓPEZ SÁNCHEZ, Joaquín. Derecho Internacional Humanitario. 3 ed. Valencia: Tirant lo Blanch, 2017. ISBN: 978-84-9119-871-0. P. 60.

[98] SALMÓN, Elizabeth. Introducción al Derecho Internacional Humanitario. Lima: Pontificia Universidad Católica del Perú y Comité Internacional de la Cruz Roja. 3a ed., 2014. P. 69.

armados[99] y, por último, se encuentra iii) el Derecho de Nueva York –desarrollado por la ONU- , que consiste en propuestas de mecanismos de sanción en caso de incumplimiento del DIH[100].

No obstante, hay todo un debate doctrinal sobre la aplicación del DIH al ciberespacio. Por un lado, hay quienes no consideran viable aplicar el DIH a los ciberconflictos porque en teoría estas reglas solo aplican a conflictos armados, y toda vez que no hay fuerza cinética, se perdería el carácter armado del conflicto[101].

Por otra parte, existen Estados y organizaciones internacionales que abogan por la aplicación del DIH al ciberespacio. Verbigracia, Australia[102] y el Reino Unido[103].

En lo que respecta a organizaciones internacionales, la Unión Europea reconoce que el DIH es aplicable en caso de que haya lugar a un conflicto

---

[99] Ibíd. p. 68; Cfr. BUGNION, François. Derecho de Ginebra y Derecho de La Haya. Revista Internacional del Comité de la Cruz Roja, 2001. Disponible en: https://www.icrc.org/spa/resources/documents/misc/5tdqeh.htm. Esta rama comprende el Convenio de Ginebra del 22 de agosto de 1864 para el mejoramiento de la suerte de los militares heridos en los ejércitos en campaña, que a su vez se revisó en 1906, 1929 y 1949, así como los cuatro Convenios de Ginebra de 1949 a saber: Convenio De Ginebra del 12 de agosto de 1949 para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, Convenio de Ginebra del 12 de Agosto de 1949 para Aliviar la Suerte que Corren los Heridos, los Enfermos y los Náufragos de las Fuerzas Armadas en el Mar, Convenio de Ginebra del 12 de Agosto de 1949 relativo al trato debido a los prisioneros de guerra, Convenio de Ginebra del 12 de agosto de 1949 relativo a la protección debida a las personas civiles en tiempo de guerra Derecho de Ginebra y el Derecho de La Haya.

[100] SALMÓN, Elizabeth. Op. Cit., p. 69.

[101] Cfr. SCHMITT, Michael. Wired warfare: computer network attack and jus in bello. En: RICR, 2002. Vol 84, No. 846. P. 375.

[102] Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security (hereinafter 'Report of the Secretary-General'), 15 July 2011, UN Doc. A/66/152, p. 6; Para conocer la estrategia de ciberseguridad de Australia, consultar: Australian Government. Department of the Prime Minister and Cabinet. Cyber security strategy. https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

[103] United Kingdom. HM Government. A Strong Britain in an Age of Uncertainty: The National Security Strategy, 2010.

armado en el ciberespacio y considera que no es necesario crear nuevas normas de derecho internacional para regular los asuntos cibernéticos[104].

A su vez, el Comité Internacional de la Cruz Roja (en adelante CICR) considera que el DIH es aplicable al ciberespacio toda vez que las operaciones se lleven a cabo en él pueden traducirse en costos humanos[105]. Sin embargo, considera que los Estados están llamados a determinar si es necesario desarrollar normas jurídicas para asegurar una protección suficiente a los civiles frente al impacto de la evolución tecnológica[106].

La ONU tampoco se ha quedado fuera de este debate. El grupo de expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional sostuvieron ante la Asamblea General que los Estados deben tener en cuenta los principios de humanidad, necesidad proporcionalidad y distinción para el ejercicio de sus actividades a través de las TIC[107].

Así las cosas, no cabe duda sobre la existencia de un quinto dominio para el desarrollo de conflictos, lo que se traduce en la necesidad de evaluar si para regular de manera efectiva este espacio basta con interpretar principios y normas de DIH existentes, - bien sea una interpretación amplia o restrictiva-.

[104] EUROPEAN COMMISSION. Op. Cit. p. 15- 16.
[105] MELZER, Nils y KUSTER, Etienne. International Humanitarian Law: a comprehensive introduction. Geneva: International Committee of the Red Cross, 2016. P. 28; International Committee of the Red Cross. Cyber warfare and international humanitarian law: The ICRC's position. Óp. Cit., p.1.
[106] Ibíd., p. 2.
[107] P. 3 y 16.

Además es pertinente revisar si es necesario el diseño de una regulación especial, como sucedió en el caso del debate sobre el uso de las armas químicas[108].

Hasta el momento, no hay desarrollo sobre las ciberoperaciones en el DIH[109], pero existen propuestas que van desde la interpretación del derecho existente, hasta la creación de un Convenio de Ginebra sobre el Ciberespacio[110], o la propuesta rusa para la elaboración de un tratado que limite el uso de la tecnología en las ciberguerras[111].

A continuación, se determinará si las normas de DIH que se refieren a la conducción de hostilidades y a los medios y métodos de guerra son suficientes para hacer frente a la problemática del ciberespacio.

i) Derecho internacional humanitario y ciberoperaciones militares: límites a las ciberhostilidades

La existencia de un conflicto es un presupuesto básico para la aplicación del DIH[112]. Sin embargo, ante la falta de claridad respecto de las normas aplicables al ciberespacio, es necesario comprender qué tipo de actividades en el marco de un conflicto armado – internacional o no internacional- darían paso a la aplicación de este régimen jurídico, pues de ese modo sería posible proponer prohibiciones y limitaciones[113].

---

[108] Cfr. Naciones Unidas. Convención sobre la prohibición del desarrollo, la producción, el almacenamiento y el empleo de armas químicas y sobre su destrucción, 1994.
[109] DROEGUE, Cordula. Get off my cloud: cyber warfare, international humanitarian law and the protection of civilians. En: International Review of the Red Cross, 2012. Volume 94, No. 886. p. 540.
[110] LIIVOJA, Rain. Op. Cit., p. 1160; SÁNCHEZ LOZANO, Martha Liliana. Óp. Cit., p. 352.
[111] Cfr. RABOIN, Bradley. Op. Cit.
[112] AMBOS, Kai. Responsabilidad penal internacional en el ciberespacio [En línea]. En: InDret: revista para el análisis del derecho, 2015. No. 2. P. 5. [Fecha de consulta: 18 de abril de 2018] Disponible en: http://www.department-ambos.uni-goettingen.de/data/documents/Veroeffentlichungen/epapers/Responsabilidad%20ciberespacio%20InDret.pdf
[113] Manual de Tallin, regla 30.

En este orden de ideas, es necesario determinar si la protección del DIH se extiende a determinadas ciberoperaciones de carácter militar, entre ellas los ciberataques, o si solo aplica en estos últimos eventos.

Así las cosas, debe analizarse qué tan estricta debe ser la interpretación de este cuerpo normativo para dar una efectiva protección a los civiles - los más afectados en este nuevo dominio-, teniendo en cuenta características como el problema del doble uso de las infraestructuras (que se abordará con posterioridad) y el hecho – casi imposible, por ahora- de separar las redes y cableados de circulación de datos[114].

En primer lugar, debe hacerse referencia a los conceptos de ataque y ciberataque en el marco del DIH.

Según los presupuestos tradicionales del DIH, los ataques son "actos de violencia contra el adversario, sean ofensivos o defensivos"[115]. Ahora bien, según el Manual de Tallin, un ciberataque es una "operación defensiva u ofensiva que razonablemente podría causar lesiones o incluso muerte a personas, y daño o destrucción de bienes"[116]. Es importante resaltar desde ahora que según el Grupo de Expertos Internacionales, la definición se extiende a los conflictos de carácter internacional y no internacional. Esto puede atribuirse al cambio de paradigma al que conlleva el ciberespacio, pues limitantes clásicos como la existencia de fronteras tienden a desaparecer cuando se realizan operaciones en este dominio[117].

[114] Cfr. DROEGUE, Cordula. Óp. Cit.
[115] Art. 49. Protocolo Adicional I de 1977.
[116] Manual de Tallin, regla 30. Traducción propia.
[117] SÁNCHEZ LOZANO, Martha Liliana. Los conflictos armados en el ciberespacio: retos del Derecho Internacional Humanitario. Bogotá: Grupo Editorial Ibáñez, 2018. P. 38.

Aunque estos conceptos son distintos, ninguno de los dos tiene en cuenta todas las eventualidades que se generan en el ciberespacio, puesto que deja de lado el funcionamiento de las nuevas tecnologías y su incidencia en la vida de los civiles. En este punto es importante recordar que el DIH protege a los civiles no solo de ataques directos, sino de los efectos que conlleven las operaciones militares[118].

Conforme a lo anterior, es razonable extender la protección del DIH a algunas operaciones militares que desde una perspectiva clásica no tienen el carácter de ataque, pero que si afectan a la población civil debido a sus efectos. Esto conlleva a un análisis a la luz de los principios que guían la conducción de hostilidades, como la distinción entre civiles y combatientes, la proporcionalidad y precaución en el ataque.

Para estos efectos, es necesario determinar qué actividades se consideran hostilidades. Con este término se hace referencia al uso de medios y métodos por una de las partes en conflicto para causar daño a la otra[119]. En el *corpus iuris* del DIH existen reglas que desarrollan el concepto de hostilidades, como los criterios de participación directa en ellas.

A partir de tres criterios se considera que una persona participa y, en consecuencia, se presentan hostilidades cuando: i) existe la probabilidad de que el acto tenga actos adversos sobre las operaciones militares o la capacidad militar de una parte del conflicto, o bien, que cause muerte, heridas, daño o destrucción a las personas o los bienes protegidos contra ataques directos umbral del daño[120], en el que no se requiere su materialización

[118] Art. 51.1, 51.3, Protocolo Adicional I de 1977; art. 13.1 y 3, Protocolo Adicional II de 1977.
[119] MELZER, Nils. Guía para interpretar la noción de participación directa en las hostilidades según el Derecho Internacional Humanitario. Ginebra: Comité Internacional de la Cruz Roja, 2010.
[120] Este concepto hace referencia a la "probabilidad de que el acto tenga actos adversos sobre las operaciones militares o la capacidad militar de una parte del conflicto, o bien, que cause

efectiva, sino la "probabilidad objetiva de que el acto tenga como consecuencia ese daño"[121] ii) causalidad directa[122] y iii) nexo beligerante[123].

Estos criterios se pueden aplicar en el ámbito del ciberespacio, pues como se explicará en el siguiente capítulo, hay ciberhostilidades que conllevan efectos como los que se describen en estas normas, así no exista fuerza cinética. Además, cabe resaltar que el CICR resaltó en su guía sobre la conducción de hostilidades que las interferencias electrónicas en redes informáticas militares, en líneas telefónicas de la misma categoría o la transmisión de información alcanzaría el umbral del daño[124].

Conforme a lo anterior, el DIH debería aplicarse a los hechos que se consideren ciberhostilidades, es decir, a ciberataques en los que se presente el uso de medios y métodos de combate[125]. Esto tiene implicaciones en la interpretación de los principios cardinales de esta rama del derecho internacional público.

En segundo lugar, es importante analizar el alcance del término violencia en los ataques. Así pues, en los comentarios a la regla 30 del Manual de Tallin se destaca la importancia de la violencia en la medida que a través de este criterio es posible distinguir los ataques de otras operaciones militares como el espionaje[126].

---

muerte, heridas, daño o destrucción a las personas o los bienes protegidos contra ataques directos". Cfr. MELZER, Nils. Guía para interpretar la noción de participación directa en las hostilidades según el Derecho Internacional Humanitario, Op. Cit., p. 46.

[121] MELZER, Nils. Guía para interpretar la noción de participación directa en las hostilidades según el Derecho Internacional Humanitario. Op. Cit. p. 47.

[122] Se refiere al "vínculo causal directo entre el acto y el daño que pueda resultar de ese acto o de la operación militar coordinada de la que el acto constituya parte integrante", Ibíd., p. 46.

[123] Ibíd. Consiste en que "propósito específico del acto debe causar directamente el umbral exigido de daño en apoyo de una parte del conflicto y en menoscabo de otra".

[124] Ibíd., p. 48.

[125] Manual de Tallin, regla 41.

[126] Comentarios a la regla 30, Manual de Tallin.

En este sentido, lo importante según este grupo es que tanto la naturaleza como las consecuencias de un ataque sean violentas[127]; incluso se ha dicho que la operación puede seguir catalogándose como ataque cuando se detiene a través de mecanismos de ciberdefensa como antivirus y firewalls[128] y, por ende, no logra su objetivo.

Es menester resaltar que la tecnología ha dado lugar al desarrollo de armas que no utilizan fuerza cinética, como las armas bilógicas o químicas, o las ciberarmas (v.g, virus, gusanos informáticos, troyanos, *spyware, bots,* o armas electromagnéticas[*129*]). A medida que estos fenómenos se presentaron, el DIH respondió a través de regulación en términos de limitación o prohibición, verbigracia, el Protocolo de Ginebra de 1925, relativo a la prohibición del empleo en la guerra de gases asfixiantes, tóxicos o similares y de medios bacteriológicos[130] o la Convención de 1993 sobre armas químicas[131].

Sin embargo, el término violencia también debe tenerse en cuenta para evaluar los efectos de las operaciones militares, incluso cuando no existan armas que involucren el uso de fuerza física o cinética. Así lo afirma, por ejemplo, el Tribunal Penal Internacional para la Ex Yugoslavia (TPIY) en el caso *Tadic*, donde consideró que el uso de este tipo de agentes en una operación militar conlleva a consecuencias violentas, así no exista uso de la fuerza física[132].

---

[127] Ibíd.
[128] Ibíd.
[129] SOLCE, Natasha. Óp. Cit., p. 305.
[130] Protocolo de Ginebra de 1925 (Protocolo relativo a la prohibición del empleo en la guerra de gases asfixiantes, tóxicos o similares y de medios bacteriológicos).
[131] Convención sobre la prohibición del desarrollo, la producción, el almacenamiento y el empleo de armas químicas y sobre su destrucción de 1994.
[132] Cfr. DROEGUE, Cordula. Op. Cit., p. 557; ICTY, Prosecutor v. Dusko Tadic´, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995, párr. 120 y 124.

Este argumento se puede trasladar al contexto del ciberespacio. En la doctrina se habla de un "enfoque basado en los efectos"[133], que se extendería a las operaciones cibernéticas. Desde esta perspectiva, los ataques que no involucren fuerza cinética *per se*, pero cuyos efectos en el mundo físico sean los mismos que se exigen en el concepto de ataques, es decir, muerte, daño o destrucción, hacen parte de un acto de violencia[134].

En este sentido, conviene establecer qué tipo de ciberoperaciones integran la categoría de los actos violentos para el DIH. Sobre el particular, Droegue[135] y Schmitt[136] mencionan algunos ejemplos, a partir de los cuales es posible construir un "semáforo" para la aplicación de las normas y principios del DIH.

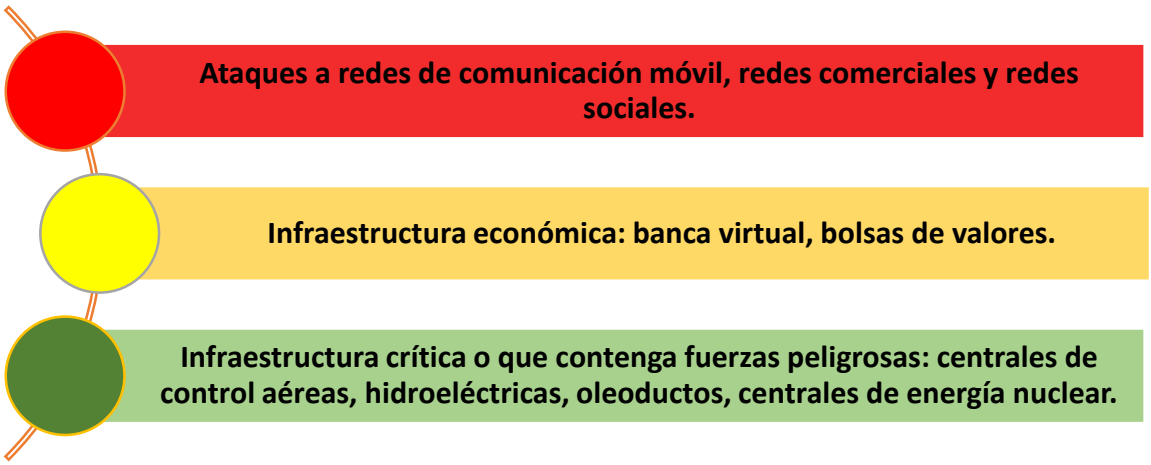

Fig. 6. Semáforo de aplicación del DIH según la infraestructura objeto de ataque.

[133] MELZER, Nils. Ciberwarfare and international law [En línea]. UNIDIR Resources, 2011. Disponible en: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. P. 26. Consultado el 26 de marzo de 2018.
[134] Ibíd.
[135] DROEGUE, Óp. Cit., p. 552.
[136] SCHMITT, Michael N. Wired warfare: Computer network attack and jus in bello. Op. Cit., pp 374 y ss.

Luz verde: ataques a infraestructura crítica.

Existen ataques a infraestructura crítica que afectan el desarrollo de la vida de la población civil y sus condiciones mínimas de existencia. Así pues, piénsese en la interrupción de los servicios de electricidad o de suministro y tratamiento de agua[137] a través de una ciberoperación. Este evento no causa destrucción *per se*, pero si alcanza un umbral de daño grave para este grupo protegido por el DIH, puesto que en cualquier lugar del mundo, estos son servicios básicos de los que depende el funcionamiento de bienes protegidos, como hospitales[138].

Tan importantes son las infraestructuras y los servicios en mención, que cuentan con protección por parte del DIH existente. Por ejemplo, el PA I consagra la protección de unidades sanitarias[139], dada su importancia estratégica para proteger derechos humanos como la vida y la integridad de los seres humanos.

A través de un ataque cibernético sería posible causar daño, muerte o lesiones a pacientes que se encuentren en unidades de cuidados intensivos.

Se afirma que todas las operaciones que se prevé causen la muerte, lesiones o daños físicos constituyen ataques, incluso cuando esos daños se deban a los efectos indirectos o secundarios previsibles de un ataque, como la muerte de pacientes en unidades de cuidados intensivos ocasionada por un

[137] Ejemplos tomados de DROEGUE, Cordula. Óp. Cit, p. 552. Traducción propia.
[138] Cfr. Comité Internacional de la Cruz Roja. El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos. XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Ginebra, 2015. 32IC/15/11. P. 54.: “incluso cuando esos daños se deban a los efectos indirectos o secundarios previsibles de un ataque, como la muerte de pacientes en unidades de cuidados intensivos ocasionada por un ciberataque contra la red de distribución eléctrica que corta el suministro eléctrico del hospital”.
[139] Art. 12. Protocolo Adicional I de 1997.

ciberataque contra la red de distribución eléctrica que corta el suministro eléctrico del hospital.

Otros ejemplos acertado son eventos como la toma de control de los sistemas de redes de control de los oleoductos o gasoductos, la fusión un reactor nuclear a través de la manipulación de sus redes de control, manipular las redes de los centros de control de las instalaciones de producción de químicos tóxicos, o bloquear los sistemas de tráficos aéreo de un aeropuerto[140].

Esto encuentra fundamento en diferentes normas consuetudinarias y convencionales de DIH. Por hacer mención a algunas, conviene recordar aquellas que expresamente prohíben causar daños ambientales para obtener ventaja militar sobre el adversario o aquellas[141], o que instan a proteger a la población civil de los efectos adversos de las operaciones militares[142].

Con base en estos ejemplos, es posible afirmar que ya existe cierto consenso sobre la prohibición de atacar infraestructuras críticas. En efecto, los expertos que participaron en la redacción del Manual de Tallin consideran que los efectos que puede tener el daño de infraestructuras de este tipo, difieren poco de los efectos que pueden causarse a través de armas tradicionales que utilicen fuerza cinética[143].

[140] SCHMITT, Michael N. Wired warfare: Computer network attack and jus in bello. Op. cit., p. 374. Traducción propia. Sobre el ejemplo del tráfico aéreo cabe resaltar que a la luz del DIH la prohibición recae sobre aeropuertos civiles, pues la operación si está permitida en aeropuertos militares, según el art. 52 del Protocolo Adicional I de 1977.
[141] Art. 35.3 y 55.1 del Protocolo Adicional I de 1977.
[142] Título IV, Sección I, Protocolo Adicional I de 1977.
[143] Cfr. Manual de Tallin, comentario a la regla 30. Además, debe tenerse en cuenta el comentario a la regla 13, donde se afirma que el término daño incluye interferencias en la funcionalidad, cuando restablecerla implica remplazar componentes físicos.

Luz amarilla: casos grises.

Debido a la interconexión, actualmente muchos servicios dependen de la conexión a redes. Debido a este fenómeno, es conveniente pensar en las consecuencias de la denegación de acceso a la banca virtual a la población civil o la interrupción o denegación de servicios en la bolsa de valores de determinado Estado [144], puesto que si bien la calidad de vida de la población se ve disminuida cuando no hay acceso al dinero, en principio no hay consecuencias que permitan hablar de violencia.

Sin embargo, al tener en cuenta los efectos de las crisis económicas como la Gran Depresión de 1929, es claro que la ausencia de medios económicos conlleva a efectos adversos como el hambre del afectado y su familia, así como a consecuencias psicológicos como la angustia y la depresión[145].

Otro caso que también se inscribe en esta categoría son los datos como objetos de ataque. Así, el DIH sería aplicable cuando las ciberoperaciones interfieran con información contenida ellos, y se compruebe que esta acción ha tenido efectos violentos[146].

Esto permite afirmar que en este tipo de ciberoperaciones, los operadores jurídicos deben hacer un cuidadoso examen de los efectos de la acción que desarrolle una de las partes del conflicto para aplicar el DIH, pues este tiene cabida siempre que se cause terror entre la población civil[147].

---

[144] DROEGUE, Cordula. Óp. Cit., p. 553; SCHMITT, Michael N. Wired warfare: Computer network attack and jus in bello. Óp. Cit., p. 337.
[145] Este ejemplo lo propone SCHMITT. Cfr. SCHMITT, Michael. Wired warfare: Computer network attack and jus in bello. Óp. Cit., p. 337.
[146] Manual de Tallin, comentario a la regla 30.
[147] Art. 51.1, Protocolo Adicional I de 1977.

Luz roja: eventos que no tienen cabida en el DIH.

Por el contrario, hay ataques que tienen incidencia directa en la vida de los civiles, pero no podrían ser objeto del DIH[148]. Dentro de este grupo se encuentra la denegación de servicios de compras por internet, el bloqueo de acceso a Facebook para prevenir la circulación de propaganda pro insurgencia, la denegación de servicios en servicios de reserva de vuelos de aerolíneas privadas para perjudicar la movilidad de la población civil[149], o el ciberespionaje[150].

Extender la interpretación para dar cabida a estos eventos tendría efectos muy nocivos y conllevaría a un alto nivel de incertidumbre para la comunidad internacional, y para los juristas que se ocupan del examen estos temas, pues existiría una excesiva subjetividad para determinar si estos eventos constituyen o no ataques.

En suma, está claro que el DIH debe replantear el alcance de sus principios y normas respecto de la conducción de hostilidades para regular de manera adecuada las ciberoperaciones de carácter militar que se den en el quinto dominio. Además de esta reinterpretación, es necesario esperar que los Estados consoliden sus prácticas en el ciberespacio para poder fijar límites a las actuaciones, que eventualmente podrían dar lugar a normas de derecho convencional, fruto del consenso en esta y otras materias[151].

---

[148] Sobre este punto, podría discutirse si dichos supuestos podrían significar alguna ventaja militar estratégica.
[149] DROEGUE, Cordula. Óp. Cit., p. 553.
[150] SCHMITT, Wired warfare: computer network attack and jus in bello. Op. Cit., p. 374.
[151] BROWN, Gary y POELLET, Keira. El derecho internacional consuetudinario del Ciberespacio [En línea]. En: Air and Space Power Journal, 2013. PP. 31- 44. Disponible en: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2013/2013-1/2013_1_06_brown_s.pdf. Consultado el 28 de febrero de 2018.

ii) Relación entre el ciberespacio, los medios y métodos de guerra y los principios del DIH.

Los medios y métodos de guerra son otra perspectiva desde la que se puede ver el ciberespacio y las ciberarmas. Las ciberarmas tienen cada día más protagonismo en los conflictos armados, y por esta razón los Estados deberían desarrollar normas para regular y limitar su uso[152].

Ahora bien, ¿cuál sería el medio y el método de combate en el ciberespacio? Si se toma como base el comentario al PA I, el medio de combate corresponde al arma – en este caso, son los códigos dañinos que circulan a través de redes, más no las redes en sentido estricto - , mientras que el método correspondería al uso que se le da al determinado código[153].

El DIH no contiene normas que prohíban las ciberoperaciones, pero el CICR sostiene que es evidente que estas deben realizarse con respeto a las normas hasta ahora vigentes[154]. Además, es importante tener en cuenta la Cláusula de Martens[155], bajo la cual los civiles y combatientes - en caso de ausencia de regulación de un supuesto determinado-, "quedan bajo la protección y el imperio de los principios del derecho de gentes derivados de los usos establecidos, de los principios de humanidad y de los dictados de la conciencia pública"[156].

---

[152] DROEGUE, Cordula. Óp. Cit., p. 536.

[153] Cfr. SCHMITT, Michael, N. Wired warfare: computer network attack and jus in bello. Óp. Cit., p. 389.

[154] Comité Internacional de la Cruz Roja. El Derecho Internacional Humanitario y los desafíos de los conflictos armados contemporáneos, 2011. Óp. Cit., p. 43.

[155] La Cláusula de Martens es una norma de derecho consuetudinario (cfr. CIJ International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996. Párr. 84,). Actualmente está consagrada en el art. 1.2 del Protocolo I Adicional de a1977. Sin embargo, su existencia data de 1899, cuando se incluyó en el Preámbulo del (II) Convenio de La Haya de 1899 relativo a las leyes y costumbres de la guerra terrestre. Cfr. TICERHURST, Rupert. La Cláusula de Martens y el derecho de los conflictos armados [En línea]. 31 de marzo de 1997. Revista Internacional de la Cruz Roja, 1997. Disponible en: https://www.icrc.org/spa/resources/documents/misc/5tdlcy.htm.

[156] Ibíd.

En este sentido, son relevantes las consideraciones de la Corte Internacional de Justicia (CIJ) en su opinión consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares, en la que afirmó - bajo la premisa de no causar daños superfluos o innecesarios a la población civil- que "los Estados no gozan de libertad ilimitada de elección en cuanto al tipo de armas que utilizan"[157].

Asimismo, la CIJ afirmó que el carácter humanitario de los principios del DIH implica que estos sean "válidos para todas las formas de guerra y todos los tipos de armas, las del pasado, las del presente y las del futuro"[158].

Por otra parte, se dice que el DIH tiene dos clases de normas en materia de tecnología: unas específicas[159], que corresponden a los tratados sobre la prohibición o la restricción del uso de ciertas armas, y otras neutrales[160], que se refieren a los efectos de los medios de guerra, más que a la tecnología que utilicen las armas *per se,* sin optar por el uso de una u otra tecnología en especial.

Dentro de este último grupo de normas hay una muy importante: el art. 36 del PA I. Su contenido exige a las Partes contratantes realizar un examen para determinar si el empleo de una nueva arma está prohibido por ese tratado o por otras normas de derecho internacional[161].

---

[157] International Court of Justice, Legality of the Threat or Use of Nuclear Weapons. Op Cit., párr. 78.
[158] International Court of Justice, Legality of the Threat or Use of Nuclear Weapons. Op. Cit., párr. 86.
[159] LIIVOJA, Rain. Op. Cit., p. 1167. Es válido resaltar algunos ejemplos que propone la autora, como la prohibición de utilizar medios o métodos de guerra que no respeten el principio de distinción (art. 23, Convenios de la Haya), o aquellas que prohíben el uso de medios y métodos de guerra que causen daños en el medio ambiente (art. 35.2 del Protocolo I adicional a los cuatro Convenios de Ginebra).
[160] Ibíd., pp. 1167-1668.
[161] Art. 36, Protocolo Adicional de 1977: "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. Un antecedente de esta norma es el la Declaración de

La existencia de esta disposición confirma que los métodos de combate no se pueden utilizar sin restricciones, incluso cuando no están regulados[162]. La exigencia de un examen jurídico interdisciplinario en las etapas de estudio, desarrollo, adquisición o adopción"[163] es una prueba de neutralidad del DIH, pues cualquier nueva tecnología con aplicaciones militares debe someterse a estudio, sin excepción.

En este sentido, el ámbito de aplicación material del art. 36 del PA I comprende "las armas de todo tipo", y "las maneras en que han de utilizarse esas armas conforme a la doctrina militar, las tácticas, las reglas de enfrentamiento, los procedimientos de operación y las contramedidas"[164], puesto que las armas no pueden analizarse sin el método de guerra para el cual están destinadas[165].

Este examen de licitud sobre nuevas armas es una obligación para los Estados, que nace en virtud de la prohibición de emplear armas, medios y métodos de guerra ilícitos o utilizar armas, medios y métodos de guerra de manera ilícita[166].

San Petersburgo de 1868 según la cual, "las Partes contratantes o adherentes se reservan entenderse ulteriormente todas las veces que se formule una propuesta precisa con miras a perfeccionamientos venideros, que la ciencia podría aportar al armamento de las tropas, a fin de mantener los principios que han planteado y de conciliar las necesidades de la guerra con las leyes de humanidad".

[162] DÖRMANN, Knut. Applicability of the Additional Protocols to Computer Network Attacks [En línea]. En: International Committe of the Red Cross. International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19.11.2004. Disponible en: https://www.icrc.org/eng/resources/documents/misc/68lg92.htm. P. 2.

[163]. LAWAND, Kathleen. Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos. Medidas para aplicar el artículo 36 del Protocolo adicional I de 1977. Ginebra: Comité Internacional de la Cruz Roja, 2006. Disponible en: https://www.icrc.org/spa/assets/files/other/icrc_003_0902.pdf.¨P. 22.

[164] LAWAND, Kathleen. Óp. Cit., p. 8.

[165] Ibíd., p. 9.

[166] Ibíd., p. 4

Debido al rápido desarrollo de determinados códigos cibernéticos[167] que tienen la categoría de armas, estos deberían someterse a un examen jurídico para determinar su licitud y las formas de uso, conforme al ámbito de aplicación material del art. 36 del PA I. En este orden de ideas, el CICR propone unos criterios de evaluación para determinar la legalidad del uso de nuevas armas, que son aplicables a las ciberarmas.

Según la Guía *para el examen jurídico de las armas, los medios y los métodos de guerra nuevos* del CICR, en primer lugar debe determinarse si el "arma o medio de guerra bajo examen está prohibido o restringido por un tratado que vincula al Estado examinador o por el derecho consuetudinario"[168]. Como se ha dicho con anterioridad, no existen normas que prohíban o restrinjan el uso de ciberarmas, y en general, ninguna que regule asuntos sobre el ciberespacio.

Debido a ese aparente vacío, debe utilizarse el segundo criterio de la guía, que corresponde a una valoración de las armas o métodos de guerra – en este caso, las ciberarmas-, conforme a "las normas generales aplicables a todas las armas, medios y métodos de guerra que figuran en el Protocolo Adicional I y en otros tratados que vinculan al Estado examinador o en el derecho internacional consuetudinario"[169].

Dentro de las normas que hacen parte del PA I, serían aplicables al ciberespacio aquellas que se refieren a normas de precaución[170], distinción[171],

[167] MELZER, Nils y KUSTER, Etienne. Op. Cit., p. 123.
[168] LAWAND, Kathleen. Óp. Cit., p. 10.
[169] LAWAND, Kathleen. Óp. Cit., p. 10.
[170] Art. 35.2, Protocolo Adicional I de 1977. HENCKAERTS, Jean Marie y DOSWALD-BECK, Louise. El Derecho Internacional Humanitario Consuetudinario. Volumen I, normas. Buenos Aires: Comité Internacional de la Cruz Roja, 2007. Norma 70.
[171] Art. 54.1b, Protocolo Adicional I de 1977. Esta norma también hace parte del derecho consuetudinario. Cfr. HENCKAERTS, Jean Marie y DOSWALD-BECK. Normas 12 y 71.

proporcionalidad[172] y las que se refieren a daños “extensos, duraderos y graves al medio ambiente”[173], que a su vez encuentran correlativos en normas consuetudinarias[174]. Este examen se realizará con posterioridad en el presente capítulo.

Además de estas normas jurídicas, se deben tener en cuenta las consecuencias militares, técnicas, ambientales y sanitarias que tenga el arma sujeta a análisis[175], en este caso, una ciberarma.

Teniendo en cuenta estos parámetros y el carácter humanitario del derecho de los conflictos, los medios y métodos cibernéticos deben partir de unos mínimos para que se puedan utilizar de tal forma que respeten y garanticen los principios y normas existentes, siempre en aras de proteger a la población civil, en la mayor medida de lo posible.

En primer lugar, existen supuestos que no resultan problemáticos, pues son inadmisibles desde cualquier punto de vista. En este orden de ideas, existen infraestructuras que no pueden ser objeto de ataque - sin importar su carácter civil o militar-, como es el caso de aquellas que contienen fuerzas peligrosas. En este grupo se encuentran “las presas, los diques y las centrales nucleares de energía eléctrica”[176], cuando los ataques liberen las fuerzas que estos contienen, que en consecuencia, generen pérdidas en los civiles.

[172] Art. 51.5b. HENCKAERTS, Jean Marie y DOSWALD-BECK, Louise. Norma 14.
[173] Arts 35.3; 55; 54.1c, Protocolo Adicional I de 1977. Esta norma también hace parte del derecho consuetudinario. Cfr. HENCKAERTS, Jean Marie y DOSWALD-BECK, Louise. Norma 45.
[174] Cfr HENCKAERTS, Jean Marie y DOSWALD-BECK, Louise. Normas 70- 71,
[175] Cfr. LAWAND, Kathleen. Op. Cit., p. 16 y ss; Comité Internacional de la Cruz Roja. Mejorar la protección en los conflictos armados y en otras situaciones de violencia armada. XVIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Ginebra, 2003. Objetivo final 2.5., p. 22.
[176] Art. 56. 1, Protocolo I Adicional de 1977.

Si se presentara un ciberataque a estos bienes a través de ciberarmas, la conducta podría catalogarse como ilegal a la luz de los principios y normas del DIH, conforme a lo expuesto hasta este punto.

El dilema de interpretación empieza con el "doble uso del ciberespacio"[177]. Debido su composición, existe un alto nivel de interconectividad entre las redes, lo que significa que pueden ser utilizadas de manera simultánea por civiles y fuerzas militares[178]. Incluso, muchas redes militares pueden llegar a depender de las redes comerciales[179].

Los problemas que genera este fenómeno causan preocupación en órganos como la Asamblea General de la ONU, que considera que el doble uso que se le puede dar a las nuevas tecnologías incide en materia del mantenimiento de la paz internacional y la seguridad nacional[180].

Así pues, las instalaciones que se ven envueltas en esta encrucijada son principalmente las centrales generadoras de energía, los puentes[181], o sistemas de comunicaciones y satélites como INTELSAT, EUROSAT y ARABSAT[182], por hacer mención a algunos ejemplos, pues no es un listado

---

[177] Este fenómeno se menciona en doctrina especializada. Cfr. DROEGUE, Cordula; SCHMITT, Michael N. Wired warfare: computer network attack and jus in bello; KELSEY, Jeffrey T. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. En: Michigan Law Review, 2008. Volume 106. P. 1427.

[178] International Committee of the Red Cross. Cyber warfare and international humanitarian law: The ICRC's position. Óp. Cit., p. .3.

[179] Comité Internacional de la Cruz Roja. El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos. XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Ginebra, 2011. 31IC/11/5.1.2. P. 41.

[180] Naciones Unidas. Asamblea General. Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, 2010. A/65/2010.

[181] O'DONELL, Brian y KRASKA, James C. Humanitarian Law: Developing International Rules for the Digital Battlefield. Oxford Academic, 2003. En: KELSEY, Jeffrey T. Óp. Cit., p. 1437.

[182] SCHMITT, Michael M. Wired warfare: computer network attack and jus in bello, p. 384; para ampliar la información sobre dichos satélites, cfr: http://www.arabsat.com/english/about; http://www.eurosat.com/about.

taxativo. Esto permite tener en cuenta otros componentes de la infraestructura civil que pueden utilizar los combatientes en tiempo de conflicto.

Conforme a lo anterior, se abordarán los puntos que más generan preocupación respecto del alcance de la interpretación de los principios de distinción, proporcionalidad y precaución para efectos del ciberespacio.

En lo que respecta al principio de distinción, el CICR considera que este es una norma de derecho internacional consuetudinario que se aplica en conflictos de carácter internacional y no internacional[183], por el cual se entiende que ni la población civil, ni sus bienes pueden ser objeto de ataques, pues estos deben dirigirse contra objetivos militares[184].

El concepto de objetivo militar se desarrolla en el art. 52. 2 del PA I, donde se establece que corresponde 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"[185].

A partir de este contenido, los redactores del Manual de Tallin consideran que este principio es aplicable a los ciberconflictos[186]. Sin embargo, el doble uso en el ciberespacio hace que aunque una ciberoperación se dirija contra objetivos militares legítimos, sea difícil limitar su alcance, pues si el código dañino es lo suficientemente dañino, probablemente no se podrá controlar su

[183] HENCKAERTS, Jean Marie y DOSWALD-BECK. Óp. Cit., p. 3. También lo ha afirmado la Asamblea General de la ONU. Cfr. Asamblea General de Naciones Unidas. Respeto de los derechos humanos en los conflictos armados. Res. 2444 de 1968.
[184] El contenido de este principio se convencionalizó. Cfr. Art. 48, Protocolo Adicional I de 1977; art. 13, Protocolo Adicional II de 1977.
[185] Art. 52.2 Protocolo Adicional I de 1977.
[186] Manual de Tallin, regla 31.

incidencia en otras redes, y por ende, puede causar efectos adversos sobre la población civil[187].

Una posible solución, según Kelsey[188], sería ampliar la interpretación de varios conceptos incluidos en este principio. Por ejemplo, propone ampliar el contenido de "objetivo militar legítimo" en el entorno cibernético, así como flexibilizar criterios como la ventaja militar definitiva, puesto que en muchas ocasiones las ciberoperaciones coadyuvarían a debilitar a la otra parte, pero no supondrían como tal una ventaja definitiva toda vez que las ciberarmas, *per se,* no son letales.

Otros como Geiss[189], consideran que en virtud de que todos los dispositivos que se conectan en el ciberespacio tienen un potencial uso militar, hay que delimitar sistemas específicos y activos en el ciberespacio, específicamente aquellos en los que los que confían millones de civiles para que no sean objeto de ataque.

Domínguez[190] habla incluso de un vaciamiento del principio de distinción en el ciberespacio, de modo que solo podría hablarse de la aplicación de los principios de proporcionalidad y precaución.

Una solución sería que los Estados fijaran pautas que probablemente surgirían del análisis de sus prácticas[191]- que ya empiezan a evidenciarse en sus políticas de ciberseguridad y ciberdefensa- para definir unos mínimos comunes del alcance del principio de distinción en el ciberespacio.

---

[187] DROEGUE, Cordula. Óp. Cit., p. 539; DÖRMANN, Knut. Óp. Cit., p 5.
[188] Cfr. KELSEY, Jeffrey. Óp. Cit., p. 1447- 1448.
[189] GEISS, Robin. Humanitarian aspects of cyber warfare. En: HEINTSCHEL von HEINEGG, Wolff. International Humanitarian Law and New Weapon Technologies. San Remo: International Institute of Humanitarian Law, 2012, p. 153.
[190] DOMÍNGUEZ VASCOY, Jerónimo. Óp. Cit., p. 637.
[191] Cfr. BROWN, Gary y POELLET, Keira. Óp. Cit., p. 31- 44.

En resumen, no es claro aún es el alcance de este principio, pues como se observó, ni siquiera los expertos en la materia llegan a un consenso. Las vicisitudes de los avances tecnológicos ponen en tela de juicio la aplicación material del principio de distinción, lo cual puede dar mayor preponderancia a los principios de proporcionalidad y distinción para el análisis de casos en concreto.

En este orden de ideas, no se debe excluir de la discusión otros principios como el de proporcionalidad, que según el Manual de Tallin, también resulta aplicable al contexto del ciberespacio[192].

Este principio parte de la existencia de eventos en los que los civiles o sus bienes sufren daños colaterales – directos o indirectos-[193], lo cual no implica la ilegalidad del ciberataque *prima facie*, pues esta depende de la relación entre el daño previsible que el atacante pueda causar y la ventaja militar anticipada que se pueda obtener como resultado del ciberataque[194].

De igual forma, se ha dicho que el principio de proporcionalidad debe tenerse en cuenta cuando exista daño como pérdida de funcionalidad en determinado bien protegido[195].

Incluso cuando se dirijan ciberoperaciones contra objetivos militares legítimos, los ciberataques deben respetar el principio de proporcionalidad con el fin proteger a los civiles y sus bienes de daños que resulten excesivos frente a la ventaja militar[196].

---

[192] Manual de Tallin, regla 51; GEISS, Robin. Óp. Cit., p. 154.
[193] Cfr. Manual de Tallin, regla 51, comentario 6.
[194] Manual de Tallin, regla 51, comentario 2.
[195] Manual de Tallin, regla 51, comentario 5.
[196] SCHMITT, Michael N. Wired warfare: computer network attack and jus in bello. Óp Cit., p. 397.

Asimismo, las partes deben planear sus operaciones conforme a este principio cuando se trate de infraestructura de doble uso[197]. Sin embargo, cuando el daño colateral es excesivo en comparación con la ventaja militar anticipada que se obtendría con la operación, esta debería ser prohibida[198].

La reinterpretación del daño colateral es un reto para el DIH, pues debido a la naturaleza del ciberespacio, se sugiere tener en cuenta concepciones nuevas. Por ejemplo, se dice que este concepto debería integrar efectos que van más allá de lo físico, puesto que en la sociedad actual existen bienes que no son perceptibles – como los sistemas de comunicaciones-, pero que resultan importantes para la sociedad, de modo que un ataque podría tener graves consecuencias para la población civil[199].

Otro principio que resulta importante es el de precaución en el ataque, que aplica "a cualquier operación de guerra terrestre, naval o aérea que pueda afectar en tierra a la población civil, a las personas civiles y a los bienes de carácter civil"[200]. Según los expertos encargados de la redacción del Manual de Tallin, este principio también resulta aplicable al ciberespacio.

Así las cosas, los comandantes militares y demás miembros que desarrollen ciberoperaciones deben tener un cuidado especial para evitar efectos adversos sobre la población civil, los civiles individualmente considerados y sus objetos[201]. Debido a la naturaleza del ciberespacio, las precauciones en el

[197] Human Rights Watch. Q & A: Violence in South Ossetia. Agosto 15 de 2008. Consultado el 28 de marzo de 2018. Disponible en: https://www.hrw.org/news/2008/08/15/q-violence-south-ossetia.
[198] Manual de Tallin, regla 51, comentario 4.
[199] GEISS, Robin. Óp. Cit., p. 156. El autor pone como ejemplo la banca virtual.
[200] Art. 49.3, Protocolo Adicional I de 1977.
[201] Manual de Tallin, regla 52.

ataque no solo deben tenerse en cuenta durante la fase preparatoria de la operación, sino a lo largo de ella[202].

Esta regla también incluye elementos como la verificación de los sujetos y objetos de ataque, con el fin de proteger a los civiles y sus objetos[203], la elección de medios y métodos que minimicen los efectos adversos contra civiles, así como su muerte o la destrucción de sus objetos[204]. Por otra parte, cuando se elijan objetivos militares legítimos, también debe procurarse el menor daño a las vidas de los civiles y a sus bienes[205].

Se dice que el problema de aplicación de este principio es la falta de conocimiento de los altos mandos militares y en general, de quienes desarrollan las operaciones en el área de combate, pues no tienen suficiente experiencia en el desarrollo de ciberoperaciones. Es evidente que esta falta de pericia constituye un obstáculo para determinar de manera exacta los "ciberobjetivos militares" y los daños colaterales que acarreen estas actividades[206], incluso en tierra, mar o aire.

En suma, debido a los rápidos cambios que se dan en el mundo de la tecnología, existen límites que se pueden fijar a través de la reinterpretación de los principios, puesto que los procesos de codificación son lentos[207]. A lo anterior se suma la dificultad para que los Estados ratifiquen el hipotético

[202] Manual de Tallin, regla 52, comentario 5.
[203] Manual de Tallin, regla 53.
[204] Manual de Tallin, regla 54.
[205] Manual de Tallin, regla 55.
[206] SCHMITT, Michael N. and WATTS, Sean. The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare [En línea]. En: Texas International Law Journal, 2015. Vol. 50. Available at SSRN: https://ssrn.com/abstract=2481629. Consultado el 22 de marzo de 2018, p. 229.
[207] DÍEZ DE VALASCO VALLEJO, Manuel. Instituciones de Derecho Internacional Público. 11ª edición. Madrid: Editorial Tecnos, 1997, p. 114.

instrumento resultante, como se ha comprobado, por ejemplo, con el difícil proceso de ratificación de diversos instrumentos de derecho internacional[208].

En este sentido, debe observarse cuál es la incipiente costumbre internacional que han creado los Estados a lo largo de la influencia de las nuevas tecnologías en el derecho[209].

[208] HENCKAERTS, Jean Marie y DOSWALD-BECK, Louise. Óp. Cit., P. XII.
[209] KELSEY, Jeffrey T. Óp. Cit., p. 1446.

CAPITULO II. LOS CIBERATAQUES

La comunidad jurídica internacional empezó a tomar conciencia sobre la importancia de las ciberoperaciones desde los años 90[210]. En aquel entonces empezó una discusión sobre la aplicación de distintas normas de derecho internacional a este dominio.

No obstante, la discusión sobre la aplicación del DIH no está zanjada. Existe una dicotomía respecto del alcance de la interpretación que debe darse a las normas existentes, es decir, si debe ser amplia o restringida.

Por una parte, la interpretación amplia sería conveniente para los Estados, en la medida que habilitaría a sus fuerzas armadas y demás organismos para realizar ciberactividades más agresivas lo cual, inevitablemente, iría en detrimento de la población civil. Por otra parte, se podría acudir a una interpretación restringida, que limitaría el alcance de las ciberoperaciones y reduciría la posibilidad de atentar contra civiles[211].

A partir del estudio de algunos casos, es posible determinar cómo se pueden aplicar las normas jurídicas que rigen los conflictos armados al ámbito del ciberespacio. Debido a que la existencia de un conflicto armado es requisito *sine qua non* para la aplicación de las mismas, se estudiarán dos tipos de casos.

En primer lugar, se analizarán los ciberataques que tuvieron lugar en el desarrollo del conflicto armado entre Georgia y Rusia durante 2008. En segundo lugar, se analizará el caso de *Stuxnet* en Irán, que resulta polémico

[210] Manual de Tallin, p. 1.
[211] SCHMITT, Michael N. and WATTS, Sean. Op. Cit.

por no desarrollarse en un conflicto armado, pero cuyos efectos podrían haber dado lugar a una confrontación armada.

Estos casos, aunque difíciles de analizar jurídicamente debido a que ningún Estado ha reconocido su responsabilidad por las acciones en el ciberespacio[212], se convierten en un referente para pensar en unas normas jurídicas capaces de responder a los retos del futuro, que inevitablemente van de la mano de la tecnología y sus vicisitudes.

2.1 CIBERATAQUES EN TIEMPOS DE CONFLICTO ARMADO

Aunque el potencial de este tema es amplio para el futuro, no existen, hasta el momento, muchos casos documentados, ni decisiones judiciales o pronunciamientos de organismos internacionales al respecto.

Así, por ejemplo, durante la guerra de Kosovo, se identificaron algunos ataques a través de las tecnologías existentes para aquel entonces. Uno de ellos fue el que llevó a cabo la OTAN sobre medios de comunicación serbios (radio y televisión "RTC"), porque según la organización, estos eran de uso militar y contribuían a la ventaja serbia, razón por la cual, se convertían en un objetivo que ayudaría a debilitar la capacidad militar del país balcánico[213].

Otro ejemplo es el bloqueo de la página web de la Casa Blanca en 1999, con el fin de tomar el control del sistema *Nimitz*, a través del cual se controlaban los portaviones estadounidenses[214]. Si bien este ataque no tuvo

[212] BROWN, Gary y POELLET, Keira. Óp. Cit., p. 33.
[213] KELSEY, Jeffrey T. Óp. Cit., p. 1440.
[214] URUEÑA CENTENO, Francisco J. Ciberataques, la mayor amenaza actual [En línea]. Documento Opinión 09/2015. Instituto Español de Estudios Estratégicos, 16 de enero de 2015. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf. Consultado el 15 de febrero de 2018, p. 16.

consecuencias letales, fue una alerta para revisar la debilidad de los sistemas de ciberseguridad de Estados Unidos.

Los desarrollos tecnológicos existentes hasta el momento también se utilizaron en la primera Guerra del Golfo, en la que se destruyó una central de generación de energía eléctrica de doble uso, con el fin de disminuir la capacidad militar de Irak. En dicho suceso, los efectos del ciberataque fueron más allá de lo militar, puesto que tuvieron efectos generalizados y prolongados para la población civil[215].

Sin embargo, debido a la falta de documentación y al bajo nivel de reflexión que suscitaron estos hechos para la época de su ocurrencia, se hará énfasis en los ciberataques que sufrió Georgia en agosto de 2008.

A) Georgia: ¿los primeros pasos hacia la ciberguerra?

Uno de los casos más recientes y documentados sobre ciberoperaciones es el ataque que sucedió en el conflicto armado internacional entre Rusia y Georgia en 2008. En agosto de ese año, estos dos Estados se enfrentaron por las tensiones existentes en torno al territorio de Osetia del Sur - una provincia separatista de Georgia, ubicada en territorio de frontera con Rusia-. El Estado ruso atacó esta zona, y como consecuencia, Mijaíl Saakashvili – presidente de Georgia- declaró el estado de guerra[216].

---

[215]. WAXMAN, Mathew. Ciberwarfare: is there a need for new law? En: HEINTSCHEL von HEINEGG, Wolff. International Humanitarian Law and New Weapon Technologies. San Remo: International Institute of Humanitarian Law, 2012, p. 145. En este evento resultarían aplicables las normas sobre proporcionalidad y distinción que se desarrollaron en el capítulo I.

[216] Cfr. Agencias. Georgia declara el estado de guerra en el segundo día de la ofensiva del Ejército ruso [En línea]. En: El Mundo, España. Consultado el 29 de marzo de 2018. Disponible en: http://www.elmundo.es/elmundo/2008/08/09/internacional/1218270936.html; MARKOFF, John. Georgia sufre la ciberguerra. En: El País, España. Consultado el 29 de marzo de 2018. Disponible en: https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html.

Fig. 7. Tomada de: Cyber attacks against Georgia: Legal Lessons Identified. Disponible en: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf, p. 67.

En este contexto, Georgia fue víctima de ciberataques con el uso de métodos como la desconfiguración de las páginas web públicas y la denegación de servicios (DDoS)[217]. Se presume que este ciberataque provino de Rusia[218].

A continuación, se presentarán los hechos del conflicto a través de una línea del tiempo:

[217] TIKK, Eneken et al. Cyber attacks against Georgia: Legal Lessons Identified [En línea]. Tallinn: Cooperative Cyber Defense Centre of Excellence, 2008. Disponible en: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf, p. 9. Consultado el 30 de marzo de 2018.
[218] BROWN, Gary y POELLET, Keira. Óp. Cit., p. 34.

Fig. 8. Línea del tiempo sobre ciberataques en Georgia. Gráfico de elaboración propia con base en los hechos descritos por TIKK, Eneken et al. Cyber attacks against Georgia: Legal Lessons Identified. Cooperative Cyber Defense Centre of Excellence, 2008. Disponible en: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf, p. 69-71 y 108-109.

Poco después de los primeros ciberataques, las fuerzas armadas rusas iniciaron ofensivas a través de medios cinéticos en el territorio en disputa[219]. A pesar de las declaraciones del ministro de relaciones exteriores de Georgia, Rusia no reconoció responsabilidad alguna frente a ciberataques, y tampoco se pudo comprobar una relación del gobierno ruso con los mismos, según los análisis de tráfico de datos[220].

A pesar del nivel de interconexión de Georgia[221], se han logrado identificar consecuencias que afectaron los sistemas miliares e incluso a la población civil. Verbigracia, los ataques tuvieron efectos graves sobre los sistemas de defensa aéreos; asimismo, el comando militar de Georgia y el control de sus operaciones pasaron a depender de inseguras plataformas de Google y de páginas del gobierno de Estados Unidos[222]. Además, la denegación de servicios de los servidores oficiales impidieron la comunicación del gobierno con la comunidad internacional y con sus habitantes en una fase crítica del conflicto[223].

Respecto de las afectaciones a la población civil, los hechos del día 13 de agosto son relevantes porque los códigos malignos afectaron el acceso a redes telefónicas y de conexión por banda ancha[224], de manera indiscriminada. Además, el equipo de respuesta ante emergencias

---

[219] RABOIN, Bradley. Op. cit. P. 620.
[220] Tikk, Eneken et al. International Cyber Incidents: legal considerations. Cooperative Cyber Defense Centre of Excellence, Tallin, 2010. Disponible en: http://www.ccdcoe.org/publications/books/legalconsiderations.pdf, p. 79.
Ibid,
[221] TIKK, Eneken et al. Cyber-attacks against Georgia: Legal Lessons Identified. Óp. Cit., p. 5 y ss.
[222] RABOIN, Bradley. Op. cit. P. 619.
[223] Ibíd.
[224] TIKK, Eneken, KASKA, Kadri y VIHUL, Liis. International Cyber Incidents: legal considerations [En línea]. Tallinn: Cooperative Cyber Defense Centre of Excellence, Tallin, 2010. Disponible en: http://www.ccdcoe.org/publications/books/legalconsiderations.pdf. Consultado el 30 de marzo de 2018, p. 101.

informáticas de Estonia (CERT- EE) informó que dos de los principales proveedores de internet dejaron de prestar servicios por varios días[225].

Las consecuencias también fueron evidentes en la prestación de servicios al público, como la banca electrónica, pues el día 18 de agosto, el Banco Nacional de Georgia ordenó a los demás bancos comerciales suspender los servicios de transacciones virtuales[226].

Aunque se desconocen los efectos de los ataques a largo plazo, se hará un análisis de la aplicación del DIH.

B) Derecho aplicable

Los análisis más recientes después de los sucesos ponían en tela de juicio la aplicación del DIH para estos ciberataques, bajo el argumento de la falta de interpretaciones o de normas internacionales que se refirieran de manera explícita a los ciberataques y al régimen de responsabilidad[227].

No obstante, la doctrina evolucionó hasta afirmar que es posible realizar un examen jurídico de los hechos a partir del mencionado régimen. Como prueba de lo anterior, es menester destacar que efectivamente se dio un conflicto armado internacional, conforme a los elementos del art. 2 común a los Convenios de Ginebra de 1949[228].

---

[225] TIKK, Eneken et al. Cyber attacks against Georgia: Legal Lessons Identified. Óp. Cit., p. 15.

[226] TIKK, Eneken et al. Cyber attacks against Georgia: Legal Lessons Identified. Óp. Cit., p. 16.

[227] TIKK, Eneken et al. Cyber attacks against Georgia: Legal Lessons Identified. Óp. Cit., p. 23. Sobre la responsabilidad de los Estados, cfr. SOLCE, Natasha. Óp. Cit. p. 22. En casos de ciberataques, la doctrina dice que debería aplicarse el concepto de “agencia” o de “control total” que el TPY utilizó en el caso Tadic. Se dice que debe evaluarse si una persona es funcionaria del Estado o particular; también debe evaluarse si los hechos pueden calificarse como acciones estatales. Estos criterios no son un impedimento para que, según el análisis en concreto, un Estado pueda ser responsable por tolerar acciones de particulares.

[228] Art. 2 común a los IV Convenios de Ginebra de 1949: “Aparte de las disposiciones que deben entrar en vigor ya en tiempo de paz, el presente Convenio se aplicará en caso de guerra

Así lo afirman expertos como los redactores del Manual de Tallin[229], o *Human Rights Watch* (HRW) [230] en un análisis sobre los hechos del conflicto en el que invitó a los Estados involucrados a respetar el DIH, toda vez que se trataba de un conflicto armado internacional. Así las cosas, la organización invitó a tener en cuenta el Derecho de La Haya, el Derecho de Ginebra y las normas de derecho consuetudinario para la conducción de las hostilidades y la protección de la población civil.

Partiendo de la existencia del presupuesto básico de aplicación del DIH, es decir, un conflicto armado –en este caso, internacional-, la pregunta no es si este es el régimen jurídico aplicable, sino cómo se aplica a los particulares hechos de esta confrontación, pues en ella coinciden dos clases de ataques: los que se hicieron con armamento tradicional, y los ciberataques, que son un medio novedoso.

Debido a la existencia de estos últimos, debe evaluarse su nexo con el conflicto. Existe un debate sobre el alcance de este término, pues por una parte, se considera que existe solo con el hecho de que los ciberataques se desarrollen en un conflicto armado[231]. Por su parte, la segunda posición es más estricta, pues parte de la base de que el DIH solo es aplicable a las ciberoperaciones que efectivamente contribuyan a las hostilidades[232].

declarada o de cualquier otro conflicto armado que surja entre dos o varias Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra.
El Convenio se aplicará también en todos los casos de ocupación total o parcial del territorio de una Alta Parte Contratante, aunque tal ocupación no encuentre resistencia militar.
Si una de las Potencias en conflicto no es parte en el presente Convenio, las Potencias que son Partes en el mismo estarán, sin embargo, obligadas por él en sus relaciones recíprocas. Estarán, además, obligadas por el Convenio con respecto a dicha Potencia, si ésta acepta y aplica sus disposiciones".

[229] Manual de Tallin, regla 20.
[230] Human Rights Watch. Óp. Cit.
[231] Manual de Tallin, regla 30.
[232] Ibíd.

Según el primer criterio, el DIH es aplicable a los hechos, pues el nexo existe en la medida que los ciberataques que sufrió Georgia se dieron en el marco de un conflicto armado internacional. Sin embargo, para satisfacer el criterio más exigente, es necesario evaluar los ciberataques a la luz de sus efectos.

Se puede afirmar que los bloqueos a algunas páginas estratégicas para el gobierno georgiano en el curso de un conflicto, como las de su ministerio de defensa o de relaciones exteriores constituyen un ataque que contribuye a las hostilidades, puesto que se disminuyó la capacidad militar de Georgia para responder ataques en una "fase crítica del conflicto"[233].

En otras palabras, podría hablarse de la neutralización de objetivos militares, en los términos del art. 52 del PA I, toda vez que los ciberataques conllevaron a la inutilización de sitios web estratégicos durante el desarrollo de las hostilidades[234], pues, impidieron la comunicación de la administración con la población civil y con el mundo[235].

Aunque se debe reconocer la dificultad de distinguir los efectos que causaron las ciberoperaciones, de los que causaron los ataques tradicionales[236], si es posible afirmar hubo atentados páginas de bancos comerciales. Según el CIRC[237], estos son objetos civiles; debido a que actualmente también se realizan transacciones a través de la red, la interpretación debería extenderse a su infraestructura cibernética.

[233] GUTIERREZ ESPADA, Cesáreo. Óp. Cit., p. 210.
[234] Art. 52, Protocolo adicional I de 1977; Comité Internacional de la Cruz Roja. XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Óp. Cit., p. 54.
[235] GUTIÉRREZ ESPADA, Cesáreo. Óp cit., p. 210.
[236] TIKK, Eneken, KASKA, Kadri y VIHUL, Liis. Óp. Cit. p. 81.
[237] Comité Internacional de la Cruz Roja. XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Óp Cit., p. 53.

Así pues, se debería tener en cuenta que el DIH se puede aplicar a algunos ciberataques, según su gravedad[238]. Este es un ejemplo de una de las zonas grises que se propuso en el semáforo de aplicación del DIH en el capítulo I. En este sentido, para evaluar esta ciberoperación, debe tenerse en cuenta la gravedad de los efectos adversos directos e indirectos sobre la población civil, pues prima facie, no es un ataque letal que conlleve a daño, muerte o lesiones.

Conforme a los argumentos hasta ahora expuestos, se confirma la aplicación del DIH, por lo cual es posible decir que los atacantes debieron respetar los principios de distinción, proporcionalidad y precaución. Si bien es cierto que en este caso se recalca el problema del doble uso de la infraestructura ciberespacial, se debió tener una especial precaución al momento del diseño de los ataques para evitar en la mayor medida de lo posible daños a dominios de uso exclusivamente civil como los bancos, o los medios de comunicación.

Las soluciones teóricas a este caso contribuirían a encontrar soluciones para casos futuros. Así pues, se destaca la importancia del examen de nuevas armas conforme al art. 36 del PA I, pues los avances en las nuevas tecnologías deben velar por la seguridad de los civiles y su menor grado de afectación.

2.2 ZONAS GRISES: CIBERATAQUES EN TIEMPOS DE "PAZ"

Existen varios ejemplos de ciberoperaciones, que incluso podrían calificarse como ataques. Sin embargo, hay ejemplos que constituyen una zona gris para el derecho internacional y, dentro de este, se encuentra el DIH. Existen casos relativamente recientes, como los ciberataques que tuvieron lugar en Estonia, en Irán o en Corea del Sur. En este tipo de sucesos la pregunta no gira en

[238] Cfr. Manual de Tallin, regla 30.

torno a cómo aplicar las normas de DIH, sino alrededor de él o los regímenes jurídicos aplicables.

Aunque pareciera un asunto del siglo XXI, se dice que el primer ciberataque de la historia sucedió en la Unión Soviética en 1982, cuando se registró la explosión de un oleoducto transiberiano debido a un *malware*. Se dice que este ataque – que presuntamente protagonizó Estados Unidos- avergonzó al Comité Ruso de Seguridad (KGB), lo cual hizo que no se produjera ninguna queja por parte de Rusia[239].

Sin embargo, al igual que en el acápite anterior, se hará énfasis en los casos más recientes para determinar algunos aspectos comunes de los ciberataques, pues a partir de esto se puede determinar cuál es el régimen jurídico aplicable cuando no existe, *de iure* o de facto, un conflicto armado.

A) Stuxnet: un salto hacia las ciberarmas

En 2010 el gusano informático *Stuxnet i*ngresó a las redes de la central de enriquecimiento de uranio de Natanz (Irán), que pertenece al programa nuclear iraní y causó la destrucción de mil centrifugadoras destinadas al proceso de enriquecimiento de uranio[240].

[239] BROWN, Gary y POELLET, Keira. Óp. Cit., p. 33.
[240] ALBRIGHT, David, BRANNAN, Paul y WALROND, Christina. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment [En línea]. ISIS, 2010. Disponible en: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/. Consultado el 14 de marzo de 2018; SÁNCHEZ LOZANO, Martha Liliana. Óp. Cit., p. 180.

Fig. 10. Mapa de instalaciones nucleares de Irán. Imagen obtenida de BBC Mundo. "Las siete instalaciones nucleares iraníes que preocupan a Occidente". Disponible en: http://www.bbc.com/mundo/noticias/2013/10/131015_emplazamientos_nucleares_iranies_preocupan_a_occidente_mxa, consultado el 31 de marzo de 2018.

Stuxnet es gusano informático que apuntan a los sistemas de control, supervisión y adquisición de datos (SCADA), los cuales permiten "la recopilación, control y vigilancia de datos en tiempo real de infraestructuras críticas"[241], tales como plantas de energía eléctrica, represas, sistemas de procesamiento de desechos entre otras operaciones industriales"[242].

El diseño de *Stuxnet* permite que los hackers puedan causar consecuencias en el mundo físico[243]. Este gusano se replica en los computadores que utilizan sistema Windows, a través de controladores lógicos programables (PLC), instala un software y da nuevas instrucciones a las máquinas industriales[244].

[241] SHAKARIAN, Pablo. Stuxnet: revolución de Ciberguerra en los asuntos militares [En línea]. Disponible en: http://www.airpower.au.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s.pdf., p. 50. Consultado el 6 de abril de 2018.
[242] Worm Stuxnet. Disponible en: https://www.symantec.com/es/mx/page.jsp?id=stuxnet. Consultado el 1 de marzo de 2018.
[243] Ibíd.
[244] SHAKARIAN, Pablo. Óp. Cit., p. 50- 51.

Según expertos en ciberseguridad, este virus pretendía afectar la central de energía nuclear de Bushehr o las instalaciones del proceso de enriquecimiento de uranio, situadas en Natanz[245].

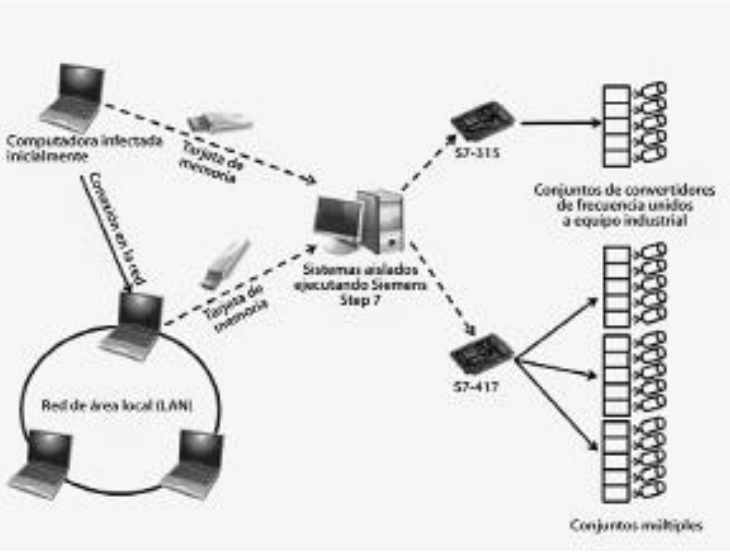

Fig. 11. "Propagación del gusano *Stuxnet.* Tomada de: SHAKARIAN, Pablo. Stuxnet: revolución de Ciberguerra en los asuntos militares. Disponible en: http://www.airpower.au.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s.pdf, p. 52.

Como es usual, nadie ha reconocido la responsabilidad por estos ataques. Sin embargo, prestigiosos periódicos como *The New York Times* han denunciado que dos Estados poderosos militarmente auspiciaron este virus: Estados Unidos e Israel[246]. Según un informe de este periódico, Stuxnet fue el medio para lograr la destrucción de 1000 centrifugadoras IR-1, de las 5000 existentes en la planta de Natanz para el momento del ataque, es decir, aproximadamente una sexta parte[247].

[245] BROWN, Gary y POELLET, Keira. Óp. Cit., pp. 34-35.
[246] SANGER, David. Obama Order Sped Up Wave of Cyberattacks Against Iran [En línea]. The New York Times, june 1 2012. Disponible en: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?hp. Consultado el 14 de marzo de 2018.
[247] Ibid; cfr. ALBRIGHT, David, BRANNAN, Paul y WALROND, Christina. Op. Cit.

Se dice que el objetivo de este “ataque” era evitar que Irán construyera armamento atómico, y que las consecuencias de este virus fueron el retraso de al menos dos años en el programa nuclear del Estado iraní[248].

Es importante resaltar que este ataque se dio sobre infraestructura estratégica para la República Islámica de Irán, dada su apuesta por un programa de energía nuclear independiente[249].

La gravedad de los efectos que causó este virus no radica exclusivamente en los resultados que tuvo en el mundo físico, sino además en la aparente incapacidad de sus creadores para controlarlo, puesto que infectó más redes alrededor del mundo en Estados como “Indonesia, India, Azerbaiyán, Pakistán y Malasia[250]”.

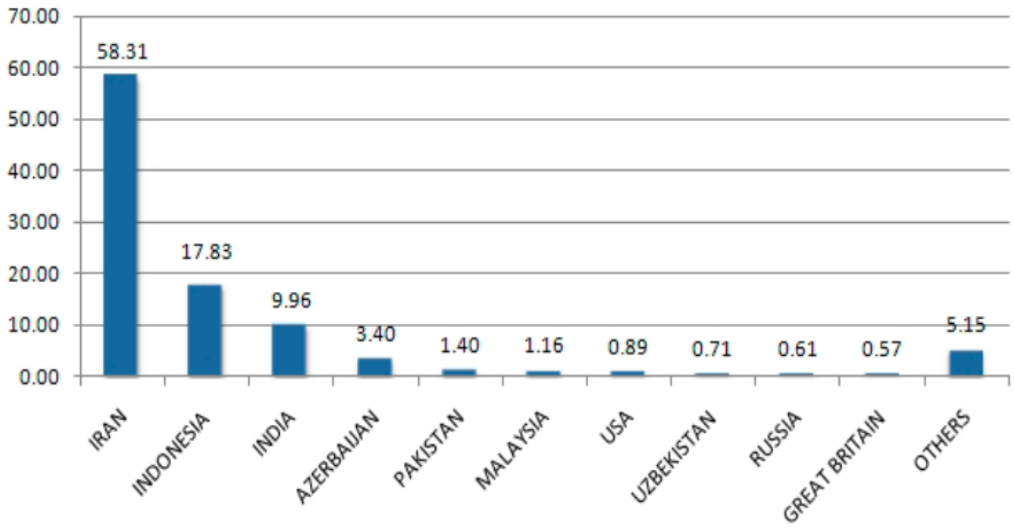

Fig. 12. Distribución Geográfica de la Infección por Stuxnet. Fuente: Symantec.

[248] LEJARZA ILLARO, Eguskiñe. Óp. Cit., p. 9.
[249] BROWN, Gary y POELLET, Keira. Óp. Cit.
[250] Ibid, p. 10.

En el mismo sentido, se determinó que este gusano informático solo actúa en dispositivos “configurados de una manera muy específica” En este caso, solo actuaba sobre dispositivos que funcionaran con él.

Frente a dichos hechos, surgieron dudas acerca de la posición de Irán. Su gobierno, en cabeza de Mahmud Ahmadineyad, hizo referencia a daños que sufrieron algunas centrifugadoras de uranio, sin entrar en detalles sobre la ubicación, el número o la causa, más allá de expresar que se debió a un programa malicioso[251].

Lo anterior genera enormes dificultades para analizar este ataque desde el derecho. Se dice que si la destrucción de esta infraestructura obedeciera a ataques tradicionales por parte de otro Estado, por ejemplo, una explosión con misiles de crucero, la respuesta de Irán hubiera sido distinta[252], e incluso hubiese dado lugar a un conflicto armado internacional.

En ese orden de ideas, es necesario determinar estos hechos dan o no lugar a un conflicto armado, y por consiguiente, si procede la aplicación del DIH u otros regímenes jurídicos.

B) Derecho aplicable

En este punto no se busca desarrollar una respuesta unívoca sobre el derecho aplicable, sino proponer, según el punto de vista de algunos expertos en materia de ciberespacio, cuál sería la interpretación del derecho más adecuada para tratar fenómenos como el de *Stunxnet*.

[251] BROWN, Gary y POELLET, Keira. Óp. Cit., p. 34-35
[252] Ibíd.

A pesar de que ningún Estado "ha calificado públicamente una operación cibernética hostil real como tal"[253], se asumirá que existe responsabilidad por parte de uno o varios Estados, en aras de proponer respuestas desde el derecho internacional.

En primer lugar, debe analizarse si la destrucción de centrifugadoras de uranio constituye o no un conflicto armado de carácter internacional, o al menos se puede considerar como un paso inicial para desencadenarlo.

En este sentido, cabe resaltar que un conflicto armado internacional es aquel que involucra un enfrentamiento entre dos Estados, mediante la violencia armada[254]. La interpretación de este tipo de conflictos en el ciberespacio corresponde a la existencia de hostilidades con categoría de ciberoperaciones entre dos o más Estados[255].

Así las cosas, se ha dicho que en caso de ciberataques entre Estados, podría existir un conflicto armado internacional[256]. Aquí surge una zona gris, pues no es posible determinar el carácter de "ataque armado" [257] de este suceso.

Sin embargo, existen dos aproximaciones a los conflictos que permiten hablar de la existencia efectiva de ellos a partir de ciberataques. Por una parte, existe una aproximación desde la responsabilidad objetiva, según la cual un ataque

[253]Comité Internacional de la Cruz Roja. XXXII. Óp. Cit., p. 51.
[254] Cfr. Art. 2 común a los Convenios de Ginebra de 1949; Art. 1, Protocolo I de 1977; SALMÓN, Eizabeth. Óp. Cit., p. 83 y ss; ICTY. Prosecutor v. Dusko Tadic. Óp. Cit., párr. 70.
[255] Manual de Tallin, regla 22.
[256] SCHMITT, Michael N., Classification of cyber conflict. En: Journal of Conflict and Security Law, 2012. Vol. 17, Issue 2, p. 252.
[257] Manual de Tallin, regla 22, comentario 14.

en la infraestructura crítica de un Estado puede alcanzar la categoría de un ataque armado según las consecuencias en la infraestructura nacional[258].

Por otra parte, se habla de una aproximación basada en los efectos o las consecuencias. Aquí el análisis gira en torno a los efectos generales o globales que tiene un ciberataque sobre un Estado, teniendo en cuenta los ataques que se mencionaron en las zonas grises del capítulo anterior, como infraestructura bancaria[259].

En este orden de ideas, Droegue[260] sostiene que se deben observar los efectos según la severidad del ciberataque. Así pues, los daños que *Stuxnet* causó sobre las centrifugadoras podrían dar pie a un conflicto armado debido a sus efectos. La autora considera que si el medio hubiese sido un ataque aéreo que implicara uso de fuerza cinética y se hubiera presentado el mismo resultado, la reacción de Irán hubiese sido distinta[261].

Al respecto, es valioso el concepto de ciberguerra que propuso el CICR en su XXXII Conferencia Internacional (2015), donde afirmó que esta puede ser una serie de operaciones que se usen en el marco de un conflicto armado o "el empleo de medios cibernéticos en ausencia de operaciones cinéticas cuando su uso se equipara a un conflicto armado"[262].

Conforme a lo anterior, podría plantearse la opción del surgimiento de conflictos armados a través de ciberataques. En consecuencia, códigos como

[258] RICHARDSON, John. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield [En línea]. (July 22, 2011). Disponible en: https://ssrn.com/abstract=1892888. Consultado el 12 de abril de 2018, p. 16.
[259] Ibíd.
[260] DROEGUE, Cordula, Óp. Cit., p. 548.
[261] Ibíd.
[262] Comité Internacional de la Cruz Roja. XXXIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Óp. Cit., p. 51.

Stuxnet deberían someterse al examen jurídico de nuevas armas, toda vez que causan efectos adversos, entre ellos, daños potenciales a la salud de los seres humanos, porque se dirigen contra infraestructura que contiene fuerzas peligrosas[263].

Siguiendo la propuesta del CICR, deberían tenerse en cuenta pruebas científicas sobre los efectos de *Stuxnet* o códigos similares en las personas, su impacto en la salud, los índices de mortalidad en el terreno y la mortalidad posterior que causaría un ataque con una ciberarma de esta naturaleza, los futuros cambios psicológicos o fisiológicos que acarrearía su uso, entre otros[264].

Además del examen jurídico del arma, este asunto debe analizarse desde los principios del DIH y la infraestructura afectada. A lo largo de estas páginas ha dicho que los principios de distinción, proporcionalidad y precaución se pueden interpretar conforme al entorno cibernético.

Para empezar, es difícil afirmar que se violó el principio de distinción. Por una parte, Brown[265] sostiene los hechos del caso *Stuxnet* tienen carácter de ataque, y por tanto, existió una violación del principio de distinción del DIH, pues este gusano informático puede replicarse en cualquier computador con acceso a Windows, sin importar si su uso es civil o militar. Sin embargo, expertos en tecnología[266]han determinado que a pesar de que este virus puede ingresar en cualquier dispositivo, actúa exclusivamente sobre PLC controlados por los software S7- 315 y S7- 417 de la compañía Siemens.

---

[263] Recordar lo expuesto sobre las infraestructuras que contienen fuerzas peligrosas a lo largo del presente trabajo.
[264] Cfr. LAWAND, Kathleen. Óp. Cit., p. 18.
[265] BROWN, Gary D. Why Iran Didn't Admit Stuxnet Was an Attack [En línea]. En: JFQ, 2011. Issue 63. Disponible en: https://ssrn.com/abstract=2485181, p. 71.
[266] BRANDSTETTER, Thomas. “Stuxnet Malware” CIP Seminar, Siemens, November, 2010. En SHAKARIAN, Pablo. Op. Cit, p. 51.

Otro matiz que se presenta en la aplicación del principio de distinción al caso *Stuxnet* es el tipo de infraestructura objeto del ciberataque. En principio, podría sostenerse que los ciberatacantes desconocieron la prohibición de atentar contra infraestructura que contenga fuerzas peligrosas. Debe recordarse que un mal manejo de las centrales de energía nuclear puede tener consecuencias nefastas en la salud de los seres humanos, consecuencia de la radiación nuclear, los daños al medio ambiente e incluso sobre las personas de manera directa[267].

Existe, sin embargo, una posición contraria a este argumento, según la cual la central de Natanz era un objetivo militar legítimo, pues existe la posibilidad de doble uso: tendría el fin civil de producir energía, y un probable uso para el desarrollo de armamento nuclear[268]. Si esto es así, sería posible atacar este tipo de infraestructura siempre y cuando no se causen efectos indiscriminados[269].

Ante estas dificultades, tiene sentido la posición del vaciamiento del principio de distinción en el ciberespacio, que se planteó en el capítulo anterior.

Esto permite realizar una aproximación al caso desde el principio de proporcionalidad, pues los efectos de un ataque importan a la hora de analizar los daños colaterales que involucren a la población civil. Si bien es cierto que *Stuxnet* está configurado de tal manera que solo infecta computadores relacionados con infraestructura industrial, sí se produjeron efectos colaterales, pues la destrucción física que causó el ataque es ostensible.

---

[267] RICHARDSON, John. Óp. Cit., p. 29.
[268] Ibid.
[269] SCHULMAN, Mark. Discrimination in the Laws of Information Warfare. En: Columbia Journal of Transnational Law, 1999. , Vol 37.

En este sentido, Ambos[270] sostiene que el principio de proporcionalidad ofrece mayor protección que el principio de distinción en el contexto del ciberespacio, pues el ultimo, según este autor, es estático y poco flexible.

Así las cosas, vuelve a ser importante el dilema del doble uso, puesto que si la central nuclear se toma como un bien civil, la destrucción de las mil centrifugadoras IR-1 es un ataque desproporcional, pues teniendo en cuenta las fuerzas peligrosas que albergan este tipo de instalaciones, es posible prever afectaciones sobre los civiles, como ya se explicó con anterioridad. Además, no está clara una hipotética ventaja militar.

Por el contrario, si la central fuera eventualmente un objetivo militar, entrarían en juego otras consideraciones, similares a las que se explicaron en el análisis del principio de distinción. Sobre este punto se ha dicho que no se evidencian graves daños colaterales que afecten a la población civil, ni en sus bienes[271].

En este orden de ideas, es necesario resaltar de nuevo la importancia del contenido del concepto de "daño colateral", pues en el contexto del ciberespacio, este debería tener una interpretación más amplia, que incluya la pérdida de funcionalidad, bien sea como efecto directo o indirecto del ataque[272].

Por último, también debe analizarse la aplicación del principio de precaución, Como se afirmó con anterioridad, esta norma implica el deber tomar todas las precauciones posibles, con el fin de evitar efectos adversos sobre la población civil. En teoría, la precisión de *Stuxnet* permitiría pensar que se tomaron las precauciones debidas para evitar daños a la población civil.

[270] AMBOS, Kai. Óp. Cit., p. 18.
[271] RICHADRSON, Óp. Cit., p. 38.
[272] AMBOS, Kai. Óp. Cit., p. 18.

Un aspecto cuestionable es que *Stuxnet* destruyó bienes de carácter civil, con el agravante de tratarse de infraestructura que contiene fuerzas peligrosas. Dicha conducta, no parece respetar a la población civil; verbigracia, no se pueden calcular los futuros daños que la liberación de radiación pueda tener en la salud del personal que trabaja en la planta.

Puesto que las precauciones deben ser razonables[273], sería interesante precisar aspectos como la cantidad de uso de la fuerza[274], la estructura y diseño de la ciberarma – siguiendo los parámetros del examen jurídico para nuevas armas del artículo 36 del PA I, y las consecuencias que esta podría tener en distintos aspectos de la vida humana, con el fin de realizar un juicio más preciso en torno de este último principio.

Lo anterior da cuenta de que este principio enfrenta dificultades similares a las del principio de distinción en lo que respecta al problema del doble uso, lo cual no quiere decir que sea imposible de aplicar.

[273] Manual de Tallin, sección 7, p. 164.
[274] SÁNCHEZ LOZANO, Martha Liliana. Óp. Cit., p. 155.

CONCLUSIONES

Los ejemplos que se abordaron en esta investigación dan cuenta de un cambio en los medios y métodos de combate que, sin duda, anuncian nuevas formas de conflicto alrededor del mundo. Frente a este escenario, es posible realizar dos grandes conclusiones:

Primera. El DIH debe adaptarse a los rápidos cambios que plantea el ciberespacio. En este sentido, urge dotar de nuevos significados a conceptos cardinales de esta rama del derecho internacional público, por ejemplo, conflicto armado, daño colateral y ventaja militar.

Esto se puede lograr a través de dos vías: la primera consiste en realizar una nueva interpretación de los principios y normas de esta rama del derecho internacional público que los llene de tal contenido y alcance, que sean límites claros a la acción de los distintos actores de un conflicto.

La segunda vía para hacer frente a este nuevo escenario de confrontación es elaborar nuevas normas convencionales, que procedería en caso de que la reinterpretación normas consuetudinarias resulte insuficiente y genere vacíos normativos.

Los Estados pueden llegar a un consenso a través de un instrumento de derecho convencional donde plasmen, conforme a las prácticas que se han desarrollado, límites a las ciberoperaciones. Sin embargo, se advierte cierta dificultad frente a esta opción, debido a que los procesos de codificación tienden a ser lentos.

Cualquiera de las alternativas planteadas debería partir no solo de las normas existentes, sino, además, de otras fuentes como las estrategias de ciberseguridad y ciberdefensa de diferentes Estados, obras académicas como el Manual de Tallin, entre otros. Lo anterior, con el fin de determinar cuál es la práctica nacional en materia de uso del ciberespacio, y cuáles son los mecanismos de respuesta ante ciberataques.

Por último, es importante resaltar que resulta imperioso hacer el examen de las ciberarmas como nuevas armas, en virtud del artículo 36 del PA I, con el fin de que la comunidad internacional tenga pautas claras sobre su licitud, su composición, y demás elementos resaltados en este trabajo.

Segunda. La cooperación es fundamental si se quiere tener control sobre actividades ilegitimas en el ciberespacio. Además de la interpretación de las normas y la eventual creación de nuevo derecho convencional, es evidente que se requiere cooperación de diferentes tipos: entre expertos en diferentes materias, entre el sector público y privado, y entre Estados, debido a la magnitud del ciberespacio y de las actividades que en él se desarrollan.

Como se evidenció a lo largo de este trabajo, las nuevas tecnologías van más allá de lo militar, por ende, se requiere que el sector privado coopere en la elaboración de estrategias de seguridad y defensa, puesto que tienen más y mejor manejo de estos conocimientos, que guardan especial importancia a la hora de proteger infraestructuras críticas.

También es necesario que los Estados cooperen entre sí, tal como lo han venido haciendo los países de la Unión Europea y de la OEA, con el fin de diseñar estrategias trasnacionales que les permitan tener altos estándares de prevención, y mecanismos de ataque coordinados y respetuosos del derecho internacional.

A su vez existen otros actores sociales llamados a colaborar en la construcción de respuestas para el futuro. Con esto se hace referencia a la academia y a organizaciones internacionales, incluso aquellas no gubernamentales, para que sigan realizando estudios como el Manual de Tallin o iniciativas similares, con el fin de tener mayor conocimiento sobre las actividades que se desarrollan en el ciberespacio, los avances en nuevas tecnologías y su incidencia en la vida humana.

Por último, la cooperación también es muy importante para realizar una tarea que no da tregua: el examen de las ciberarmas según el art. 36 del PA I. Solo a través de un trabajo interdisciplinario se pueden trazar límites a los combatientes que estén pensando en utilizar ciberarmas como medios de combate. Se debe dejar claro que el ciberespacio y las demás herramientas que se dan en este entorno no son sinónimo de libertad absoluta debido a la falta de regulación.

Por esta razón, urge que se llegue a un consenso sobre la aplicación del derecho a este nuevo dominio, pues es una manera de evitar que los avances en nuevas tecnologías se usen de manera indebida y terminen causando consecuencias atroces a la humanidad.

BIBLIOGRAFÍA

DOCTRINA

ANDREW LEWIS, James. Estrategias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos. Banco Interamericano de Desarrollo, 2016.

BUGNION, Francois. Derecho de Ginebra y Derecho de La Haya. Revista Internacional del Comité de la Cruz Roja, 2001.

CERVELL HORTAL, María José. La legítima defensa en el derecho internacional contemporáneo. Valencia: Tirant lo Blanch, 2017. P. 300.

COMISIÓN EUROPEA. Comunicado de prensa: Estado de la Unión 2017 – Ciberseguridad: la Comisión intensifica la respuesta de la UE a los ciberataques. Bruselas, 2017.

DÍEZ DE VALASCO VALLEJO, Manuel. Instituciones de Derecho Internacional Público. 11ª edición. Madrid: Editorial Tecnos, 1997.

DOMÍNGUEZ VASCOY, Jerónimo. Aplicación del Derecho Internacional Humanitario a las operaciones en el ciberespacio. En: RODRÍGUEZ-VILLASANTE Y PRIETO, José Luis, LÓPEZ SÁNCHEZ, Joaquín. Derecho Internacional Humanitario. 3 ed. Valencia: Tirant lo Blanch, 2017. ISBN: 978-84-9119-871-0.

DROEGUE, Cordula. Get off my cloud: cyber warfare, international humanitarian law and the protection of civilians. En: International Review of the Red Cross, 2012. Volume 94, No. 886. p. 540.

FELIU ORTEGA, Luis. La ciberseguridad y la ciberdefensa. En: Monografías del CESEDEN, No. 126. Madrid: Centro Superior de Estudios de la Defensa, 2012.

GEISS, Robin. Humanitarian aspects of cyber warfare. En: HEINTSCHEL von HEINEGG, Wolff. International Humanitarian Law and New Weapon Technologies. San Remo: International Institute of Humanitarian Law, 2012.

GÓMEZ DE AGREDA, Ángel. El ciberespacio como escenario de conflicto. Identificación de amenazas. En: El ciberespacio. Nuevo escenario de confrontación, Monografías del CESEDEN no. 126, febrero de 2012.

GUTIÉRREZ ESPADA, Cesáreo. La ciberguerra y el derecho internacional. En: MARTÍNEZ PÉREZ, Enrique. Las amenazas a la seguridad internacional hoy. Valencia: Tirant lo Blanch, 2017.

HENCKAERTS, Jean Marie y DOSWALD-BECK, Louise. El Derecho Internacional Humanitario Consuetudinario. Volumen I, normas. Buenos Aires: Comité Internacional de la Cruz Roja, 2007.

KASKA, Kadri, OSULA, Anna-Maria, STINISSEN, LTC Jan. The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013.

KELLO, Lucas. The virtual weapon and international order. New Heaven [CT]: Yale University Press, 2017.

KELSEY, Jeffrey T. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. En: Michigan Law Review, 2008. Volume. 106.

LÓPEZ DE TURISO Y SÁNCHEZ, Javier. El ciberespacio como escenario de conflicto. Identificación de amenazas. En: Ministerio de Defensa de España. El ciberespacio. Nuevo escenario de confrontación. Madrid: Monografías del CESEDEN no. 126, 2012.

MELZER, Nils. Guía para interpretar la noción de participación directa en las hostilidades según el Derecho Internacional Humanitario. Ginebra: Comité Internacional de la Cruz Roja, 2010.

_____ y KUSTER, Etienne. International Humanitarian Law: a comprehensive introduction. Geneva: International Committee of the Red Cross, 2016.

PÉREZ GONZÁLEZ, Manuel. El derecho internacional humanitario frente a la violencia bélica. En: RODRÍGUEZ-VILLASANTE Y PRIETO, José Luis, LÓPEZ SÁNCHEZ, Joaquín. Derecho Internacional Humanitario. 3 ed. Valencia: Tirant lo Blanch, 2017. ISBN: 978-84-9119-871-0.

RABOIN, Bradley. Corresponding evolution: international law and the emergence of cyberwarfare. En: Journal of the National Association of Administrative Law Judiciary, 2011. Vol. 31, 602.

ROBAYO GALVIS, Wilfredo, Elementos del Estado: el territorio. En: CORREA HENAO, Magdalena, RAMÍREZ CLEVES, Gonzalo Andrés y OSUNA PATIÑO, Néstor (editores). Lecciones de Derecho Constitucional: tomo I. Bogotá: Universidad Externado de Colombia, 2017.

RODRÍGUEZ- VILLASANTE Y PRIETO, José Luis. Fuentes del Derecho Internacional Humanitario. En: RODRÍGUEZ-VILLASANTE Y PRIETO, José Luis, LÓPEZ SÁNCHEZ, Joaquín. Derecho Internacional Humanitario. 3 ed. Valencia: Tirant lo Blanch, 2017. ISBN: 978-84-9119-871-0.

ROSCINI, Marco. World Wide Fare – Jus ad bellum and the Use of CyberForce. En: Max Planck Yearbook of United Nations Law, 2010. Volume 14.

SALMÓN, Elizabeth. Introducción al Derecho Internacional Humanitario. Lima: Pontificia Universidad Católica del Perú- Comité Internacional de la Cruz Roja. 3a ed, 2014.

SÁNCHEZ LOZANO, Martha Liliana. Los conflictos armados en el ciberespacio: retos del Derecho Internacional Humanitario. Bogotá: Grupo Editorial Ibáñez, 2018.

SCHMITT, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013.

_____. Classification of cyber conflict. En: Journal of Conflict and Security Law, 2012. Vol. 17, Issue 2.

_____. Wired warfare: computer network attack and jus in bello. En: RICR, 2002. Vol 84, No. 846.

SHACKELFORD, S.J. Who Controls Cyberspace? Analyzing Cyber Regulation through Polycentric Governance. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge: Cambridge University Press, 2014.

SOLCE, Natasha. The Battlefield Of Cyberspace: The Inevitable New Military Branch—The Cyber Force. En: Albany Law Journal od Science & Technology, 2008. Vol. 18, No. 293.

UIT, Rec UIT- T X. 1205. Sector de Normalización de las Telecomunicaciones de la UIT (04/2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Seguridad en el ciberespacio-ciberseguridad. Aspectos generales de la ciberseguridad, abril de 2008.

VAN CREVELD, Martin. From 2000 BC to the present, revised ed., The Free Press, New York, 1991

VELA ORBEGOZO, Bernardo. Lecciones de derecho internacional. Tomo I. Bogotá: Universidad Externado de Colombia, 2012.

WAXMAN, Mathew. Ciberwarfare: is there a need for new law? En: HEINTSCHEL von HEINEGG, Wolff. International Humanitarian Law and New Weapon Technologies. San Remo: International Institute of Humanitarian Law, 2012.

DOCUMENTOS EN INTERNET

Agencias. Georgia declara el estado de guerra en el segundo día de la ofensiva del Ejército ruso [En línea]. En: El Mundo, España. Consultado el 29 de marzo de 2018. Disponible en: http://www.elmundo.es/elmundo/2008/08/09/internacional/1218270936.html

ALBRIGHT, David, BRANNAN, Paul y WALROND, Christina. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment [En línea]. ISIS, 2010. Disponible en: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/. Consultado el 14 de marzo de 2018.

AMBOS, Kai. Responsabilidad penal internacional en el ciberespacio [En línea]. En: InDret: revista para el análisis del derecho, 2015. No. 2. [Fecha de consulta: 18 de abril de 2018] Disponible en: http://www.department-ambos.uni-goettingen.de/data/documents/Veroeffentlichungen/epapers/Responsabilidad%20ciberespacio%20InDret.pdf

Australian Government. Department of the Prime Minister and Cabinet. Cyber security strategy. https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

BBC Mundo. “Las siete instalaciones nucleares iraníes que preocupan a Occidente” [En línea]. Disponible en: http://www.bbc.com/mundo/noticias/2013/10/131015_emplazamientos_nucleares_iranies_preocupan_a_occidente_mxa, consultado el 31 de marzo de 2018.

BROWN, Gary D. Why Iran Didn't Admit Stuxnet Was an Attack [En línea]. En: JFQ, 2011. Issue 63. Disponible en: https://ssrn.com/abstract=2485181.

BROWN, Gary y POELLET, Keira. El derecho internacional consuetudinario del Ciberespacio [En línea]. En: Air and Space Power Journal, 2013. Disponible en: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2013/2013-1/2013_1_06_brown_s.pdf. Consultado el 28 de febrero de 2018.

CANDAU ROMERO, Javier. Estrategias nacionales de ciberseguridad. Ciberterrorismo. En: JOYANES AGUILAR, Luis. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Madrid: Instituto español de estudios estratégicos e Instituto Universitario “General Gutiérrez Mellado, 2010. Disponible en: http://www.ieee.es /Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

CARO BEJARANO, María José. Alcance y ámbito de la seguridad nacional en el ciberespacio. En: JOYANES AGUILAR, Luis. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Madrid: Instituto español de estudios estratégicos e Instituto Universitario “General Gutiérrez Mellado, 2010. Disponible en: http://www.ieee.es/Gal erias/fichero/cuadernos/CE_149_Ciberseguridad.pdf.

CCM. ¿Qué es un proxy? En: https://es.ccm.net/faq/2755-que-es-un-proxy

Comando General de las Fuerzas Militares de Colombia. Plan Estratégico Militar -PEM- 2030., 2015. Disponible en: https://cdn.fac.mil.co/sites/d efault/files/plan_estrategico_militar_2030.pdf.

COMITÉ INTERNACIONAL DE LA CRUZ ROJA. Colombia: tres expertos discuten los desafíos del DIH. 11 de septiembre de 2015. Disponible en: https://www.icrc.org/es/document/colombia-tres-expertos-discuten-los-desafios-actuales-del-dih. Consultado el 19 de marzo de 2018.

DÖRMANN, Knut. Applicability of the Additional Protocols to Computer Network Attacks [En línea]. En: International Committe of the Red Cross. International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, November 17-19, 2004. Disponible en: https://www.icrc.org/eng/resources/do cuments/misc/68lg92.htm.

EUROPEAN COMMISSION. Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace. Joint communication to the European Parliament, the council, the European economic and social committee and the committee of the regions. Disponible en: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_ comm_en.pdf.

GLOBAL CYBER SECURITY CAPACITY CENTRE. Cybersecurity Capacity Maturirty Model for Nations (CMM). University of Oxford, 2016. Disponible en: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

Gobierno de España. Estrategia de ciberseguridad nacional [En línea]. Madrid, 2013 Disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf. Consultada el 16 de marzo de 2018.

Gobierno de España. Estrategia de Ciberseguridad Nacional, 2013. Disponible en: www.dsn.gob.es/es/file/146/download?token=Kl839vHG

Gobierno de España. Publicación del Manual de Tallín sobre “Ley Internacional en la Ciberguerra”. Portal de Tecnología e Innovación del Ministerio de Defensa, 22 de enero de 2013. Disponible en: https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59. Consultado el 18 de abril de 2018.

Human Rights Watch. Q & A: Violence in South Ossetia. Agosto 15 de 2008. Disponible en: https://www.hrw.org/news/2008/08/15/q-violence-south-ossetia. Consultado el 28 de marzo de 2018.

International Committee of the Red Cross. Cyber warfare and international humanitarian law: The ICRC's position [En línea]. Junio de 2013. Disponible en: https://www.icrc.org/eng/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf. Consultado el 18 de febrero de 2018.

JOYANES AGUILAR, Luis. Introducción. Estado del arte de la ciberseguridad en Ciberseguridad. En: Retos y amenazas a la seguridad nacional en el ciberespacio [En línea]. Madrid: Instituto español de estudios estratégicos e Instituto Universitario “General Gutiérrez Mellado, 2010. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf.

Kapersky lab daily. ¿Qué es un botnet? En: https://www.kaspersky.es/blog/que-es-un-botnet/755/

KASPERSKY Eugene. The Flame That Changed the World [En línea]. 14 de junio de 2012. Disponible en http://eugene.kaspersky.com/2012/06/14/the-flame-that-changed-the-world/#more-2717. Consultado el 3 de febrero de 2018.

KUTT NEBRERA, Alexander. La importancia de dominar los *global commons* en el siglo XXI [En línea]. Documento marco. Instituto Español de Estudios Estratégicos, 2015. Disponible en: http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf

LAWAND, Kathleen. Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos. Medidas para aplicar el artículo 36 del Protocolo adicional I de 1977. Ginebra: Comité Internacional de la Cruz Roja, 2006. Disponible en: https://www.icrc.org/spa/assets/files/other/icrc_003_0902.pdf

LEJARZA ILLARO, Eguskiñe. Ciberguerra, los escenarios de confrontación [En línea]. Documento de opinión. Instituto Español de Estudios Estratégicos, 2014. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO182014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf.

LEWIS, James A., TIMLIN, Katrina. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. Center for Strategic and International Studies. UNDIR Resources, 2011. Disponible en: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

LIIVOJA, Rain. Technological change and the evolution of the law of war. En: International Review of the Red Cross, 2015. No. 900. Disponible en: https://www.icrc.org/es/international-review/article/los-cambios-tecnologicos-y-la-evolucion-del-derecho-de-la-guerra.

MARKOFF, John. Georgia sufre la ciberguerra. En: El País, España. Consultado el 29 de marzo de 2018. Disponible en: https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html.

MELZER, Nils. Ciberwarfare and international law [En línea]. UNIDIR Resources, 2011. Disponible en: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Consultado el 26 de marzo de 2018.

Ministry of Economic Affairs and Communication, Estonia. Cyber Security Strategy 2014-2017, 2014. Disponible en: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

OEA/Ser.K/XXXVIII CES/dec.1/03 rev. Organización de Estados Americanos. Declaración Sobre Seguridad en Las Américas, 28 octubre 2003. Disponible en: www.oas.org/csh/spanish/documentos/cp12364s04.doc

OEA/Ser.L/V/II CIDH/RELE/INF.17/17. Comisión Interamericana de Derechos Humanos. Estándares para una internet libre, abierta e incluyente. Relatoría Especial para la Libertad de Expresión. 15 de marzo 2017. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

REGUERA SÁNCHEZ, Jesús. Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario [En línea]. Grupo de Estudios en Seguridad Internacional, Universidad de Granada. Marzo 18 de 2015. Disponible en: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario. Consultado el 19 de enero de 2018.

República de Colombia. Departamento Nacional de Planeación. Documento CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa, 14 de julio de 2011. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

República de Colombia. Departamento Nacional de Planeación. Política Nacional de Seguridad Digital, documento CONPES 3854 de 2016. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Revista Semana. ¿Qué es un Malware y cómo se puede prevenir? En: https://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3. Consultado el 20 de abril de 2018.

RICHARDSON, John. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield [En línea]. (July 22, 2011). Disponible en: https://ssrn.com/abstract=1892888. Consultado el 12 de abril de 2018.

ROBLES CARRILLO, Margarita. El ciberespacio: presupuestos jurídicos para su ordenación [En línea]. En: Revista Chilena de Derecho y Ciencia Política. Enero- abril, 2016. Vol. 7, no 1. Disponible en: http://portalrevistas.uct.cl/index.php/RDCP/article/view/1025.

ROSENBERG, Matthew, CONFESSORE, Nicholas and CADWALLADR, Carole. How Trump Consultants Exploited the Facebook Data of Millions [En línea]. The New York Times, 17 de marzo de 2018. Disponible en: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Consultado el 25 de abril de 2018.

SANGER, David. Obama Order Sped Up Wave of Cyberattacks Against Iran [En línea]. The New York Times, june 1 2012. Disponible en: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?hp. Consultado el 14 de marzo de 2018.

SCHMITT, Michael N. and WATTS, Sean. The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare [En línea]. En: Texas International Law Journal, 2015. Vol. 50. Available at SSRN: https://ssrn.com/abstract=2481629. Consultado el 22 de marzo de 2018.

SCHMITT, Michael N. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed [En línea]. *En: Harvard International Law Journal*. Vol 54, 2012. Disponible en: http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf

SCHWAB, Klaus. El reto de dar forma a la Cuarta Revolución Industrial. En: Project Syndicate [En línea]. Enero 11 de 2016. Disponible en: https://www.project-syndicate.org/commentary/fourth-industrial-revolutio

n-human-development-by-klaus-schwab-2016-01/spanish?barrier=accessreg. Consultado el 20 de abril de 2018.

SCHWAB, Klaus. Cuatro principios de liderazgo de la Cuarta Revolución Industrial. World Economic Forum [En línea]. 12 de octubre de 2016. Disponible en: https://www.weforum.org/es/agenda/2016/10/cuatro-principios-de-liderazgo-de-la-cuarta-revolucion-industrial/. Consultado el 19 de abril de 2018.

SHAKARIAN, Pablo. Stuxnet: revolución de Ciberguerra en los asuntos militares [En línea]. Disponible en: http://www.airpower.au.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s.pdf., p. 50. Consultado el 6 de abril de 2018.

Techtarget. Malware. Definition. En: https://searchsecurity.techtarget.com/definition/malware.

Techtarget. Proxy hacking. Definition. En: https://searchmicroservices.techtarget.com/definition/software.

Techtarget. Software. Definition. En: https://searchmicroservices.techtarget.com/definition/software.

TICERHURST, Rupert. La Cláusula de Martens y el derecho de los conflictos armados [En línea]. 31 de marzo de 1997. Revista Internacional de la Cruz Roja, 1997. Disponible en: https://www.icrc.org/spa/resources/documents/misc/5tdlcy.htm

TIKK, Eneken et al. Cyber attacks against Georgia: Legal Lessons Identified [En línea]. Tallinn: Cooperative Cyber Defense Centre of Excellence, 2008. Disponible en: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf. Consultado el 30 de marzo de 2018.

TIKK, Eneken, KASKA, Kadri y VIHUL, Liis. International Cyber Incidents: legal considerations [En línea]. Tallinn: Cooperative Cyber Defense Centre of Excellence, Tallin, 2010. Disponible en: http://www.ccdcoe.org/public

ations/books/legalconsiderations.pdf. Consultado el 30 de marzo de 2018.

TORRES SORIANO, Manuel R. El dilema de interpretación del ciberespacio [En línea]. Instituto Español de Estudios Estratégicos. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO03-2018_Dilema_Ciberespacio_ManuelRTorres.pdf.

UIT. Sobre la Unión Internacional de Telecomunicaciones (UIT). En: https://www.itu.int/es/about/Pages/default.aspx

URUEÑA CENTENO, Francisco J. Ciberataques, la mayor amenaza actual [En línea]. Documento Opinión 09/2015. Instituto Español de Estudios Estratégicos, 16 de enero de 2015. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf. Consultado el 15 de febrero de 2018.

WILLIAMS, Christopher. How Egypt shut down the internet. The Telegraph [En línea]. Enero 28 de 2011 Disponible en: https://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html. Consultado el 20 de abril de 2018.

WORLD ECONOMIC FORUM. El fascinante mapa donde puedes ver el recorrido oculto de los cables marinos que nos conectan a internet [En línea]. 17 de mayo de 2017. Disponible en: https://www.weforum.org/es/agenda/2017/05/el-fascinante-mapa-donde-puedes-ver-el-recorrido-oculto-de-los-cables-marinos-que-nos-conectan-a-internet/?utm_content=buffer59801&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer. Consultado el 15 de febrero de 2018.

Worm Stuxnet. Disponible en: https://www.symantec.com/es/mx/page.jsp?id=stuxnet. Consultado el 1 de marzo de 2018.

FUENTES DE DERECHO INTERNACIONAL

Asamblea General de Naciones Unidas. Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, 2010. A/65/2010.

Asamblea General de Naciones Unidas. Función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme. 23 de diciembre de 1997. A/RES/52/33.

Asamblea General de Naciones Unidas. Función de la ciencia y la tecnología en el contexto de la seguridad internacional y el desarme. 4 de enero de 1999. A/RES/53/73.

Asamblea General de Naciones Unidas. Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. 20 de noviembre de 2000. A/RES/55/28.

Asamblea General de Naciones Unidas. Respeto de los derechos humanos en los conflictos armado, 1968. Res. 2444 de 1968.

CIJ International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996.

Comité Internacional de la Cruz Roja. El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos. XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Ginebra, 2011. 31IC/11/5.1.2.

Comité Internacional de la Cruz Roja. El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos. XXXII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Ginebra, 2015. 32IC/15/11.

Comité Internacional de la Cruz Roja. Mejorar la protección en los conflictos armados y en otras situaciones de violencia armada. XVIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja. Ginebra, 2003.

Convenios de Ginebra de 1949.

General Assembly. United Nations. Developments in the field of information and telecommunication in the context of international security. Report of the Secretary-General, 15 July 2011, UN Doc. A/66/152.

ICTY. Prosecutor v. Dusko Tadic´, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995.

Naciones Unidas. Convención sobre la prohibición del desarrollo, la producción, el almacenamiento y el empleo de armas químicas y sobre su destrucción, 1994.

Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977.

Protocolo II adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional, 1977.

NORMATIVA

Reino de España. Ley 8 de 2011.

REPÚBLICA DE COLOMBIA. Comisión de Regulación de Telecomunicaciones. Resolución 2058 de 2009.