“ATAQUES EN EL CIBERESPACIO BAJO EL DERECHO HUMANITARIO Y POLÍTICAS DE CIBERSEGURIDAD COMO FORMA DE DEFENSA”

por

Iris Paredes Roibás

bajo la dirección de

Profesora Elvira Rodríguez Redondo

XIII Edición Máster en Protección Internacional de los Derechos Humanos (Universidad de Alcalá de Henares)

INDICE

INDICE DE ABREVIATURAS

IoT: Internet of Things

ICRC/CICR: International Comité of the Red Cross/Comité Internacional de la Cruz Roja

OTAN: Organización del Tratado del Atlántico Norte

DoS/DDoS: Denial of Service/Distributed Denial of Service

GGE: Gubernamental Group of Experts

GPS: Global Position System

GIE: Grupo Internacional de Expertos

CERT-CN: Centro de Emergencia de Respuesta Temprana-Centro Nacional

RBN: Russian Business Network

AIEA: Agencia Internacional de la Energía Atómica

CCD o CoE: Cooperative Ciber Defence o Center of Excellence

CIRCC: Computer Incident Response Capability Center

ERIE: Equipos de Respuesta a Incidencias de Emergencia

NIS: Network Information System

ECRC: European Cybersecurity Research and Competence Centre

RESUMEN: El ciberespacio es un dominio del que se tiene gran dependencia hoy en día, esto lo convierte en un objetivo muy atractivo para la mayoría de ataques maliciosos que se llevan a cabo tanto por agentes estatales como no estatales ¿Un ciberataque al sistema que controla las compuertas de una presa es equiparable a uno que suponga detonar explosivos con la misma finalidad?, ¿podemos aplicar las leyes actuales del derecho humanitario a la ciberguerra? Tras abordar un estudio de la aplicabilidad de los principios generales del derecho humanitario a este tipo de ataques, se analizarán las normativas que se han llevado a cabo por diferentes organismos internacionales para enfrentarse a este creciente nido de debate que es el ciberespacio y los ataques que en él se dan.

ABSTRACT: *They cyberspace is a domain which creates a big dependency on itself nowadays, this makes it a very atractive object for the mayority of malicious attack been carried by both, state and non-state agents. Is a cyberattack the one that is been carried against the system that controls a damn comparable to one consisted on detonate explosive with the same outcome? Can we apply current international humanitarian law on cyberwar operations? After developing a study on applicability of the principles of international humanitaria law, international organizations's documents and dispositions will be analyzed in order to set ground in this emerging debate about cyberspace and operations in it.*

Key words: humanitarian law, cyberspace, cyberwar, principles of humanitarian law, cyberattacks, cyberoperations, defense, capacity building, cybersecurity, international cooperation.

I. INTRODUCCIÓN

El propósito de este trabajo es el estudio de diferentes ejemplos de ciberataques que se han venido sucediendo en la última década y las políticas de ciberseguridad que los organismos internacionales han llevado a cabo para responder ante esta amenaza tan creciente. La sociedad en la que vivimos depende fuertemente de las tecnologías y entre esos avances, se encuentra internet. Este espacio digital se ha convertido en indispensable para nuestro día a día; muchos son los usos para los que aplicamos esta red de comunicación desde que nos despertamos hasta que nos acostamos: despertador, mensajería instantánea y emails, gps, cámara fotográfica, compras, transferencias bancarias, consultas generales. Casi todos los dispositivos electrónicos actuales están conectados a la red global lo que, junto con el "Internet of Things" (IoT), hace que se creen cada vez más vulnerabilidades de las que tanto actores estatales como no estatales puedan aprovecharse.

En 2007, varios servicios electrónicos privados y públicos de Estonia fueron víctima de una ciberoperación maliciosa. Estos ataques coordinados contra un país enfocaron la atención internacional en los riesgos que implica la alta dependencia de los estados y su población al ciberespacio[1]. La humanidad se encuentra en una era apasionante para los avances científicos y tecnológicos, internet ha conectado a la gente y el conocimiento de una manera que ninguna otra tecnología había hecho antes, pero todas las nuevas tecnologías suponen nuevos desafíos y a la vez nuevos riesgos.

Ya que el tema de estudio es joven y novedoso se utilizará una metodología científica exploratoria que permita dar una visión general aproximativa respecto a la realidad del ciberespacio. Se llevará a cabo primero una descripción sistemática de los principios generales del derecho humanitario, para continuar aplicándolos a las

[1] Toomas Hendrik Ilves, Presidente de la República de Estonia, Prólogo de "Manual de Tallin sobre ley internacional aplicable a ciberoperaciones 2.0" (Ed. Cambridge) 2017.

características de casos hipotéticos de ciberataques a través de una breve referencia a las normas en vigor de derecho internacional y su aplicabilidad en el caso concreto.

Principalmente, la pregunta a plantearnos son las siguientes: ¿un ciberataque se podría considerar un ataque o amenaza a la independencia política e integridad territorial de un Estado como prohíbe el artículo 2.4 de la Carta de Naciones Unidas? ¿activaría esta violación del artículo 2.4. la cláusula de legítima defensa del artículo 51 de la Carta?

No siempre se desarrolla la ley paralelamente a la tecnología por lo que, ante la aparición de estos avances debe plantearse la cuestión de si las leyes actuales son aplicables o si, por el contrario, necesitamos nuevos cuerpos legales que regulen el ciberespacio.

La relevancia académica de este estudio se centra en la importancia de llegar a una comprensión común de las implicaciones del ciberespacio para poder promover sus ventajas como un ambiente pacífico, abierto, estable y accesible a las tecnología de la comunicación y la información[2].

Con la intención de que el trabajo sea fiel al estado actual de la materia, las fuentes que se utilizan serán siempre resoluciones y documentos oficiales de organismos internacionales como Naciones Unidas, la OTAN o el Comité Internacional de la Cruz Roja, así como Institutos de Derechos Humanos de varios países. También se hará uso de artículos académicos y periodísticos, y manuales de referencia y reconocida importancia como el Manual de "Tallín sobre la aplicación de la ley Internacional a ciberoperaciones 2.0" (Ed. Cambridge 2017). Este manual, aunque solo es una fuente subsidiaria de Derecho Internacional de acuerdo con el artículo 38 del Estatuto de la CIJ y el Derecho consuetudinario, es la referencia más autoritaria en la materia.

Se comenzará hablando sobre origen del derecho humanitario para regular una guerra clásica hasta llegar a una ciberguerra, poniendo de manifiesto cómo las tecnologías han influenciado su desarrollo y como el escenario bélico ha ido evolucionando.

---

[2] Bert Koenders, Ministerio de Asuntos Exteriores de Netherland, Prólogo de "Manual de Tallin sobre ley internacional aplicable a ciberoperaciones 2.0" (Ed. Cambridge) 2017

Segundo, el trabajo desarrollará un análisis de las características de un ciberataque aplicando los principios generales del derecho humanitario de distinción, precaución y proporcionalidad; también se estudiará cómo la soberanía de los estados y su jurisdicción se ven afectadas con el uso del ciberespacio.

En el tercer apartado, y quizás el más práctico se tratarán algunos de los ciberataques más importantes de la última década (Estonia, Georgia, Irán y virus Wannacry) y que son, además, los que nos han abierto el interrogante de si cabe la posibilidad de una ciberguerra en internet. Se estudiará el contexto histórico y geopolítico para entender las posibles razones de cada ataque y cómo se respondió ante él.

En el último apartado se entrará a desarrollar un breve análisis de las políticas y actuaciones de organismos internacionales en reacción a los diversos escenarios que se pueden dar en la actualidad, cómo una perspectiva defensiva; es decir, las grandes potencias internacionales buscan principalmente mejorar su sistema de ciberdefensa a través de medidas de ciberseguirdad, en lugar de implementar el desarrollo de estrategias ofensivas.

El último apartado se dedicará a las conclusiones finales que se ha llegado tras realizar este trabajo de investigación.

II. EVOLUCIÓN DEL DERECHO HUMANITARIO HASTA LA CIBERGUERRA

A) Nociones previas sobre derecho humanitario.

El Derecho Internacional Humanitario se ubica dentro del Derecho Internacional Público. Desde el origen de los tiempos se vislumbró la necesidad de regular las relaciones entre diferentes Estados soberanos, los cuales tenían autonomía y soberanía suficiente para llevar a cabo el uso de la fuerza si lo creían conveniente sin sometimiento, en principio, a ninguna regla previamente acordada entre los actores. Sin embargo, era necesario, teniendo en cuenta los intereses propios del Estado acordar una regulación común de los conflictos bélicos que pudiesen surgir, compatible con la convivencia y que contuviese los terribles efectos de la guerra.

El derecho internacional humanitario son las normas que regulan el uso de armas, los métodos de guerra, las que tratan de proteger a las víctimas de los conflictos bélicos ya sean civiles o combatientes, participen o no en las hostilidades o hayan dejado de hacerlo. El bien supremo que respalda es la vida y la dignidad de la persona[3]. Es importante regular todo el sistema de normas de una sociedad civilizada pero la guerra, y su naturaleza de estado "excepcional", hace que las prioridades de protección difieran ligeramente de las de una situación común.

Durante toda la historia de la humanidad se han ido desarrollando reglas, que independientemente del origen sociocultural, político o ideológico de quien las redactó contenían las pautas para regular situaciones conflictivas. Evitando así, que la justicia fuese tomada por cada uno. La evolución del derecho de la guerra ha ido desarrollándose, a la par que el ser humano aumentaba sus capacidades de preparación

[3] International Comité Red Cross, "What is humanitarian law?" Advisory service article on international humanitarian law, Ed. ICRC (Geneva 2004) pag 1. Acceso a la web: 26/01/2018 [16:56] https://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf

ante el conflicto[4]. Hasta que no aparecieron los primeros navíos, no se concebía la posibilidad de trasladar la guerra de la tierra al mar, y lo mismo sucedió cuando se pusieron en activo los primeros aeroplanos en combate. Un avance como ese en la tecnología, que otorga semejante ventaja al que lo posee pasó a ser regulado para evitar así un uso indiscriminado y barbárico contra el enemigo. Cuanto mayor era la capacidad militar de un Estado, mayor era su poder soberano[5] y su ventaja estratégica militar.

Es por eso que surge el Derecho Humanitario, para regular jurídicamente esa realidad alterada donde las violaciones de derechos se concentran mayoritariamente sobre la vida, la dignidad de las personas y su seguridad. En palabras de Nelson Mandela: "*Los Convenios de Ginebra* [los cuáles conforman parte del Derecho Humanitario] *continúan recordándonos con gran fuerza la obligación que tenemos de cuidarnos mutuamente*".

Para llevar a cabo una regulación correcta y preocupada por proteger a la vida principalmente, el Derecho Humanitario se basa en una serie de principios básicos que lo apoyan en unas bases humanistas, centradas en la protección de las personas.

La humanidad y la guerra han evolucionado de la mano a lo largo de la Historia. El ejército fue creado para proteger a la población y ya en la Antigüedad existía una diferencia entre el combatiente y el no combatiente. A la hora de proteger a no combatientes como mujeres o niños se fueron creando normas consuetudinarias basadas en concepciones morales como el honor o respeto.

Los relatos de Henry Dunant en su obra "Recuerdo de Solferino", conmovieron a la sociedad del siglo XIX, y dieron lugar a ese primer movimiento humanitario con la creación del Comité Internacional de la Cruz Roja (CICR o ICRC)[6].

Durante este siglo y por impulso del ICRC, se crea la Conferencia Diplomática de Suiza donde se firma el Convenio de Ginebra de 22 de agosto de 1864, para el

---

[4] SWINARSKI, CHRISTOPHE, "Principales nociones del Derecho Internacional Humanitario como sistema internacional de protección de la persona" ed. Instituto Interamericano de DDHH, Cátedra Jean Pictet (San José, 1990), pag. 12.

[5] Consulta web ICRC, artículo "Principales nociones e institutos del Derecho Internacional Humanitario como sistema de protección de la persona humana" Acceso a web: 26/01/2018 [16:17] https://www.icrc.org/spa/resources/documents/misc/swinarsky.htm

[6] BRAUMAN, Rony, *L'action humanitaire, Dominos Flammarion*, Paris, 1995, ps.15-34

mejoramiento de la suerte de los militares heridos de los ejércitos en campaña. Aquí comienza a vislumbrarse una joven idea de lo que será derecho humanitario. Aunque por ahora solo se protege a las víctimas combatientes.

No se busca con el derecho humanitario más que proteger a una sociedad del entorno bélico que les rodea. El deseo de reducir los efectos de los conflictos armados al mínimo posible, es el fundamento del derecho humanitario. Cuando se da una situación de conflicto armado, ya sea internacional o nacional se intenta limitar violaciones y proteger a las víctimas; todo ello sin juicios políticos o jurídicos en cuanto al motivo y razón que impulsó la acción armada[7].

Más adelante, los Convenios de Ginebra de 1949, serán los que codifiquen la mayor parte del derecho humanitario internacional. El contexto histórico tuvo grandísima influencia en la redacción de estos tratados. La Segunda Guerra Mundial alcanzó niveles de violencia y de violaciones de derechos humanos nunca antes vistos en la historia de la Humanidad; la violencia entre combatientes internacionales a gran escala se vio unida a la violencia contra la población civil. Los campos de concentración, los exterminios llevados a cabo por los nazis y los horrores de la guerra sacudieron la moral de sociedad internacional de la época; lo que llevo a la creación de los Convenios de Ginebra para impedir que crímenes semejantes se pudiesen repetir. Estas Convenciones estuvieron rodeadas de un alto nivel de consenso e interés por parte de los Estados Contratantes alcanzando nivel de ratificación.

Pero no debemos olvidar que las Convenciones de Ginebra de 1949 y el derecho que recogen son hijas de su momento histórico y cultural. Nacieron tras una guerra mundial clásica de ejércitos y soldados, de combatiente contra combatiente, donde las víctimas pasaron a ser también los civiles. Las consecuencias de estas masacres fueron una tendencia humanista preocupada por los efectos de la guerra.

Por otro lado, al hablar del derecho humanitario y su contexto de los conflictos armados, no podemos olvidar de mencionar el llamado "Derecho de la Haya". Este derecho surge de las Convenciones de la Haya de 1899 y 1907 donde se recoge el Derecho de la Guerra, es decir, la conducción de hostilidades. Podemos decir, por tanto,

---

[7] GUTIERREZ PONSE, Hortensia DT., *"Elementos del Derecho Internacional Humanitario",* Edit. Eudeba, Buenos Aires 2015, pag. 15.

que el derecho de la Haya es un derecho anterior al conflicto, que estructura cómo debe llevarse a cabo diferenciando entre combatientes y no combatientes, definiendo objetivos militares, la conducción de ataques, así como los principios en los que se deben basar estos ataques.

Ambos derechos, Ginebra y La Haya, se compaginan a la hora de estudiar el derecho en conflictos bélicos. La Corte Internacional de Justicia concluyó que:

> "Estas dos ramas del derecho aplicable en los conflictos armados han desarrollado vínculos tan estrechos que se considera que, en forma gradual, han formado un único sistema complejo, hoy llamado derecho internacional humanitario. Las disposiciones de los Protocolos adicionales de 1977 expresan y dan prueba de la unidad y la complejidad de ese derecho [10][8]".

Algo que ha caracterizado el avance de los tiempos es, ante todo, el gran desarrollo tecnológico de los últimos años. Avance que también afecta, y se ve afectado por el derecho. Desde un punto de vista humanitario, y en el estudio de la guerra, el escenario bélico ha cambiado por completo.

Esta evolución conduce tanto a una mejora de la calidad de vida gracias a la tecnología y las comodidades que nos aporta, sin embargo, a su vez, aumenta el alcance destructor de la Guerra. José Saramago, en relación con el rápido desarrollo de las capacidades bélicas y sus consecuencias, decía, en "Memorial del Convento" que:

"*Un hombre nunca sabe cuándo la guerra acaba. Dice, Mira, se acabó, y de repente no se acabó, vuelve a empezar, y viene diferente, la muy puta, aún ayer eran floreos de espada y son hoy cañonazos, aún ayer se derrumbaban murallas y hoy se desmoronan ciudades, aún ayer se exterminaban países, y hoy se revientan mundos, aun ayer morir era una tragedia y hoy es una banalidad el que se evapore un millón* […]".

Con todo esto el autor del trabajo quiere hacer ver que la evolución del Derecho Humanitario ha ido evolucionando al igual que las tecnologías y avances de la época. Tanto el Derecho de Ginebra como el Derecho de la Haya son derecho estructurados

[8] Op. Consultiva de la Corte Internacional de Justicia del 8 de julio de 1996 sobre la licitud de la amenaza o del empleo de armas nucleares.

para sus épocas. De la misma manera que se redactó el Derecho del Mar cuando comenzaron a surgir conflictos en relación a cómo regular las actuaciones llevados a cabo en él, se regularon los diferentes tipos de armamentos que fueron apareciendo como minas anti personas o armas químicas tras ser desarrolladas.

Con la aparición del ciberespacio y sus posibilidades, se abrió una nueva tecnología con ventajas e inconvenientes a la que el derecho humanitario se debe adaptar. Las guerras con las que se crearon los Convenios de Ginebra y de la Haya han quedado apartadas a otro tiempo; el campo de batalla que presenció Henry Dunant en Solferino es hoy muy diferente El ciberespacio se configura, por lo tanto, como un nuevo campo de batalla; y al igual que sucedió con el espacio terrestre, marítimo y aéreo, se deben contemplar las posibilidades que aporta y las consecuencias de uso como método o medio de guerra.

Con el aumento de ciberataques y crímenes en el ciberespacio por parte de actores no estatales, así como de gobiernos, ha crecido, como debe ser, el debate en torno a este nuevo campo. Con la aparición de internet se creó una red mundial de ordenadores interconectados que ha acabado por convertirse en un elemento casi indispensable para la vida moderna[9].

Además, el ciberespacio se ha convertido en un campo de acción para los Estados los cuales, preocupados por la seguridad nacional y política, han llevado a cabo operaciones en el ciberespacio. Esta finalidad política o de seguridad nacional es lo que diferencia un "ciber-crimen" llevado a cabo por un actor no-estatal (como puede ser el bullying online, fraude a través de la red o robo de datos personales o identidad), de un "ciberataque" llevado a cabo por un Estado (como en los casos que más adelante se mencionaran sobre ciberataques a Estonia o Georgia)[10].

B) Tecnología y conflictos bélicos en referencia al ciberespacio

---

[9] DOREY GABRIELLE, "*Cyberspace: the new battlefield?", Ed. online Centre International pour la paix et les droits de l'homme*" (May 2017) Acceso a la web: 26/01/2018 [17:40] www.cipadh.org/en/cyberspace-new-battlefield

[10] HATHAWAY O., and CROOTOF R., "The law of Cyberattack" (2012), Faculty Scholarship Series. Paper 3852. http://digitalcommons.law.yale.edu/fss_papers/3852

La gran parte de los avances tecnológicos llegan al sector militar o de defensa mucho antes que a las manos de los consumidores y usuarios civiles. T.K. Derry y T.I. Williams en "Historia de la Tecnología" señalan al hablar de los diferentes usos y el descubrimiento del hierro, lo siguiente: "[…] *pero no debemos caer en la exageración y la anticipación. El nuevo metal se usó primero para hacer armas; después para fabricar azadas y hachas y picos para granjas y minas; finalmente, para las herramientas que hemos descrito*."

Al igual que nuestra sociedad cambia, también lo hacen los métodos para la guerra. Son pocos los países con capacidad económica para desarrollar nuevas tecnologías. Generalmente los países menos desarrollados o con menos recursos económicos, no pueden acceder a este tipo de tecnologías, con las que se pueden conseguir ataques más específicos, con menos coste como el que supone la movilización de ejércitos y la ocupación de territorios. Esto hace que el enemigo, no siempre un Estado, decida atacar a la población.

Generalmente, este distanciamiento entre una sociedad desarrollada que observa la guerra "desde su casa" y una sociedad menos desarrollada en el terreno, da una sensación que deshumaniza al enemigo viéndosele más como un criminal que como un combatiente. Esto lleva una deshumanización de la guerra y debate de juicio moral[11].

Esta situación trae a colación la "mentalidad PlayStation"; es decir, situar a un soldado de la generación *Call of Duty* en frente de una pantalla sujetando un joystick, pero ahora, en lugar de situarse en una guerra virtual sin bajas, se encuentra en un escenario real donde las víctimas mueren. Se debe plantear la cuestión de si esa frivolización de la guerra, ese alejamiento de las consecuencias reales de su acción, está rebajando el valor de la vida[12].

El progreso tecnológico cambia la guerra; al principio solo existía el campo de batalla terrestre, y posteriormente surgió la posibilidad de trasladar la batalla tanto al mar como al aire. Gracias al desarrollo de las comunicaciones, surgió la posibilidad de

---

[11] BERNARD, VINCET, "Comentario Editorial", *International Review of the Red Cross* (Summer 2012), Volume 94 Number 886, pag. 457 https://www.icrc.org/en/international-review/new-technologies-and-warfare

[12] ALSTON, PHILIP and SHAMSI, HINA, "*A killer above the law*?", The Guardian (febrero 2010) Vol. Opinion on Afghasnistan.

interceptar comunicaciones o incluso la presencia de un submarino enemigo; esto otorgó gran ventaja estratégica y, a la vez, distanció a los combatientes de sus objetivos[13]. Este desarrollo de las comunicaciones ha dado como resultado final internet y con ello la pregunta de si podemos considerar este dominio como un lugar donde puede darse un conflicto bélico, de la misma manera que sucede con el mar, el aire y la tierra.

Es por esto que, en las últimas décadas, el ciberespacio ha pasado a formar parte de una de las mayores preocupaciones de los gobiernos en cuanto a seguridad y defensa se refiere. Desde que en 2009 Estados Unidos ordenara la creación de un cibercomando, más de 100 países han optado por crear unidades de defensa y seguridad en el ciberespacio[14].

Esta redefinición de la guerra y sus componentes, hace que también nos planteemos redefinir los conceptos de a quién se considera combatiente, bajo qué requisitos se considera que se ha realizado un ataque, qué o cuáles son los objetivos militares, etc. La información es poder y hoy más que nunca, los bancos de datos, por ejemplo, deberían ser considerados como objetivos militares. Estos almacenes de datos generalmente están situados en servidores o *clouds* a los que, con las nuevas tecnologías se puede acceder fácilmente y casi desde cualquier parte del mundo simplemente con un ordenador y conexión a internet.

Muchos años han pasado ya desde que se redactaron los Convenios de Ginebra y de la Haya, y en todo este tiempo el incesante avance de la tecnología ha superado con creces la evolución del marco legal que define y regula el derecho de la guerra y la protección de las víctimas. Tanto es así que a día de hoy se plantean cuestiones imposibles de imaginar en el siglo pasado.

En oposición, la tecnología a su vez nos permite mejorar la solución de situaciones de una manera que no se creería posible hace años. Desde la posibilidad de documentar crímenes de guerra a través de vídeos grabados desde smartphones particulares,

---

[13] GERMAIN, ERIC, "*Out of sight, moral issue in the globalization of the battlefield*", International Review of the Red *Cross* (2015), 97 (900), The evolution of warfare. Pag. 1065–1097.
[14] HARRISON, FERGUS, "*Waging war in peacetime: Cyber attacks and international norms", The Interpreter* (2015), Madrid 10 de enero de 2017 [13:37] https://www.lowyinstitute.org/the-interpreter/waging-war-peacetime-cyber-attacks-and-international-norms

recopilar pruebas y evidencias de desplazamientos de personas a través de imágenes vía satélite, hasta la capacidad de registrar y responder a desastres naturales en los que las ONGs pueden actuar, se ha visto beneficiada por el incremento del intercambio de información vía ciberespacio. La mayor ventaja de éste ha venido siendo la inmediatez de la respuesta de la comunidad ante la información circulante vía Twiter, Facebook o blogs de noticias[15].

Al mismo tiempo debemos plantearnos preguntas sobre el tipo de regulación y las situaciones que se pueden dar cuando las nuevas tecnologías al alcance de todos, y la guerra se unen en el mismo encuadre. Por ejemplo, al hablar del ciberespacio, nos encontramos con una tecnología que abarca tanto a militares en dependencias del Ejército de turno, como a civiles en sus casas, como a actores no-estatales como bandas criminales, grupos armados o terroristas.

La universalidad que ocupa el ciberespacio, y su común acceso, provoca que un ciberataque pueda afectar no solo a las instalaciones del Ejército, sino también al resto de la población que navega por el mismo canal. Una operación en el ciberespacio de este tipo puede ser llevada a cabo por un software enviado a un ordenador desde otro, desde cualquier parte del mundo. La variedad de actores que pueden perpetrar el ataque hace que los motivos detrás de los mismos sean igual de variados.

Antes de pasar al estudio que llevaremos a continuación sobre los ataques en el ciberespacio y su análisis, debemos recordar cuatro aspectos característicos en relación al uso del ciberespacio[16]:

En primer lugar, como ya hemos dicho, su uso está alcance tanto de civiles como de combatientes.

En segundo lugar, las consecuencias de un ciberataque pueden darse tanto en el mundo virtual (roba de datos) como en el mundo real (inutilización del sistema de

---

[15] SINGER, PETER W., "*Interview with Peter W. Singer*" en respuesta a la pregunta "Can new technologies benefit the humanitarian community?", *International Review of the Red Cross* (Summer 2012), Volume 94 Number 886, pag. 474. https://www.icrc.org/en/international-review/new-technologies-and-warfare

[16] BACKSTROM, ALAN and HENDERSON, IAN, "*New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews*", International Review of the Red Cross (Summer 2012), Volume 94 Number 886, pag. 503 https://www.icrc.org/en/international-review/new-technologies-and-warfare

funcionamiento de una infraestructura de energía o mediante la contaminación de aguas de uso público bloqueando una depuradora).

En tercer lugar, el estudio de la ciberguerra y los ciberataques deben ser tenidos en cuenta dentro del marco legal del derecho humanitario (si se dieran durante un conflicto armado) y el derecho de los derechos humanos (si se diera fuera de un conflicto armado); a su vez, se podría analizar si este ataque supone un ataque armado o no, con la consiguiente posibilidad del uso de fuerza como forma de autodefensa.

Y, por último, la determinación la autoría o incluso la procedencia del ataque, lo que implica una dificultad añadida en el contexto del ciberespacio.

III. CIBERATAQUES. ANALISIS EN CONEXCIÓN CON EL DERECHO INTERNACIONAL HUMANITARIO

A) Principio de distinción

1. Aproximación al concepto y su acogida en el DIH

El principio de distinción entre objetivos militares y civiles es una viga maestra del Derecho Humanitario. Establece la necesaria distinción entre civiles y combatientes, tanto personas como objetivos. La concepción de este principio la podemos encontrar recogida en el artículo 48 del Protocolo I adicional a los Convenios de Ginebra:

> "A fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las Partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares".

Como se desprende de la definición, el objetivo de este principio es garantizar el respeto y la protección de los civiles. Se pretende que las hostilidades se conduzcan contra objetivos militares y combatientes con la menor interferencia en la vida de la población civil.

Esta idea de "inmunidad de la población civil" en los conflictos bélicos encuentra su precedente inmediato en la Conferencia de San Petersburgo de 1868 para

prohibir ciertos proyectiles en tiempos de guerra, cuando se consideró que la única finalidad legítima que los Estados deben proponerse durante la guerra/conflicto armado es el debilitamiento de las fuerzas militares del enemigo[17]. Esto no resta protección a los combatientes que tiene sus derechos regulados en el Estatuto del Combatiente o Prisionero de Guerra en el Título III, Sección II del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales.

Conocida la necesidad de distinción, no debemos olvidar que este impedimento de atacar a personas civiles fuera del combate, desaparece cuando los civiles pasan a formar parte de él, convirtiéndose en combatientes.

El Reglamento de la Haya en su artículo 25 ya prohibía "*atacar* o bombardear, *cualquiera que sea el medio que se emplee*, ciudades, aldeas, habitaciones o edificios que no estén defendidos". En otros Protocolos[18], así como en las Convenciones de Ottawa sobre Minas Antipersona de 1997[19], también se presenta este principio de distinción.

Por otro lado, La Corte Penal Internacional, en su Reglamento también se pronuncia sobre esta distinción entre civiles y combatientes al establecer en su artículo 8.2.b.i y ii. que:

> "b) Otras violaciones graves de las leyes y usos aplicables en los conflictos armados internacionales dentro del marco establecido de derecho internacional, a saber, cualquiera de los actos siguientes: i) Dirigir intencionalmente ataques contra la población civil en cuanto tal o contra personas civiles que no participen directamente en las hostilidades; ii) Dirigir intencionalmente ataques contra bienes civiles, es decir, bienes que no son objetivos militares."

Para entender el alcance de este principio en la Comunidad Internacional debemos valorar el alto nivel de ratificación de todos estos instrumentos. El Comité

---

[17] Extracto de la Conferencia de San Petersburgo de 29 de Noviembre a 11 de Diciembre de 1868. Acceso a la web: 11/01/2018 [12:15] https://www.icrc.org/spa/resources/documents/treaty/treaty-declaration-1864-st-petersburg.htm

[18] Protocolo II de la Convención sobre ciertas armas convencionales convencionales (1980), art. 3.2; Protocolo II enmendado de la Convención sobre ciertas armas convencionales convencionales (1996), art 3.7; Protocolo III de la Convención sobre ciertas armas convencionales convencionales (1980), art. 2.1;

[19] Convención de Ottawa (1997), Preámbulo

Internacional de la Cruz Roja de la mano de varios autores como Jean-Marie Henckaerts y Louise Doswald-Beck manifiestan la aceptación de este principio consuetudinario[20]. La práctica reiterada de los Estados en respeto de este principio han llevado a la plasmación del mimos en diferentes tratados, recogiéndose también en Resoluciones de la Asamblea General de las Naciones Unidas que estableció que el principio de distinción es aplicable a todos los conflictos armados sin distinción entre aquellos de origen nacional o internacional[21].

El Protocolo I adicional a los Convenios de Ginebra de 1949 en el Título III, Sección II, redacta el Estatuto del Combatiente. Este Protocolo establece en el artículo 43 que las fuerzas armadas serán:

> "1. Las fuerzas armadas de una Parte en conflicto se componen de todas las fuerzas, grupos y unidades armados y organizados, colocados bajo un mando responsable de la conducta de sus subordinados ante esa Parte, aun cuando ésta esté representada por un gobierno o por una autoridad no reconocidos por una Parte adversa. […]".

Es decir, se considera combatiente a toda persona que forme parte de las hostilidades dentro de un mando militar organizado subordinado una de las partes. Por otro lado, se considerará población civil toda persona a la luz del artículo 50 del Protocolo I, es decir toda persona que no pertenezca a fuerzas armadas parte de las hostilidades.

Por otro lado, para el estudio que se hará en este trabajo, debemos considerar también la clasificación de objetos militares y civiles y su distinción, ya que un ciberataque puede ser ejecutado o llevado a cabo a través de un ordenador personal o desde instalaciones militares.

Existe una prohibición de atacar bienes civiles en el Protocolo Enmendado II sobre ciertas Armas Convencionales de 1996. Cuando bienes civiles se vean afectados

---

[20] Jean-Marie Henckaerts y Louise Doswald-Beck, "El derecho internacional humanitario Vol. 1", Editorial ICRC Centro de Apoyo y Comunicación para Latinoamerica y el Caribe (Buenos Aires 2007) pag. 65

[21] Resolución de AG. Naciones Unidas 2444 (XXIII), aprobada por unanimidad, sin votos en contra o abstenciones.

por un ataque, este hecho no tendrá consideración de hecho ilícito siempre y cuando se dirija contra un objetivo militar; además los daños causados no podrán ser excesivos y desproporcionales[22].

2. Análisis del principio en relación a las características de un ciberataque

Este principio de distinción analizado anteriormente resulta de difícil aplicación en el entorno del ciberespacio. La utilidad del ciberespacio es universal, esta red es utilizada de igual manera por militares como civiles; para explicarlo de una manera sencilla, supongamos que ambos navegan en el mismo mar, aunque con distintas naves, por lo que la posibilidad de que los civiles se vean afectados por un conflicto entre diferentes actores es posible. Además, estos actores pueden ser Estatales, es decir, Gobiernos y sus subordinados militares o policiales: y no-estatales como bandas criminales, organizaciones terroristas, criminales solitarios, activistas e incluso corporaciones privadas. Todos ellos con diferentes intereses y motivaciones.

En una guerra al uso, en el mundo físico, la posibilidad de identificar al combatiente y al civil es más sencilla a través de insignias, portabilidad de armas, banderas o algún tipo de distintivo. En el mundo virtual esa distinción se camufla tras la pantalla, por lo que es difícil saber quién son los que están participando; el anonimato en internet actúa como ventaja y desventaja. La forma de diferenciar entre un civil y un combatiente radicará, por tanto, en el análisis de sus motivaciones e intereses[23]. Lo más eficiente será, por ahora, centrarse en un análisis caso por caso: una vez identificado un ataque, analizar sus actores o posibles actores y sus motivaciones tras el ataque. En la clasificación de objetivos militares y objetos civiles, como ya se indicó anteriormente, el ciberespacio es global y los sistemas utilizados como servidores, routers o líneas de fibra óptica, son de acceso común a civiles y combatientes; por lo que no podemos determinar si un ataque es militar basándonos solo en sí el ataque ha sido realizado por

---

[22] HENCKAERTS JEAN-MARIE, DOSWALD-BECK LOUISE, "*El Derecho Internacional Humanitario Consuetudinario Vol. I: Normas",* Ed. del ICRC Argentina 2007, pag. 33

[23] REYES MANZANO, ROSA, "*El ciberespacio como un nuevo reto del Derecho Internacional. La ciberguerra en el Derecho Internacional Humanitario*", Trabajo de Fin de Máster 2012-2013. Acceso a la web: 11/01/2018 [15:33] https://www.academia.edu/5455118/_El_ciberespacio_como_un_nuevo_reto_del_Derecho_Internacional._La_ciberguerra_en_el_Derecho_Internacional_Humanitario_

un militar. Las amenazas pueden proceder de cualquier actor, y hoy en día debido a las guerras asimétricas es más difícil si cabe su identificación[24].

Sin embargo y aunque sea una tarea difícil en manos de expertos informáticos, los juristas y abogados deben intentar delimitar la autoría del ataque para saber si estamos ante un civil o un militar. Esta búsqueda de responsabilidad se complica, como ya se menciona gracias al anonimato en el ciberespacio. Al determinar si los hechos han sido llevados a cabo por un Estado, esto permite al Estado víctima responder contra su responsable, accionando así su derecho de autodefensa.

El principio de distinción debe ser respetado en la conducción de los ciberataques también, pero algunas operaciones "contra civiles" podrían no ser consideradas como ciberataques. Tal es el caso del envío de propaganda masiva a civiles a través de cuentas de Twitter, Facebook u otras redes sociales; ¿cabría aquí preguntarse si la propaganda política circulante en estas redes por parte de cuentas falsas vinculadas supuestamente con Rusia, durante las últimas elecciones de los Estados Unidos en 2016, podrían suponer una violación del artículo 2.4 de la Carta de Naciones Unidas si son consideradas como una amenaza a la "independencia política" de un Estado? De acuerdo al derecho convencional y consuetudinario actual, éstas actuaciones no son consideradas ataques armados, por lo que no autorizan la respuesta como autodefensa. Todavía.

Dentro de este principio de distinción en el ciberespacio se encuentra el hecho de que la tecnología necesaria para perpetrar un ataque es de fácil acceso por parte de la población civil y desde cualquier parte del globo[25]. Por ejemplo, si un mando militar ordena enviar emails masivos a la población del enemigo abogando por una independencia, o por un levantamiento contra su régimen, este ataque en el contexto del ciberespacio sería lícito de acuerdo a las leyes internacionales sobre conflictos armados[26]. Sería contrario al principio de distinción un ataque donde sufriesen un

---

[24] SANCHEZ MADERO, GEMA, "Internet: una herramienta para las guerras del siglo XXI" Revista Política y Estrategia, nº114 Universidad de la Rioja (2009) pág. 22

[25].MAYOR SMART, STEVEN JR. "*Ataque conjunto inteligente en el ciberespacio*" pag.3 Acceso a la web: 11/01/2018 [16:53] http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2013/2013-3/2013_3_06_smart_s.pdf

[26] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 422

perjuicio mayor como enviar malware de denegación de servicios (DoS) impidiéndoles un libre acceso a internet.

Otro elemento a tener en cuenta a la hora de determinar si el ciberataque viola el principio de distinción será, el nivel o impacto del ataque. Como hemos visto anteriormente, un ataque a una persona individualizada por razones de estrategia militar no supondría violación de leyes internacionales; en cambio, un ciberataque enviado al sistema de control de una planta química, que pueda escalar en una explosión y esparcimiento de materiales químicos sobre poblaciones próximas si convertiría a la población en objeto de ataque debido a la magnitud del mismo[27]. En esta misma línea y por poner otro ejemplo más claro: en el lanzamiento de una bomba atómica es muy difícil realizar un análisis sincero sobre si se respeta el principio de distinción o no, ya que el ataque es de unas dimensiones que rara vez no van a implicar víctimas civiles no participantes de las hostilidades. En el caso de los ciberataques se debe analizar este principio general en un sentido similar valorando la finalidad del ataque y la repercusión del mismo sobre la población civil a la hora de analizar si viola el derecho internacional o no.

El artículo 50.1 del Protocolo Adicional I recoge que en caso de duda sobre la categoría de si una persona es civil o militar se le debe considerar civil. En algunos casos el uso de una red concreta o de un ordenador no es indicativo de un status de civil o de combatiente por sí solo. Por lo tanto, si un civil participa en las hostilidades, tendrá papel de combatiente solo de cara a esa participación en las hostilidades como indica la "Rule 97" del Manual de Tallin en su Edición de 2017. Por el contrario, si un ordenador ha sido infectado en contra de la voluntad y con desconocimiento de su dueño, ese civil no será considerado combatiente y mantendrá su status de civil.

El ICRC interpreta que la participación directa en las hostilidades que otorga status de combatiente supone varios requisitos como que haya un nexo causal respecto al ciberataque o que el propósito del acto sea causar un daño considerado como "ataque

[27] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 423

suficiente"[28]. En el caso anterior, de un ordenador infectado sin conocimiento de su dueño, implicaría que su dueño NO es considerado militar, pero su ordenador, como bien civil, podría pasar a ser considerado objetivo militar y perder así su inmunidad de ataque.

Por otro lado, cualquier participación en un ciberataque como la creación de malware para infectar un sistema enemigo, se consideraría participación directa en las hostilidades con todas sus consecuencias legales. Es diferente robar fondos de un Estado con fin de ánimo de lucro privado o para financiar operaciones militares particulares.

A la hora de aplicar el principio de distinción respecto a bienes, el Protocolo Adicional I[29], los define de manera excluyente; entendiendo que son objetos civiles todos aquellos que no sean objetos militares. Es un reflejo de costumbre internacional interpretado así por una gran mayoría de países, por lo que aplicado a un ciberataque se podría entender como objeto militar la "ciber infraestructura" es decir, el virus o malware en concreto, el software capaz de afectar un sistema otorgando así una ventaja militar, pero no la computadora particular concreta desde la que se envía si ésta pertenecía a un civil[30].

El principio de distinción está intrínsecamente relacionado con la consideración de combatiente o no de una persona, por ello para su análisis debemos atender a cada caso concreto teniendo en cuenta la finalidad del ataque, la conclusión y efectos que implica sobre la población. A la hora de realizar un ciberataque en el seno de un conflicto armado nacional o internacional se deberá respetar siempre el principio de distinción.

B) Principio de precaución

1. Aproximación al concepto y su acogida en el DIH

---

[28] MELZER, NILS, "*Guía de interpretación de la noción de participación directa en las hostilidades según el derecho internacional humanitario*", Editorial del ICRC, Suiza 2010 pág. s/n
[29] Artículo 52 Protocolo Adicional I: definición de objeto militar
[30] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 436

El artículo 51.4 del Protocolo Adicional I prohíbe los ataques indiscriminados contra la población civil, entre otros "los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o los que emplean métodos o medios de combate cuyos efectos no sea posible limitar […] y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil".

Continuando el análisis, se pueden dar "bajas incidentales" o "daños colaterales" ,reconocida posibilidad en los conflictos armados; el Manual de San Remo[31], las define como "las pérdidas de vidas de civiles u otras personas protegidas o las lesiones que se les inflijan, así como los daños causados al medio ambiente natural o a bienes que no son objetivos militares en sí mismos, o su destrucción". Los civiles pueden ser víctimas de un error a la hora de aplicar el principio de distinción, citado en el apartado anterior de este trabajo. Por lo tanto, será un deber y obligación que el ataque armado cumpla también con el principio de precaución a la hora de ser llevado a cabo.

Es decir, aunque el ataque se vaya a realizar sea lícito, previamente debe realizarse un examen y análisis de su cobertura a fin de evitar daños innecesarios, excesivos o bajas de civiles. Por todos es sabido que en la guerra es difícil realizar esos cálculos tan precisos, pero, al menos, deberían tomarse las mayores precauciones a fin de evitarlos.

Existen obligaciones de aviso de evacuación desde tiempo atrás recogidas en las costumbres y sus usos del derecho internacional; concretamente el régimen jurídico que regula las precauciones en el ataque durante un conflicto armado internacional está establecido en el artículo 57.2 y 57.3 del Protocolo adicional I. Respecto a los ataques se prescribe que se tomarán las precauciones al preparar y decidir el ataque (momento anterior), además de suspenderse el ataque si se advierte que el objeto no es militar o goza de protección especial (momento durante) así como la obligación de dar aviso con la debida antelación y medios suficientes si el ataque pudiese afectar a la población civil.

En el párrafo 1 del ese artículo aparece la "*obligación de realizar las operaciones militares con el cuidado constante de preservar a la población civil, a las personas*

[31] Norma 13 c) del Manual de San Remo sobre la ley aplicable a los conflictos armados en el mar

civiles y a los bienes de carácter civil". Esta obligación implica una aplicación consecuente al principio de distinción.

La obligación de verificar la naturaleza del objeto para atacar y evaluar los daños, también se relaciona con el status de objeto militar o civil, pero además entraña una obligación de debida diligencia a la hora de evaluar los daños posibles resultantes del ataque. Como señala Yoram Dinstein: "Es indudable que no se puede tener certezas absolutas en el proceso de evaluar el carácter militar de un objetivo elegido para un ataque, pero existe la obligación de actuar con la debida diligencia y de buena fe"[32].

La obligación de elegir medios y métodos de ataque para evitar o, al menos, reducir todo lo posible las bajas entre la población civil y los daños a los bienes de carácter civil que recoge el artículo incentiva una prevención en el uso de medios altamente destructivos como bombas atómicas, minas antipersonas (que fueron prohibidas) o armas de destrucción masiva; todas ellos son medios que dificultan la necesidad de respetar el principio de distinción.

Respecto a la obligación de dar aviso con la debida antelación de cualquier ataque que pueda afectar a la población civil (del mismo artículo), el Protocolo adicional I establece que habrá que dar aviso "salvo que las circunstancias lo impidan". Por lo tanto, deja en manos del mando militar la toma de decisión, si consideran que podría menoscabarse su fin militar[33].

No se entiende como una obligación el hecho de tomar medidas absolutas de precaución, pero si se debe actuar de buena fe y tomar medidas factibles, aun cuando los seres humanos que las realicen pueda cometer errores[34].

Este principio de precaución combinado con el principio de distinción tiene un papel resaltante a día de hoy debido al desarrollo de las tecnologías de la informática y la información que ponen medios de comunicación modernos al alcance de militares y civiles. Todo esto sumado al aumento de las guerras asimétricas donde grupos no-

---

[32] YORAM DISTEIN, "*The Conduct of Hostilities under the Law of International Armed Conflict*", Cambridge University Press, Cambridge, 2004, pag. 126.
[33] QUÉGUINER, JEAN-FRANÇOIS, "*Precauciones previstas por el derecho relativo a las conducciones de hostilidades*", International Review of the Red Cross, diciembre de 2006, N.º 864 pág. 16.
[34] William J. Fenrick, "*Targeting and proportionality during NATO bombing campaign against Yugoslavia*", EJIL, vol. 12 (3) (2001), p. 501

estatales, grupos no militares, organizaciones y civiles actúan en la misma red de comunicación ha hecho que el principio de precaución tenga un relieve importante, sobre todo a la hora de planificar políticas internas de ciberseguridad en la defensa. "En la era de la información, esta segregación presenta numerosos desafíos nuevos" [35].

2. Análisis del principio en relación a las características de un ciberataque

Cuando analizamos si un ciberataque constituye una violación del principio de precaución se debe entender que, el comando militar que ordena el ciberataque está en constante seguimiento del mismo, según va avanzando por diferentes fases. Las peculiaridades del ciberespacio hacen que la "activación del ataque" y su efecto puedan distar en tiempo y espacio. Poniendo de ejemplo un virus informático, el comando militar que lo accione deberá tomar la precaución de evitar que ese virus acabe "infectando" objetos civiles como la red del sistema informático de un hospital, de un ministerio o incluso de entidades financieras de las que la población hace uso. Además, deberán tomar todas las precauciones necesarias para que los efectos de ese ataque, a posteriori, tampoco afectan a la población civil o lo hagan de la manera menos gravosa [36].

La complejidad de las ciberoperaciones, y el escaso conocimiento general sobre las mismas hace que este deber de precaución requiera de expertos en la materia que puedan monitorear el ciberataque desde su planificación hasta su lanzamiento.

La Regla 115 del Manual de Tallin dicta que aquellos que decidan realizan un ciberataque deberán hacer todo lo posible para asegurar que no atacan a civiles o a objetos civiles o de especial protección. Esto resulta de una aplicación analógica del artículo 57.2.a del Protocolo Adicional I. Cuando hablamos de un ciberataque se podría considerar un ejemplo de "tomar todas las medidas posibles" el hecho de monitorear el estado y seguridad de determinadas redes, crear firewalls para proteger sistemas que no revelen vulnerabilidades, etc.

---

[35] SHULMAN, MARK, "*Discrimination in the laws of information warfare*", Columbia Journal of Transnational Law, vol. 37 (1999), p. 963.
[36] SCHMITT, MICHAEL N. "T*allin Manual of International Law appliable to cyberoperations"* Ed. Cambridge University Press, 2017, pag. 477

Respecto a la elección de los métodos de guerra y su finalidad, respecto a ciberataques supóngase como ejemplo que se busca infectar una red enemiga para inhabilitar sus instalaciones o capacidades; en este caso se deberá considerar si existe la posibilidad de que se contamine también una red civil y la población se vea afectada por ese ciberataque y, de ser así, tomar las precauciones necesarias para evitarlo.

El artículo 57.3 del Protocolo Adicional I en la conducción de hostilidades, recalca que, a la hora de planificar y ejecutar un ataque contra un objetivo militar, se debe escoger siempre el objetivo militar más ventajoso pero que menos daños civiles colateralmente cause. El Grupo de Expertos que redactó el Manual de Tallin, de mayoritario acuerdo, aceptó entender este debe de escoger un objetivo ventajoso y no gravoso civilmente en cuanto a que no provoque un daño a la población civil[37]. Este daño antes de la revolución tecnológica venía interpretándose como un daño físico, a día de hoy y en relación a un ciberataque este Grupo de Expertos entiende que un descenso o privación de la funcionalidad de una red podría suponer un daño. Si tomamos como supuesto que al enviar un virus a la base de datos de un hospital para atacar a una persona que es objetivo militar, cabe la posibilidad a su vez de que los datos de civiles se vean expuesto también al riesgo, cabría considerar si este ataque cumple con los requisitos ya que si no se controla adecuadamente podría afectar a población civil.

Una vez planificado un ciberataque puede darse la situación de que se necesite suspenderlo o cancelarlo si se teme que el objeto no sea un objetivo militar, que cambie su status debido a alguna circunstancia especial o que se espere que cause algún tipo de daño directo, indirecto o incidental a la vida de civiles, que les lesione o que les cause algún daño o una combinación de ambos que sea excesiva[38].

La complicada naturaleza de la universalidad del ciberespacio hace que sea difícil delimitar un ataque, o cómo considerarlo. Independientemente de los métodos usados para atacar, un ciberataque contra el sistema de control de semáforos de una ciudad podría no causar un daño directo, pero podría ocasionar caos y accidentes de tráfico que conlleven daños. Esta ciberoperación se consideraría ataque, por lo que

---

[37] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 482

[38] Artículo 57.2.b Protocolo Adicional I

como método de guerra usado podría estar causando daños a civiles y violar el principio de precaución por parte de los atacantes, a la hora de afectar a la población[39].

Las reglas de conducción de hostilidades no tienen la finalidad de prohibir todas las operaciones que afecten a la comunicación civil, una privación de servicios a sistemas de universidad o televisión no supondría un ataque; no lo supondría tampoco a interpretación del derecho humanitario actual el envío de propaganda, noticias falsas, son simplemente inconveniencias[40]. Por otro lado, afectar el sistema bancario de un país podría suponer una interpretación como ataque si implica un grave daño a la población al no poder acceder a sus cuentas para comprar alimentos o bienes y servicios primarios.

Todo nos esto lleva a la conclusión de que hoy en día la línea en la definición de ataque se difumina ligeramente debido a la dependencia actual de sistemas de redes en el ciberespacio para la gran mayoría de actividades cotidianas; a la hora de analizar este principio de precaución son los atacantes lo que deben asegurarse que durante toda la conducción del ataque hostil no se ponga en peligro excesivo ninguna persona u objeto civil. Indirectamente siempre pueden darse daños colaterales pero las partes del conflicto en respecto de la buena fe debería intentar proteger y evitar esas situaciones.

C) Principio de proporcionalidad

1. Aproximación al concepto y su acogida en el DIH

El principio de proporcionalidad está recogido en el artículo 51.5.b y 57.2.ii del Protocolo Adicional I. Realizar un ataque sabiendo que el daño colateral será excesivo en comparación con la ventaja militar que éste podría otorgar va contra las leyes internacionales de derecho humanitario y violaría la buena fe. Ciertos daños colaterales son comprensibles y permitidos desde la aproximación militar, pero cuando éstos exceden lo razonable suponen una violación del derecho humanitario. A la hora de planear y ejecutar un ataque se deberán considerar todas las variables de la ecuación para que el daño posible sea el mínimo y sea proporcional con lo que pretendemos alcanzar en ese avance.

---

[39] DROEGE, C. "*Get off my cloud: ciberwarfare, humanitarian law and the protection of civilians*", International Review of the Red Cross, Ed. Volume 94 Number 886 Summer 2012, Geneva pag. 26
[40] DROEGE, C. "*Get off my cloud: ciberwarfare, humanitarian law and the protection of civilians*", International Review of the Red Cross, Ed. Volume 94 Number 886 Summer 2012, Geneva pag. 560

Este principio ha calado desde las primeras grandes guerras como una necesidad de humanidad en el derecho a la vida y a la dignidad. El principio ha ido apareciendo en muchos instrumentos internacionales como la Convención sobre la Prohibición o Restricción del uso de minas, booby-traps y otros dispositivos. Esta Convención en su artículo 3 recoge lo siguiente:

> "Queda prohibido el empleo indiscriminado de las armas a las que se aplica el presente artículo. Empleo indiscriminado es cualquier ubicación de estas armas: a) que no se encuentre en un objetivo militar ni esté dirigido contra un objetivo militar. En caso de duda de si un objeto que normalmente se destina a fines civiles, como un lugar de culto, una casa u otro tipo de vivienda, o una escuela, se utiliza con el fin de contribuir efectivamente a una acción militar, se presumirá que no se utiliza con tal fin; b) en que se recurra a un método o medio de lanzamiento que no pueda ser dirigido contra un objetivo militar determinado; o c) del que se pueda prever que cause fortuitamente pérdidas de vidas de personas civiles, heridas a personas civiles, daños a bienes de carácter civil o más de uno de estos efectos, que serían excesivos en relación con la ventaja militar concreta y directa prevista."

Este "uso indiscriminado" hace referencia a la desproporcionalidad del efecto de ciertas armas, como en este caso las minas antipersonas y otros dispositivos. En su párrafo c) se refiere a usos en los que éste "será excesivo en relación con la concreta y directa ventaja militar anticipada".

El ICRC interpreta que debe darse un pequeño margen de decisión al comando de la operación en cuanto a considerar esa "ventaja militar" y lo "excesivo" del ataque en proporción y, aun bajo ese margen, las actuaciones deben ser basadas en la buena fe y la diligencia debida a la hora de asegurar el principio de distinción y precaución también[41]. Los expertos del ICRC escribieron sobre esa "excesividad" lo siguiente:

> "El término "excesivo" a menudo se malinterpreta. No se trata de contar bajas civiles y compararlas con la cantidad de combatientes enemigos que han sido puestos fuera de combate. Se aplica cuando existe un desequilibrio significativo

[41] WRIGHT, JASON D., "*Excessive' ambiguity: analysing and refining the proportionality standard",* International Review of the Red Cross, Volume 94 Number 886 Summer 2012 Acceso a la web: 15/01/2018 [11:10] https://www.icrc.org/en/international-review/article/cyber-conflict-and-international-humanitarian-law

entre la ventaja militar anticipada ... y el daño colateral previsto para los civiles y los objetos civiles"[42]

Es decir, no se debe valorar el ataque por sus efectos cuantitativos solamente; se deben valorar en cuanto si esas bajas son proporcionales a la ventaja que se obtiene por ellas. Bombardear una ciudad con grandes armas de destrucción masiva porque se sabe que allí se encuentra un objetivo militar sería desproporcionado porque la destrucción de ese objetivo, supondría también la destrucción de la ciudad; constituiría un ataque excesivo e indiscriminado.

El Tribunal Internacional para Yugoslavia, se refirió a la proporcionalidad en el caso *Prosecutor v. Gálic.* El Comandante Gálic fue declarado culpable en 2003 por crímenes de guerra y contra la humanidad por violar del principio de proporcionalidad en la ejecución de una misión en Sarajevo donde murieron cientos de civiles y quedaron heridos otros tantos[43].

En la sentencia se dijo que al determinar si un ataque es proporcionado se debe examinar si una persona razonablemente bien informada en las circunstancias del Comandante, haciendo un uso razonable de esa información que le era disponible podría haber previsto excesivas bajas civiles como resultado del ataque[44].

El principio de proporcionalidad es importante a la hora de ejercer una protección sobre la población civil, pero aparte, ayuda a mantener la guerra dentro de unos límites "morales". El fin de la guerra no debe ser eliminar por completo al enemigo devastando y arrasando el campo de batalla indiscriminada y cruelmente. El objetivo primordial de la guerra deber ser vencer al enemigo, su rendición, pero no necesariamente su destrucción bajo cualquier coste civil o militar.

En el momento de determinar el principio de proporcionalidad en un ataque, debemos tener en cuenta dos puntos: la ventaja militar y el daño colateral esperado. A la

---

[42] Idioma original: "The term 'excessive' is often misinterpreted. It is not a matter of counting civilian casualties and comparing them to the number of enemy combatants that have been put out of action. It applies when there is a significant imbalance between the military advantage anticipated ... and the expected collateral damage to civilians and civilian objects"

[43]ICTY, The Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, 43 ILM 794 Judgment (Trial Chamber 1), 5 December 2003 párrafo 40

[44] ICTY, The Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, 43 ILM 794 Judgment (Trial Chamber 1), 5 December 2003, párrafo 58.

hora de realizar una aproximación legal sobre un ataque debemos valorar caso por caso, aplicando la buena fe y considerando las circunstancia y la información que se tiene en ese momento[45].

2. Análisis del principio en relación a las características de un ciberataque

Una ventaja de los ciberataques es que generalmente no implica víctimas ni civiles ni militares directamente. Su principal característica es que navega en el ciberespacio de manera abstracta, y no se manifiesta en la realidad sino como una consecuencia; es decir, enviar un virus informático contra un sistema no supone el mismo daño que lanzar un misil. Lo que se analiza aquí es la proporcionalidad de sus consecuencias.

Un ciberataque del que se prevea que puede provocar pérdida de vidas, daño a personas u objetos civiles o una combinación de ambos estará prohibido de acuerdo a una aplicación analógica del Protocolo Adicional I; pero si se diera éste deberá respetar este principio de proporcionalidad respecto a la ventaja militar que implique.

En aplicación de este principio en el ámbito del ciberespacio un daño incidental podría ser un daño a un ordenador, a una red de sistema o cualquier otra ciberestructura como bases de datos. A la hora de desplegar esos ciberataques es muy común que se transmitan a través de satélites o cableado también de uso civil por lo que evitar el daño o deterioro de bienes civiles puede ser complicado, o incluso ineludible; es por ello que el principio de proporcionalidad reviste mayor dificultad a la hora de analizar la legalidad de un ciberataque[46].

Un ejemplo recogido en el Manual de Tallin que representa un caso hipotético sería un ciberataque contra GPSs como bienes de doble uso. Si es atacado un sistema de GPS puede afectar tanto a fuerzas enemigas militares que serán incapaces de conocer el posicionamiento de sus tropas, pero a la vez podría afectar al tráfico aéreo o marítimo civil. Estos ataques serían lícitos de acuerdo al derecho humanitario siempre y cuando

---

[45] WRIGHT, JASON D., "*Excessive' ambiguity: analysing and refining the proportionality standard",* International Review of the Red Cross, Volume 94 Number 886 Summer 2012 Acceso a la web: 15/01/2018 [12:30] https://www.icrc.org/en/international-review/article/cyber-conflict-and-international-humanitarian-law

[46] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 471

no sean excesivos los daños respecto a la ventaja que suponga deshabilitar las capacidades del enemigo.

A correlación, el Manual también recoge la opinión del Grupo Internacional de Expertos y de Michael N. Schmit sobre ciberoperaciones que supongan inconveniencia, o estrés para las personas. Entienden que no califican como daño colateral ya que no suponen una pérdida de vida, lesión o daño a objetos civiles. Establecen que no serán consideradas como un daño. La mayoría de Expertos en este Grupo también advirtieron que un daño colateral podría ser legal si la ventaja militar adquirida es grande, pero, contrariamente un mínimo daño colateral sería ilegal si la ventaja militar obtenida es también mínima[47].

Cuando hablamos de ciberataques estos factores son muy difícil de calcular; el daño colateral no es preciso ya que muchas veces se desconoce la aplicabilidad de las técnicas o hasta donde pueden llegar las consecuencias ya que se está ante una tecnología muy nueva.

Por último, este principio está también recogido en la Regla 117 del Manual de Tallin combina proporcionalidad y precaución estableciendo que:

"Aquellos que planean o deciden atacar, deben evitar decidir ejecutar cualquier ciberataque que pueda preverse que cause daño incidental de pérdida de vida, lesiones a civiles, o daños a objetivos civiles, o una combinación de ambos, el cual sería excesivo en relación a la concreta y directa ventaja militar anticipada."

D) Principio general de inviolabilidad de la soberanía y jurisdicción

De manera amplia y general, se entiende por jurisdicción la competencia de los Estados para regular personas, objetos y conductas bajo la ley nacional en dependencia de los límites impuestos por el derecho internacional a través de costumbre o tratados ratificados por los Estados.

Supone para el Estado una autoridad total sobre sus ciudadanos, dentro de los límites legales ante mencionados. Cuando hablamos de jurisdicción territorial no

[47] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 473

referimos al ejercicio de ese poder dentro de su demarcación territorial; cuando nos referimos a jurisdicción extraterritorial nos referimos al ejercicio de ese poder fuera de su territorio a través de agentes, de su ejército o de personas a su cargo y en representación de una función relacionada con el Estado.

Los Estados gozan de varios tipos de jurisdicciones. Existen la jurisdicción en cuanto a leyes, es decir, un Estado tiene la autoridad de someterse a conductas a través de firmas de tratados o convenios internacionales y a dictar sus propias leyes en régimen interno. Por otro lado, tienen jurisdicción con poder ejecutivo lo que equivale a capacidad para hacer cumplir esas leyes o perseguir si son violadas. Y por último poseen jurisdicción judicial por la que, los Estados, tienen competencia para llevar ante los jueces disputas relativas a asuntos de su competencia.

La jurisdicción está plenamente relacionada con la soberanía de cada Estado para obligarse por sus propios medios a la realización de las ramas que se mencionan en el párrafo anterior. La soberanía y competencia que tiene estos Estados en el caso del ciberespacio es compleja.

Por un lado, el ciberespacio es un espacio global, virtual y sin fronteras; lo que hace que la delimitación del "territorio" sea problemática. Un Estado será soberano en el plano físico en relación con el ciberespacio respecto a redes, infraestructuras u ordenadores físicamente bajo su jurisdicción tanto territorial como extraterritorial[48]. Otro plano sería el social a través de aplicaciones o bancos de datos y protocolos que permiten ese intercambio entre los objetos del plano físico; y por último el presupuesto social son las personas que forman parte de esas relaciones en el ciberespacio[49]

El ciberespacio podría considerarse como un quinto espacio físico (agua, tierra, aire, espacio exterior) pero con la peculiaridad de que no se ha delimitado todavía. Es un dominio global, muchos autores consideran que debería formar parte de la categoría legal que adquieren las aguas internacionales o el espacio. Pero, una ciberoperación tiene que prepararse desde un lugar físico con un equipo concreto compuesto por ordenadores, sistemas de redes y, sobre todo, personas expertas llevando a cabo esas

[48] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 12
[49] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 12

actividades; por lo que los Estados tendrán soberanía sobre esas personas a la hora de aplicar leyes o someterlas a litigios ante sus tribunales. Esas personas tienen una nacionalidad por lo tanto depende y están sometidos a la competencia de un Estado. La Regla 2 del Manual de Tallin advierte, respecto a la jurisdicción interna o territorial, que: "Un Estado disfruta autoridad soberana con relación a una ciberestructura, personas y ciberactividades localizadas en su territorio sujetas a sus obligaciones de carácter internacional".

Lo que quiere decir que, un Estado dentro de su jurisdicción tiene libre soberanía para tomas las medidas que considere oportunas respecto este tipo de actividades en el ciberespacio o a través de ciberestructuras localizadas en su territorio, de acuerdo y en respeto a las leyes internacionales por las que se haya obligado.

El problema que surge con el ciberespacio es que las frecuencias electromagnéticas, a diferencia de los cableados de telecomunicación, no tiene una dimensión física palpable que permita establecer unos límites en cuanto a fronteras territoriales de los Estados se refiere. Desde un punto de vista legal el Estado puede promulgar legislación que requiera de firmas electrónicas, encriptaciones y demás sistemas de seguridad a la hora de realizar una actividad en la red; también pueden bloquear el acceso a determinadas web.

Respecto a la jurisdicción extraterritorial, el Manual entiende que un Estado es libre de conducir ciberactividades en sus relaciones internacionales, salvo norma internacional obligatoria en contrario (Regla 3).

De hecho, los Estados continuamente claman su derecho de control sobre ciberestructuras situadas en su jurisdicción territorial y sobre su derecho de protegerlas[50]. La aplicación del principio general de soberanía y jurisdicción no desaparece debido a los nuevos retos que supone el ciberespacio, pero tampoco se pueden seguir aplicando de la manera tradicional[51]. El derecho humanitario fue creado en un tiempo en que no se concebía mínimamente ni la existencia de un ordenador

---

[50] WOLFF HEINTSCHEL von HEINEGG, "*Legal Implications of Territorial Sovereignty in Cyberspace*", Ed. NATO CCD COE Publications, Tallinn (2012) pag. 10 Acceso a la web: 15/01/2018 [20:39]http://www.ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

[51] I*dem*. pag. 11 Acceso a la web: 15/01/2018 [22:11]

personal como lo conocemos hoy en día, por lo tanto, no todas las normas tienen una aplicabilidad lógica.

Los Estados tendrán derecho a ejercer control sobre las infraestructuras cibernéticas que se encuentren dentro de su zona de jurisdicción, esta jurisdicción podrá tener límites como son los casos de inviolabilidad de ciertos lugares como embajadas o consulados y los materiales que allí se encuentren[52] como ordenadores, memorias usb, bancos de datos en servidores, etc.

Las ciberoperaciones que violen el ejercicio de soberanía de otros Estados constituyen una violación a su soberanía y están prohibidos por el derecho internacional[53]. Para entes no estatales, esta prohibición de violación de soberanía no se aplica, a menos que esos entes no-estatales hayan actuado por atribución de un Estado. En cambio, en tiempos de conflicto armado, ciertas violaciones de la soberanía de otros Estados pueden ser llevadas a cabo de manera lícita si constituyen un objetivo militar o ayudan a la consecución de una ventaja militar. Tal es el caso del vuelo de drones americanos sobre espacio aéreo iraní.

A la hora de ejercer jurisdicción por parte de los Estados, surge otro problema, los sistemas de almacenamiento en nube o *clouds*. Esto supone que una ciberactividad puede ser llevada a cabo aun cuando la ciberinfraestructura se encuentre localizada en otro lugar debido a la ubicuidad de internet.

La "doctrina de los efectos" supone que se podría otorgar competencia jurisdiccional a un Estado si, aunque no tenga competencia sobre actos cometidos fuera de su territorialidad, los efectos de los mismos revierten en un lugar o persona sobre los que sí que te tienen competencia.

En palabras del Abogado General europeo Darmon:

> "The two undisputed bases on which State jurisdiction is founded under international law are territoriality and nationality. The former confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place. The latter confers jurisdiction over nationals of the State concerned. Territoriality itself has given rise to two distinct

---

[52] Convención de Viena sobre Relaciones diplomáticas artículo 27.1 y art 22

[53] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 17

> principles of jurisdiction: […] (ii) objective territoriality, which conversely, permits a State to deal with acts which originated abroad but which were completed at least in part within its own territory [The effects doctrine] confers jurisdiction upon a State even if the conduct which produced [the effects] did not take place within the territory."[54]

Si se aplica esta regla al ciberespacio y las actividades realizadas en él, se podría debatir la soberanía de competencia que podría tener un Estado sobre ciberataques que le afecten, aunque hayan sido realizados contra servidores fuera de su zona de jurisdicción territorial. Es decir, por ejemplo, si se lanza un ciberataque contra los servidores de un banco americano, los cuales se encuentran en Europa. El ciberataque ha sido enviado desde un tercer país contra un objeto situado en un país europeo, pero cuyas consecuencias afectan principalmente a personas o actividades llevados a cabo en territorio americano, en este caso se podría debatir sobre si EEUU tendría competencia debido a la doctrina de los efectos.

De la costumbre y la opinión iuris se pude concluir que los Estados, además, tienen una obligación afirmativa para prevenir que, dentro de las fronteras de Estados no actores, se cometan ataques. Por lo que un Estado que tiene capacidad de prevenir ese ataque pero no lo hace falla en su deber de prevenir[55].

Expertos Independientes que ayudaron a la redacción del Manual de Tallin recoge, en la Regla 4 (apartado 25) que una ciberoperación atribuible a un Estado que no está intencionada hacia la violación de la soberanía por otro Estado, pero que sin embargo genera esa interferencia, viola la soberanía del otro Estado. Por ejemplo, si un Estado ejecuta un ciberataque contra un Estado, pero la operación sin previsión afecta a un tercer Estado, provocando daño a un nivel suficiente, se podrá considerar que ha habido una violación de la soberanía de este Estado[56].

---

[54] DARMON, N. Opinión en los casos *"CASES 89, 104, 114, 116, 117 AND 125 TO 129/85*" (25 Ma y 1988) párrafo 19. Acceso a web: 16/01/2018 [13:47] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61985CC0089&from=EN

[55] Sklerov Lieutenant, Matthew J. Sklerov "*Solving the dilema of State response to cyberattacks: justification for the use of active defenses against states who neglect their duty to prevent*", Thesis Presented to The Judge Advocate General's School, United States Army, in partial satisfaction ofthe requirements for the Degree of Master of Laws (LL.M.) in Military Law (abril 2009) pag. 76

[56] SCHMITT, MICHAEL N. "*Tallin Manual of International Law appliable to cyberoperations*" Ed. Cambridge University Press, 2017, pag. 24

Aunque no existe una costumbre o práctica establecida debido a lo reciente de este campo, algunos países han mostrado su deseo de regularlo; países altamente activos en las ciberoperaciones, como China entre otros, han desarrollado códigos de conducta con los que apelan al respecto de la soberanía, la integridad territorial y la independencia política, comprometiéndose a:

a) "Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security"
b) "To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotaje"[57]

Esto no supone una ley ni una aceptación de someterse a instrumentos internacionales, pero ciertamente, supone un avance en el desarrollo y en el debate sobre los límites legales que rodean las actuaciones en el ciberespacio; y además, a largo plazo podría crear costumbre debido a una práctica reincidente y una opinión iuris en ese sentido por parte de más Estados.

Por desgracia, no existe ningún tratado internacional que regule estas cuestiones. Ante un ciberataque, un Estado no tiene un modo concreto y tasado de respuesta por lo que debe interpretar normas habidas de forma analógica.

La forma que tiene un Estado para responder ante estos ciberataques puede ser estudiada desde la perspectiva de considerarlo un "ataque armado" aplicando los principios del derecho humanitario en consideración al derecho de los conflictos armados internacionales y nacionales; o atajarlo desde una perspectiva de derecho público y considerarlo como actos criminales internacionales. La respuesta armada al ciberataque solo puede darse cuando se trata de Estado contra Estado.

Respecto a ciberataques es imposible atribuir la autoría en el momento en que se está ejecutando, y la forma de localizar al autor suele ser rastrear y monitorear la actividad del ciberataque en los momentos anteriores a su desplego. Esta operación suele prolongar el tiempo de respuesta ya que requieren de un gasto económico y temporal considerable; los contrataques en el ciberespacio no se caracterizan por la

[57] UN. Doc A/69/723 "International Code of Conduct for Information Security", de China, Kazajstán, Kyrgyzstán, Rusia, Tajikistán y Uzbekistán ante la Secretaría General de UN (enero 2013) pág. 4

inmediatez temporal de respuesta. La ciberguerra es una más lenta y prolongada en el tiempo que la guerra tradicional.

Esta tarea de identificación y atribución del ciberataque es necesaria, pero también lo es una cooperación entre agencias internacionales y Estados. Debido a las características de internet y el ciberespacio, así como su ubiquidad se debe cooperar e intercambiar información y conocimientos si se quieren tomar medidas prácticas en el ciberespacio[58].

Los principios de jurisdicción, soberanía y territorialidad son igualmente aplicables tanto en el espacio físico, como en el ciberespacio. Poniendo a un lado las complejas características y conocimiento experto que se necesita para realizar estas operaciones, los Estados deben desarrollar y mejorar sus técnicas y protocolos internos para asegurar que sus redes son seguras tanto para ellos mismo, como para otros Estados que estén interconectados.

IV. CASOS PRÁCTICOS REALES YANÁLISIS

A) Estonia (2007)

1. Contexto

La República de Estonia es un país báltico situado en el norte de Europa limítrofe con Rusia por su frontera este.

Durante la Segunda Guerra Mundial, Rusia expulsó a los alemanes nazis de lo que hoy es Estonia, y como homenaje a esa victoria existe una Estatua en Tallin al "Soldado de Bronce" desde 1947. Por entonces Estonia pertenecía a la Unión Soviética por lo que muchos estonios de as, ascendencia rusa consideran esta victoria positivamente. Por otra parte, un gran número de estonios considera que con esa estatua se elogian los ideales comunistas y ensalza la figura de la Unión Soviética y sus consecuencias sobre la población estonia, obligada a someterse a ese régimen político.

Más adelante, en 1990 Estonia declara su independencia de la Unión Soviética. Desde aquel momento existieron varias posiciones políticas dentro del país: estonios de

[58] WOLFF HEINTSCHEL von HEINEGG, "*Legal Implications of Territorial Sovereignty in Cyberspace*", Ed. NATO CCD COE Publications, Tallinn (2012) pag. 19 Acceso a la web: 16/01/2018 [16:39]http://www.ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

origen rusos y habla rusa simpatizantes con la Federación Rusa, y estonios de ascendencia báltica más convencidos con los ideales de libre mercado y cooperación de la Unión Europea.

En la primavera de 2007, el Gobierno estonio decide remover esa estatua al "Soldado de Bronce" a un cementerio militar, por motivo de realizar unas excavaciones en la plaza donde se encontraba para realizar excavaciones y desenterrar cuerpos de soldados caídos durante la guerra y enterrarlos en el cementerio militar. Este hecho fue considerado por algunos sectores como ofensivo y con pretensión de borrar la presencia histórica rusa en el país por lo que se produjeron manifestaciones y levantamientos. Para la minoría local rusa el soldado representa al «libertador» mientras que para los estonios representa al «opresor». El Gobierno preveía que habría violenta revueltas sobre todo por parte de los estonios de ascendencia y habla rusa[59]. El "Soldado de Bronce" y la plaza donde se encuentra, se convirtió en el punto de encuentro de manifestantes extremistas; la plaza a partir de entonces tuvo una vigilancia especial por parte de la Policía. La Sociedad estonia se encontraba cada vez más dividida entre pro-rusos influenciados por la prensa rusa, y estonios nacionalistas. Hubo más de mil arrestados, cientos de heridos y un muerto.

Aproximadamente desde 1997-200 Estonia ha apostado por la innovación y ha transformado casi el cien por cien de sus departamentos y ministerios, así como instituciones, a formato online. Es decir, los estonios hoy por hoy gozan de completo acceso a internet para consultar administrativas públicas, pago de impuestos, campus sobre educación, identificación digital o sistemas de blockchain[60]. Esto ha convertido al país en la meca de la tecnología en Europa, pero a su vez, ha aumentado el número de vulnerabilidades que el país posee de cara a ciberataques.

En 2007 tras las revueltas por la retirada de la Estatua al "Soldado de Bronce", las manifestaciones y revueltas pasaron de lo real a lo virtual, y en pocas horas el país se vio sumido en caos. Lo que continuó tras estos sucesos fue lo que podríamos describir como una guerra en el ciberespacio, una guerra del futuro.

Desde el día 27 de abril de 2007, mientras continuaban las protestas y enfrentamientos en las calles, sucedieron una serie de acontecimientos: se comenzaron a

---

[59] LANDLER, MARK, "*Digital fears emerge after data siege in Estonia*", Ed. New York Times, 29 Mayo 2007.

[60] https://e-estonia.com/ En esta web puede observar cómo funciona el e-Goverment de Estonia

producir ciberataques contra sistemas informáticos de gobiernos y administraciones, mientras la prensa cubría la noticia desde muy diferentes y politizados puntos de vistas. Los medios pro-rusos mostraron la noticia como una agresión policial contra estonios de ascendencia ruso que se manifestaban pacíficamente, sin mencionar los actos vandálicos y las revueltas.

La prensa europea como el "Financial Tiemes, Germany" (edición 5 de mayo de 2007) sacó a la luz una conversación telefónica mantenida por el Ministro de Asuntos Exteriores de la Federación Rusa Yevgeny Primakov con el ministro de asuntos exteriores alemán, Frank-Walter Steinmeier, donde el ministro ruso aseguraba que el gobierno de la federación rusa se aseguraría de que la policía forzara la finalización del bloqueo bajo condición de que la embajadora estonia abandonara Moscú.[61]

2. Desarrollo del ciberataque

Según el Ministro de Defensa estonia entonces, los ataques tuvieron dos fases[62]. Por un lado, los ataques llevados a cabo del 27 de abril al 29; estos ataques buscaban atraer sentimentalmente y de forma personal a los simpatizantes pro-Rusia. En estos ataques tenían como punto común que no suponían grandes conocimientos técnicos y que la mayoría fueron llevados a cabo a través de webs rusas donde se indicaban el modo de proceder para ello, junto con propaganda en contra de las actuaciones de la policía estonia contra los pro-rusos y estonios de ascendencia rusa. Con estos primeros ataques se puso el foco en webs del Gobierno estonio, de ministerios, especialmente Defensa; así como web de principales partidos políticos. Cuando el Gobierno estonio confirmó que se estaban siendo atacados de forma virtual, y que no se trataba solo de un fallo activó un comité de seguridad liderado por el CERT (Equipo Nacional de Respuesta Incidentes Informáticos).

A partir del 30 de abril los ciberataques pasaron a ser más técnicos y desarrollados, por lo que requieren mayor inversión tanto económica, como de personal. Aquí se observa un mayor conocimiento de métodos de "ciberguerra". Se usaron grandes cantidades de botnets, perfectamente coordinador y precisos en el ataque.

---

[61] GANUZA ARTILES, NESTOR "S*ituación internacional de la ciberseguridad en el ámbito de la OTAN: Caso Estonia*" pag. 117, Acceso a la web: 18/01/2018 [12:18] https://dialnet.unirioja.es/descarga/articulo/3837337.pdf

[62] Lauri Alman entrevisa con Wyatt Kash para GCN, 13 de junio de 2008

Los ataques fueron de varios tipos. Primero los ataques por denegación de servicios (DoS) consisten en hacer un objetivo inaccesible para sus usuarios. Cuando este ataque se realiza desde varios puntos se denomina "ataque distribuido de denegación de servicios". Una manera de hacer inaccesible una web puede ser a través de propaganda (congregando a gente para que acceda a la misma página a la misma hora), a través de botnets (ordenadores infectados sin conocimiento de su dueño que entrarían de forma automática a la página refrescándola automáticamente) o a través de granjas de servidores (con gran capacidad de computación). Todos estos son recursos costosos y técnicos.

Además, se dieron también ataques de hackeo de página web para modificar su contenido y crear confusión en la población civil y envíos masivos de spam. También se dieron ataques a servidores de direcciones de dominio públicas que afectaron a los principales ministerios del país, así como servidores de proveedores de servicios de internet en Estonia. Quedó claro, por tanto, que este tipo de ataques concretos, precisos y estudiados estaban detrás de un interés ruso en contra de Estonia. Los daños políticos, económicos, comerciales y de telecomunicación fueron costosos. Se atacó el Gobierno digital, por lo que se podría decir que se atacó al Estado, así como a los servicios de e-banking de los principales bancos del país, haciendo imposible que la población sacase dinero o efectuase cualquier gestión.

Todo ello, sumado al cierre de fronteras comerciales que realizó Rusia durante los ataques, impidiendo el tráfico de mercancías entre ambos países, provocó una grave crisis en el país.

La relación entre Rusia y Estonia ha sido políticamente complicada desde hace tiempo. Rusia no vio con agrado la incorporación de Estonia a la OTAN y al ser un país pequeño y muy dependiente de internet y las tecnologías, era el perfecto objetivo para conocer la ventaja tecnológica de la OTAN por parte de Rusia sin bajas, o imputación legal debido a lo complicado de esclarecer la autoría en internet. Rusia siempre ha negado su participación en los hechos.

3. Análisis legal del ciberataque

Considerando el artículo 2 del Convenio de Ginebra 1949, se considera conflicto armado internacional una guerra declarada o cualquier otro conflicto armado que surja entre dos o más Estados parte, aunque uno de ellos no haya reconocido el estado de

guerra. El Tribunal de Yugoslavia ha declarado en numerosas ocasiones que habrá conflicto armado si la situación fáctica lo revela, independientemente de que jurídicamente se haya declarado así. Lo que se quiere analizar aquí es si, a falta del uso de la fuerza física, un ataque informático podría suponer el detonante de un conflicto armado. Responder a esto depende de si un ataque informático es atribuible a un Estado y si equivalente al recurso a la fuerza armada[63].

A la hora de hablar sobre la atribución de un acto en el contexto del ciberespacio debemos recordamos lo complicado de localizar al autor, pero si se pueden localizar otros presupuestos. Por ejemplo, si un ataque informático surgió de una infraestructura gubernamental de un Estado, se podría atribuir ese Estado, ya que la norma del derecho internacional establece que los Estados no deben permitir que su territorio sea utilizado para actos contrarios a los derechos de otros Estados[64]. En el caso de Estonia, los análisis forense técnicos encontraron que algunsa IPs pertencían a la administración presidencial y a agencias estatales rusas[65].

Además de la atribución de responsabilidad, se debe estudiar si las operaciones cibernéticas equivalen al uso de la fuerza en el sentido del artículo 2 de la Carta de las Naciones Unidas, y/o se trata de un ataque armado del artículo 51.

El artículo 2.4 de la Carta de Naciones Unidas recoge lo siguiente:

> "Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas."

Se debe abrir el debate sobre si una operación cibernética del calibre de la ocasionada contra Estonia podría considerarse que amenaza la integridad territorial o independencia del país. El autor de este trabajo entiende que el colapso de las comunicaciones entre el gabinete del Gobierno, afectó claramente a su independencia política del país, que recurrió a la cooperación internacional para intentar paliar las consecuencias del ataque.

---

[63] DROEGUE, CORDULA , "*Fuera de mi nube: guerra cibernética, derecho internacional humanitario y protección de la población civil*", International Review of the Red Cross, Junio de 2012, N.º 886 de la versión original

[64] Corte Internacional de Justicia (CIJ), Caso del Canal de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte c. Albania), fallo del 9 de abril de 1949, página 22.

[65] EVRON, GADI «*Battling botnets and online mobs*», Revista «Science & Technology» Winter/spring 2008, página 125

Respecto al artículo 51 de la Carta que acciona el derecho a la legítima defensa en este caso no fue aplicado ya que el Consejo de Seguridad de Naciones Unidas no considera un ataque informático como un ataque armado aún. Éstos ciberataques generalmente ocasionan que se inhabilite el uso de un sistema, pero no conllevan su destrucción física. Eso no quiere decir que no sea un ataque, ni algo amenazante. Podrían enviarse un virus informático a la Bolsa de un país y causa graves daños financieros tanto al Estado como a su población, o impedir el acceso a red eléctrica en una ciudad durante días con el riesgo de que hospitales por ejemplo se encuentren sin energía y sus pacientes más graves o dependientes de máquinas corran peligro. En los tiempos que corren y debido a la dependencia que tiene la sociedad de internet y de las redes, un ataque informático podría tener más consecuencias realmente que un ataque físico como la destrucción de un edificio por un misil.

Los países deben comenzar a plantearse los retos de los nuevos métodos de guerra y su regulación para que no sucede, como en el caso de Estonia, que no se pudo achacar el ataque a nadie en concreto, cuando la mayoría de miradas de todo el mundo estaban sobre Rusia. El tema de estudio de este trabajo no es determinar culpables en el ataque Estonia sino analizar y debatir sobre la aplicabilidad del derecho humanitario en este caso.

Otros factores que debemos valorar a la hora de analizar un ataque para su determinación como ataque "usando la fuerza" o como "ataque armado" sería entre otros

que resulte cierto nivel de gravedad de las consecuencias del ciberataque, los medios empleados, la participación militar o de gobierno, la duración de la operación o el carácter civil o militar del objetivo.

En el caso de Estonia, la pronta actuación del país al reconocer la amenaza, la colaboración internacional por parte de EEUU y Europa para localizar los servidores de botnets, así como el cierre y reapertura de internet en todo el país, permitió mitigar el ataque y controlar las consecuencias. Sin embargo, también permitió ver como el sistema administrativo de un país podía venirse abajo sin tener que recurrir a soldados, tanques o campos de batalla físicos.

B) Georgia - Rusia (2008)

1. Contexto

Georgia en un país limítrofe con Rusia, Azerbaján, Armenia, Turquía y el Mar Negro. Es un enclave estratégico tanto militar como energéticamente ya que existen grandes reservarse hidrocarburos y es un lugar de paso de oleoductos hacia Europa. Los conflictos entre Rusia y Georgia no son jóvenes. Desde 1922 hasta 1991 aproximadamente perteneció a la Unión de Repúblicas Soviéticas y tras la caída del régimen declaró su independencia en 1991.

Formó parte de la Unión de Repúblicas Soviéticas hasta 1991, pero la influencia rusa siempre se mantuvo en ciertos territorios. Durante la Segunda Guerra Mundial lucharon contra los ejércitos nazis. Durante los 80 se forjó un importante movimiento independentista. En 1991 tras la disolución de la Unión de Repúblicas Soviéticas, Georgia declaró su independencia. El primer presidente de Georgia fue depuesto con un golpe de Estado construido con apoyo ruso. El país entró en un periodo de guerra civil, los conflictos separatistas y pro-rusos fueron aumentando. En las regiones de Abjasia y Osetia del Sur comenzaron a surgir brotes independentistas y, apoyadas por Rusia, declaran su independencia[66].

2. Desarrollo del ciberataque

Tras la Revolución de las Rosas en 2003 se dieron ciertas reformas democráticas y económicas y se comenzó a debatir sobre la entrada de Georgia en la OTAN. Abjasia y Osetia del Sur deciden declararse independientes con el apoyo de militares pro-rusos. Georgia comenzó el ataque y posteriormente, las tropas rusas bombardearon ciudades al norte de Georgia y dieron apoyo tanto a las fuerzas de Osetia como a las de Abjasia, tras el intento de Georgia de recuperar territorios con el ataque en la batalla de Tsjinval. En este caso, y con el antecedente de Estonia narrado en el párrafo anterior, Rusia procedió además con ataques cibernéticos. Las tensiones de la zona y los ataques armados se fueron incrementando en el curso de los días.

Los ciberataques comenzaron un poco antes del estallido del conflicto en agosto de 2008. En junio de 2008 se registraron pequeños ataques de denegación de servicios distribuidos (DDoS) pero con poco impacto a nivel Estatal. A la vez que comenzaron

---

[66] GANUZA ARTILES, NESTOR "S*ituación internacional de la ciberseguridad en el ámbito de la OTAN: Caso Georgia*" pag. 196, Acceso a la web: 23/01/2018 [15:42] https://dialnet.unirioja.es/descarga/articulo/3837337.pdf

las ofensivas militares en tierra en agosto de 2008, los ciberataques se intensificaron y perfeccionaron. Los hackers rusos se pusieron como objetivo varias páginas web y dominios del gobierno de Georgia. Las páginas web se colapsaron con un sistema similar al que se dio en Estonia, a través de botnets que saturaban las páginas a las que eran redirigidos[67]. El Gobierno georgiano no era capaz de mantener comunicaciones políticas entre sus distintos departamentos y, a su vez, se veía incapaz de comunicar a sus ciudadanos lo que estaba pasando a través de prensa o noticias. Se dio casos de contenido falso en webs estado con el fin de confundir a la población y hacer una guerra propagandística. El gobierno de Rusia culpó a de los ciberataques al Kremlin como parte de la intervención en los conflictos de Osetia del Sur y Abjasia[68].

La vinculación de los ataques con el gobierno ruso proviene de las circunstancias geopolíticas del momento, la localización de muchas de las direcciones IP recopiladas, la participación de hackers informáticos rusos, así como el parecido en la estructura de ataque con los sucedidos en Estonia en 2007.

Primero se realizaron una serie de ciberataques a través de botnets dispersos por el globo como sucedió en Estonia. La calidad en la organización estratégica del ataque y su temporalidad fue evidente y con mayor número de participantes[69] y por lo tanto con mayor coste económico y de recursos humanos. Las principales webs afectadas fueron el Ministerio de Defensa y Presidencia. Además de en entidades bancarias nacionales e instituciones financieras importantes en el país.

De la misma manera que el caso de Estonia, el salvoconducto de Georgia como país de pequeñas dimensiones y recursos fue recurrir a la cooperación internacional. Es por ello que algunas empresas como Google ayudaron al país durante el ataque[70]. Esta fue la única medida de control de que dispuso el Gobierno georgiano. La web del Presidente Saakashvili cambió su host a Google Blogs, el Ministerio de Defensa a servidores privados en Atlanta, el Ministerio de Asuntos Exteriores a Estonia y Polonia permitió

---

[67] SHACHTMAN, NOAH, "Georgia under online assault", The Wired, 10 de agosto de 2008; Acceso a la web 23/01/2018 [15:56] https://www.wired.com/2008/08/georgia-under-o/

[68] SAWAINE, JOHN, "Georgia: `Rusia conducting cyberwar`", The Telegraph, 11 agosto 2008; Acceso a la web 23/01/2018 [16:09] http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

[69] GANUZA ARTILES, NESTOR "S*ituación internacional de la ciberseguridad en el ámbito de la OTAN: Caso Georgia*" pag. 200, Acceso a la web: 23/01/2018 [16:44] https://dialnet.unirioja.es/descarga/articulo/3837337.pdf

[70] SHACHTMAN, NOAH, "GOOGLE HELP 'CYBERLOCKED' GEORGIA", The Wired, Acceso a la web: 23/01/2018 [17:18] https://www.wired.com/2008/08/civilge-the-geo/

que el gobierno de Georgia utilizara su página web para enviar algunos mensajes oficiales.

La primera fase de defensa fue aumentar los filtros para evitar que el tráfico se redirigiera hacia servidores rusos, pero esto no tuvo mucho éxito ya que los hackers habían utilizado también redes "dormidas" pero infectadas en EEUU y Europa Occidental. Finalmente, Georgia contó también con la ayuda de Estonia, que envió un grupo de expertos que habían diseñados mecanismos de control de daños tras lo sucedido en Estonia un año antes.

3. Análisis legal del ciberataque

El análisis legal del ciberataque de Georgia se encontró con las mismas dificultades que el de Estonia. Aunque la mayoría de ataques tenían origen en servidores rusos, grupos de hackers con apoyo del gobierno ruso y el contexto de guerra contra Rusia, no se puede acusar directamente a Rusia. Sumado a todo esto se encuentra la dificultad de encontrar a un responsable concreto, ni siquiera atribuir personalidad a ese sujeto. Debido a la asimetría de estas guerras en internet, y a la posibilidad de ocultarse tras el anonimato el ataque puede quedar sin culpables reales definidos.

Sumados a las organizaciones gubernamentales rusas, se encuentran los hacktivistas nacionalistas y los grupos pro-Kremlin (Nashi, pro-Putin). Ésta colaboración pública y civil hace imposible la atribución de los ataques. Los hacktivistas realizan los ataques, las organizaciones de crimen organizado proporcionan los medios como computadores, servidores etc., y la Russian Business Network (RBN) vende identidades o servicios de internet IPs. Todo ello con el apoyo gubernamental si se trata de atacar intereses del país, o si no es con apoyo, sin oposición a ello

Esto fue lo que sucedió en el caso de Estonia, y lo que sucede también con el caso de Georgia. El daño queda hecho, el debilitamiento del gobierno se palpa más aun en un período de guerra declarada. En el plano físico la guerra era oficial, pero la ciberguerra quedó en un segundo plano no reconocida por Rusia como responsabilidad suya; pero claramente le desestabilizar esos sistemas de información del gobierno georgiano le otorgó ventaja militar. Si se debilita la situación económica y de administración del

país, indirectamente se aumenta la capacidad militar del contrario para avanzar militarmente. [71].

Los ataques sufridos por Georgia desde un punto de vista del derecho humanitario, en el plano de la guerra física son claramente una competencia del derecho humanitario ya que la guerra era real, declarada y de facto en el terreno. Pero, el estudio de este trabajo se centra en analizar humanitariamente las consecuencias de un ciberataque y sus características.

Por lo tanto, un ciberataque consistente, como en este caso, en ataques propagandísticos, ocupación de webs con contenido falso o denegación de servicios que impiden a la población a acceder a canales de noticias fiables, crean una desinformación y desconfianza de la población respecto a lo que está sucediendo.

El artículo 2 de la Carta de Naciones Unidas impide el uso de la fuerza contra la estabilidad política e integridad de un Estado. A través de propaganda falsa que incitaba a la confusión se buscaba quebrantar la idea de lo que estaba sucediendo, en la mente de la población. Los ataques pro-rusos se basaban en contenido que criticaban las acciones de Georgia en el conflicto.

Los ciberataques en Georgia no solo afectaron a sus sistemas bancarios, comercio y finanzas de uso civil; además, mediante el uso de contenido falso en webs oficiales, se llegó a que los georgianos civiles y militares dudaran de la legitimidad de las acciones llevadas a cabo por su país.

En este caso la interpretación legal fue la misma que para el caso de Estonia, la diferencia recae en el contexto. En este caso el ataque en el ciberespacio estaba rodeado del conflicto armado que estaba llevándose a cabo en el plano físico, sumado a ello, la tensión por motivos energéticos en la zona. Todos estos factores podrían hacer que se entienda que el ciberataque formaba parte de la ofensiva rusa para desestabilizar al Estado de Georgia, y así ayudar a las regiones de Osetia del Sur y Abjasia a perseguir la independencia.

Desde el punto de vista de derecho humanitario solo se podría activar la defensa propia por un uso de la fuerza como recoge el artículo 51 de la Carta de Naciones Unidas. Pero en este caso quien inició las acciones fue Georgia; solo cabría debatir si,

---

[71] Informe Mensual Ciber elCano, nº 10/ enero 2016, Acceso a la web: 24/01/2018 [11:18] http://www.realinstitutoelcano.org/wps/wcm/connect/d26694804b495a16a1e0e3c12a87c07d/Ciber_Elcano_Num10.pdf?MOD=AJPERES&CACHEID=1452614978930

en caso de que los ciberataques fuesen llevados a cabo por Rusia o por subordinados de Rusia, si se violó la prohibición de atacar objetos civiles.

Esta regla basada en el principio de distinción se recoge en los artículos 51.2 del Protocolo Adicional I, y 13.2 del Protocolo Adicional II, reflejo de costumbre internacional. Cuando los civiles no puede acceder a sus entidades bancarias, o a información veraz sobre lo que está sucediendo, se debería debatir hasta qué punto las consecuencias de esos ciberataques a sistemas estatales afectan a la vida diaria de los civiles. Aun cuando estos ciberataques, como arma en la guerra puedan ofrecer una ventaja militar a costa de crear cierta desinformación entre la población para deslegitimar los actos del país atacado, sigue siendo difícil catalogar hasta qué punto este ataque podría considerarse un uso de la fuerza.

C) Irán (2010)

1. Contexto

Para entender la importancia y los motivos del ciberataque llevado a cabo por el virus Stuxnet debemos entender primero la situación política de Irán en años anteriores y posteriores, así como la evolución de su programa nuclear, el cuál atacó el virus informático.

Irán tiene un papel importante en la región, es uno de los países más poblados de Oriente Medio y ha tenido una historia de influencia norteamericana reciente debido a la influencia del gobierno de Reza Pahlevi. Éste gobierno llevó a cabo medidas modernas de reforma de país que causaron gran revuelo entre el clérigo, entre ellas, la liberalización de la mujer con derecho a voto, o la modernización de ciudades. El clero tomó esto como un intento, pero occidentalización y se opuso, por lo que fue expulsado a París su Ayatollah Jomeini. Se buscaba una modernización de país y comenzaron a encargarse la construcción de centrales nucleares. Poco a poco se fue perdiendo el apoyo popular. En poco tiempo, a penas semanas, la capital Teherán se encontró en manos de los revolucionarios contrarios a Pahlevi y al régimen social demócrata occidentalista, y Jomeini volvió a Irán para ser declarado presidente de la República Islámica de Irán.

La ideología contraria a Estados Unidos aumentó hasta llegar al punto de los sucesos de la Embajada de Estados Unidos en Teherán donde se secuestró a ciudadanos

americanos durante varios meses, incrementando la tensión entre ambos países. Irán seguiría, sin embargo, pese a las medidas poco sociales que propuso el nuevo Régimen, con los planes de centrales nucleares comenzados anteriormente. Su adversidad a Estados Unidos y a la cultura Occidental, que apoyen militar y económicamente a grupos como Hamás y el desarrollo de su programa nuclear son hechos que han mantenido en vilo a la comunidad internacional.

El Tratado de No proliferación de Armas Nucleares, de 1 de julio de 1968, en vigor desde el 5 de marzo de 1970 ha tenido gran éxito, ha sido ratificado por una gran mayoría de países. En 2002 Irán declara públicamente que está construyendo centrales nucleares en Arak y Natanz[72].

Tras estas declaraciones se suceden una serie de hechos y negociaciones para impedir el desarrollo militar de armas nucleares por parte de Irán. La oposición de la comunidad nacional es abierta y grande por lo que Irán declara que simplemente quiere dotar de energía eléctrica a su población y que no tiene fines militares. Así con todo, las tensiones y la desconfianza siguen existiendo. Tras varias resoluciones de Naciones Unidas, del Consejo de Seguridad así como de otros actores, las acciones de Irán respecto a su programa nuclear no se paralizaron[73].

En 2010 se pone en marcha la central nuclear de Bouchehr, pero más adelante en noviembre de 2010 el programa nuclear iraní se paraliza debido al virus informático Stuxnet y a la muerte de dos científicos nucleares en Teherán. La importancia de éste ciberataque se encuentra en que por sus características es considerada el "ciberarma" más moderna a día de hoy.

2. Desarrollo del ataque

En enero de 2010, técnicos de la Agencia Internacional de Energía Atómica (AIEA), se dieron cuenta que las centrifugadoras de la planta nuclear de Natanz fallaban. Éstas eran las encargas de enriquecer uranio. Esto se repitió a lo largo del país en otros sistemas; tiempo después se descubrió que el motivo era un virus informático: Stuxnet. Este virus fue diseñado para infectar plantas nucleares, afectando a casi 1000

[72] Declaración de Reza Aghazadeh, por entonces Presidente de la organización de la energía atómica de Irán en la International Agency for Atomic Energy.
[73] BERMEJO GARCIA, ROMUALDO, "The nuclear program of the Islamic Republic of Iran and its development (Politics and Law)", Anuario Español de Derecho Internacional Vol. 31 (2015) pag. 33

ordenadores, enviándoles comando para autodestruirse y rastrear información[74]. Su desarrollo fue el siguiente:

En primer lugar, el virus, una vez que infecta el sistema cambia los códigos para tomar el control del ordenador, pero sin que se puedan percatar de ello sus controladores principales. Por lo cual los hackers pueden controlar el sistema de manera remota y sin ser descubiertos[75]. Las personas que desarrollaron este virus tuvieron que trabajar en equipo durante, al menos, varios meses y además, tener conocimientos complejos sobre la arquitectura interior y exterior de sistemas industriales como los de las plantas nucleares. Con el virus ya formado, una persona tuvo que introducirlo en los sistemas por medio de un USB. Esto tiene relevancia a la hora de analizar jurídicamente, más adelante, la atribución de responsabilidad por el hecho.

En segundo lugar, una vez el sistema fue infectado, el virus de manera inteligente se dirigió hacia los sistemas de control de las centrifugadoras y de los termómetros que indicaban su temperatura; en el camino no dejó de lado la información que iba recabando sobre el resto de sistemas; información que remotamente controlaban los autores del virus y del ataque.

Los principales ataques, y los que se podía considerar que amenazaban la estructura de la planta, consistieron en acelerar las centrifugadoras a velocidades peligras que podrían haberlas hechos explotar y, posteriormente, decelerarlas. Esto se repitió en varias ocasiones. Durante este ataque varias máquinas centrifugadoras quedaron inutilizadas, retrasando así el programa nuclear de Irán.

3. Análisis legal del ciberataque

La principal diferencia entre el caso de Estonia y Georgia es que, por un lado, no existía un conflicto armado declarado en sí como en el caso de Georgia y, además, el virus Stuxnet perseguía un efecto en el mundo físico como el de acelerar y desacelerar las centrifugadoras. Es decir, no se trataba solo de infectar ordenadores o páginas web como en el caso de Estonia o Georgia donde el mayor daño directo podría considerarse

---

[74] iWonder, BBC Mundo, 11 Octubre 2015 *"El virus que tomó el control de mil máquinas y les ordenó autodestruirse"*. Acceso a la pagina web 24/01/2018 [16:21] http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[75] Información sobre el virus por parte de Compañía Symantec. Acceso a la web 24/01/2018 [16:30] https://www.symantec.com/es/mx/page.jsp?id=stuxnet

la “inutilización” parcial de internet. En este caso, no se buscaba saturar servidores web a través de botnets, ni falsificar páginas web. Este caso mucho más preciso buscaba una acción reflejada en el mundo físico como la consistente en dirigir remotamente y controlar el movimiento de las centrifugadoras y sistemas de la central.

A primera vista puede parecer que Stuxnet no supone grandes efectos. Pero la diferencia es potencialmente grande. En el caso de Stuxnet podrían haber detonado las centrales nucleares, o al menos podría plantearse la duda de qué sucedería si sucede ese escenario.

El autor de este trabajo considera que no se puede determinar con exactitud si la finalidad del ataque fue económica, política o militar. Lo que sí se puede concluir es que se dio un ataque que retrasó el avance de un programa nuclear que estaba siendo observado por todo el mundo, y con la oposición de importantes actores internacionales.

De acuerdo al artículo 49 del Protocolo Adicional I, se considera ataque los actos de violencia contra el adversario ofensivos o defensivos […] en cualquier territorio donde se realicen; añade que los Protocolos se aplicarán 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.

La central nuclear de acuerdo a Irán tenía carácter civil, pero comprensiblemente podría considerarse un bien con doble uso. Por lo que un ataque sería justificado en un contexto de conflicto, pero en el presente caso el país no se encontraba en guerra, aunque sí en negociaciones tensas. Por otro lado, simplemente con el virus no podría considerarse que se trata de un ataque armado, y desencadenar el derecho a la defensa, recogido por la Carta de Naciones Unidas; pero, ¿qué habría sucedido si algo sale mal y las centrales nucleares explotan? ¿qué sucederá la próxima vez que el mundo vea un ataque de este tipo, pero con resultados menos favorecedores para la población civil?

Los daños potenciales que podría alcanzar una ciberoperación como Stuxnet podrían ser desastrosos y violar varios principios del derecho humanitario internacional como el principio de distinción y proporcionalidad recogidos en los artículos 48, 51 y 52 del Protocolo Adicional I.

La dificultad a la hora de canalizar la atribución de responsabilidad hace que las medidas coercitivas o las sanciones para este tipo de ataques queden obsoletas. Varios

artículos de prensa y declaraciones hacen ver que el ataque fue orquestado por Israel y EEUU, pero una confirmación oficial no ha sido realizada.

Por otra parte, el artículo 36 del Protcolo Adicional I recoge, respecto a nuevas armas, que:

> "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."

EEUU, Israel, Irán o cualquier otro país estudió el virus Stuxnet. Toda la comunidad internacional lo estudió y analizó para conocer sus resultados, consecuencias y hasta donde podría escalar esa tecnología. Por lo tanto, de acuerdo a lo sucedido con respecto a este virus informático y al uso de ciberataques como armas en la guerra, esta materia debería pasar a un estudio por los estados parte para determinar si su uso podría estar prohibido en todo o en parte por el Protocolo o cualquier otra norma de derecho internacional.

El Derecho humanitario no contempla directamente interpretaciones sobre ciberoperaciones y su legitimidad, pero podemos aplicar análogamente lo recogido en párrafos anteriores respecto al modo de conducción de hostilidades y a los métodos y modos de llevar la guerra.

Pese a todo, este método de guerra conlleva varias complicaciones:

- El otorgamiento de autoría y responsabilidad debido al anonimato y ubiquidad del ciberespacio
- El derecho humanitario nace de la base de que los efectos de los métodos de guerra serán destructivos y violentos poniendo en peligro a la población o creando víctimas y en el caso de los ciberataques, generalmente el número de bajas es mínimo o inexistente.

- Otro problema es la distinción en derecho humanitario entre objetos civiles y militares. El derecho humanitario los considera claramente identificables y, en el caso del ciberespacio, las infraestructuras suelen ser de doble uso[76].

D) Un ciberataque global: virus Wannacry (2017).

Como ya hemos dicho anteriormente, para poder aplicar las reglas, normas y tratados del derecho humanitario internacional debemos encontrarnos ante un conflicto armado nacional o internacional donde alguno de los Estados parte de las Convenciones de Ginebra y la Haya sea atacante o atacado. La evolución de la guerra a la que se refirió en el primer apartado del trabajo nos hacía ver como hoy en día, la guerra ha tomado una dimensión asimétrica y ya no son solo los Estados los que participan en ella. Nos podemos encontrar que actores no-estatales como organizaciones criminales, corporaciones, grupos armados independientes de un rango jerárquico vinculado a un Estado o individuos particulares que deciden llevar a cabo un ataque en la red como pueden ser grupos de hacktivistas (financiados o no por otros Estados, actuando con su consentimiento o con su no oposición). En definitiva, los actores son varios y el ciberespacio es un canal al que todos pueden acceder.

En el caso del virus Wannacry, el ciberataque no se dirigió contra un Estado concretamente; este virus infectó más de 200.000 ordenadores en todo el mundo, de manera indiscriminada: desde grandes corporaciones, sistemas administrativos de Estados, ordenadores personales, e incluso hospitales[77].

Se ha decidido el autor del trabajo por analizar este tema en última instancia, por su cercana relación entre el derecho humanitario y el derecho internacional de los derechos humanos. Como ya vimos, ambos derechos se entrelazan y, ante un clima de guerras asimétricas, ciberataques de este tipo no quedan exentos de análisis. Cuando ataques de esta magnitud afectan a países enteros, amenazan su seguridad de la misma manera que los ataques mencionados con respecto a Estonia o Georgia.

Empezando por analizar en qué consistía este virus, podremos ver más claramente las consecuencias en que podría escalar y como ataques similares podrían

---

[76] DROEGE, C. "*Get off my cloud: ciberwarfare, humanitarian law and the protection of civilians*", International Review of the Red Cross, Ed. Volume 94 Number 886 Summer 2012, Geneva pag. 550

[77] Consulta online: google search "wannacry virus" https://www.avast.com/es-es/c-wannacry Acceso a la web: 25/01/2018 [17:55]

usarse en el contexto de un conflicto armado o para instigar uno. Un ataque de este tipo centrado en un Estado como único objetivo, ¿podría activar la cláusula de legítima defensa de la Carta de Naciones Unidas por violación de su artículo 2 sobre prohibición de ataques contra un Estado parte que amenacen su soberanía e integridad? Ante un ciberataque de este tipo, que pueda afectar a población civil indiscriminadamente, de conocerse su autoría y tratarse de otro Estado o un actor bajo su subordinación, ¿podría activar la legítima defensa y desencadenar en un conflicto armado?, ¿se interpretaría entonces este ciberataque como un ataque armado en el supuesto anterior, con su consiguiente interpretación legal al analizar la conducción de hostilidades?

Últimamente los Estados modernos empiezan a verse como actores de éstas prácticas militares y de inteligencia como podrían ser el envío de ciberataques o virus espía. Edward Snowden reveló varios de los secretos de este tipo de la Agencia de Seguridad Nacional americana, también vimos cómo se atribuyó el hackeo a Sony por parte de Corea del Norte, las posibles intromisiones rusas en las elecciones americana y francesa y, los casos mencionados en otros apartados respecto a Estonia y Georgia. Todos estos acontecimientos nos hacen ver a los Estados, como un posible actor de ciberataques a gran escala[78].

El virus Wannacry consiste en un virus que amenazó a cientos de miles de ordenadores en todo el mundo entre el 12 al 18 de mayo de 2017. El ciberataque consistía en un código malicioso que encriptaba y bloqueaba las computadoras a las que infectaba; explotando vulnerabilidades de sistemas operativos, principalmente Windows, este virus encriptaba documentos y archivos de los ordenadores de las víctimas y exigía un pago en moda digital bitcoin [79](casi imposible de rastrear) antes de una fecha determinada, de lo contrario eliminaría todos los archivos del equipo. Se ha sugerido por algunos expertos que, por el modo de redactar el código, este ataque pudo haber provenido del gobierno norcoreano buscando financiación[80].

---

[78] STAUFFACHER, DANIEL and MEYER, PAUL, "Wannacry, the Geneva Digital Convention and the urgent need for cyber peace", artículo online de ICT4Peace. Acceso a la web: 25/01/2018 [19:02] http://ict4peace.org/wp-content/uploads/2017/06/CyberWannacry-forICT4PeaceMay222017-1-1.pdf

[79] FRIEIRO BARRIOS, RUBEN; PEREZ SANJOSE, PABLO; PASCUAL VILLANUEVA, XABIER, "¿Qué impacto ha tenido el ciberincidente de Wannacry en nuestra economía? Editado por CyberRisk para Deloitte en Junio 2017. Acceso a la web 25/01/2018 [18:38] http://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf

[80] MENN, JOSEPH, "Symantec says 'highly likely' North Korea Group behind ransomware attack", Ed. Reuters online techonology news (Mayo 2017) Acceso a la web: 25/01/2018 [19:30]

Entre varios de los sistemas informáticos que atacó este virus, se encontraban el Sistema de Sanidad Británico (NHS); en este caso hasta 16 hospitales de Gran Bretaña sufrieron el ataque quedando completamente paralizados. Los enfermos más graves tuvieron que ser desplazados a otros hospitales, al resto de la población se le pidió que no acudieran a los hospitales salvo casos graves[81]. Si este ciberataque hubiese sido lanzado como un ataque "zero-day", es decir, sin que se haya conocido la vulnerabilidad del sistema operativo y, pudiendo así, atacar a muchos más ordenadores, el número de víctimas habría escalado.

En solo dos semanas este ciberataque colapso la sanidad británica, compañías españolas de telefonía y ordenadores particulares entre otras víctimas. Esta es la escala a la que hoy en día pueden llegar la tecnología de hoy. El derecho debe, por lo tanto, evolucionar paralelamente a estos sucesos, es por ello que debemos plantearnos si la ciberseguridad debería ser considerada como un derecho humano más en estrecha relación con el derecho de libertad de expresión o privacidad[82], entre otros.

El hecho de navegar en un ambiente seguro, el uso de bases de datos, sistemas de almacenamiento en nube, el acceso a conocimiento universal a través de portales educativos, tutoriales didácticos, intercambios de información en tiempo real, colaboraciones entre instituciones de todo el mundo de manera sencilla o conocer que está sucediendo en el mundo de una manera fácil y directa son muchas de las ventajas de internet. Todo esto se suma a facilitar el derecho al desarrollo, como *emerging human right*; en relación con otros como el derecho a la paz, a la calidad de vida o la libertad informática[83].

El programa de Naciones Unidas para el Desarrollo en un informe sobre el desarrollo humano señaló que interpretar la seguridad de manera que se centré más en proteger un territorio que en proteger a la gente en su vida diaria, carecía de sentido[84].

---

https://uk.reuters.com/article/us-cyber-attack-northkorea/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks-idUKKBN18I2SH

[81] GUIMÓN, PABLO, "Un ciberataque paraliza 16 hospitales de Reino Unidos y les exige dinero", El Pais online (Mayo 2017). Acceso a la web 25/01/2018 [19:39] https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html

[82] DEL CAMPO, AGUSTINA, "Hacia un internet sin censura", *Centro de Estudios en Libertad de Expresión y Acceso a la información"* Facultad de Derecho de Palermo (Buenos Aires 2017) pag. 58

[83] PEREZ LUÑO, A., "La tercera generación de derechos humanos", Ed. Thompson/Aranzadi (Navarra) 2006 pag. 33 y sig.

[84] Programa de Naciones Unidas para el Desarrollo (PNUD), *Informe sobre Desarrollo Humano 1994,* Fondo de la Cultura Económica (México 19914) pag. 25 y siguientes.

La seguridad debe ser vista como parte del desarrollo humano de la persona, por lo que es el Estado el encargado de buscar mecanismo para que esa seguridad sea real, tanto en plano físico como en el virtual.

Para dotar al ciberespacio de libertad y seguridad muchos países han comenzado a redactar y debatir sobre leyes de ciberseguridad. Esto, desde un punto de vista estatal estaría relacionado exclusivamente con la defensa de sus intereses y la protección de infraestructuras. Al igual que una central nuclear, una presa o un campo de pozos petrolíferos, las infraestructuras y sistemas que permiten mantener internet en funcionamiento pueden convertirse en objetivos tanto para otros países (como objetivos militares) como para agentes no estatales (como objetivos con un interés de ánimo de lucro como fue el caso del virus Wannacry, exigiendo un pago para la liberalización del ordenador).

La seguridad que buscan los Estados está relacionada con la "seguridad nacional" y la protección de su soberanía, su integridad política, económica y militar. El Estado tratará de proteger a sus ciudadanos de cualquier crisis o amenaza. Tras las Segunda Guerra Mundial, en respuesta a la amenaza nuclear, esta concepción de tratar de mantener una convivencia segura se tradujo en políticas de seguridad nacional[85].

El Informe sobre Desarrollo de Naciones Unidas de 1994 hacía referencia a la seguridad de la siguiente manera:

> "En primer lugar, significa seguridad contra amenazas crónicas como el hambre o la enfermedad y la represión. En segundo lugar, significa protección contra las alteraciones súbitas y dolorosas de la vida cotidiana, ya sea en el hogar, en el empleo o en la comunidad".

¿Lo sucedido con el virus Wannacry podría considerarse que fue una alteración súbita de la vida cotidiana o en el empleo, de la comunidad? El autor del presente trabajo entiende que alteraciones como la suspensión del sistema informático de 16 hospitales, así como la imposibilidad de utilizar ordenadores a lo largo de varias empresas en todo el mundo no solo altera la vida cotidiana de una comunidad, sino que puede llegar a provocar grandes pérdidas económicas o incluso humanas. El concepto de seguridad debería hacer referencia en el caso del ciberespacio a una seguridad de

---

[85] ROJAS, FRANCISCO and SOTO, DANIEL, "Estándares internacionales y Seguridad Pública", Revista de Derecho Público Vol. 77 (Santiago de Chile 2012) pag. 443

acceso a la información, un derecho a la confidencialidad y a la privacidad y, en definitiva, al fin para el que fue diseñado un sistema[86].

La gestión de la seguridad está siendo ahora enfocada por muchos países desde la posición de la defensa. Debido a lo complicado y costoso que puede resultar la investigación forense para dar con el autor de un hecho en el ciberespacio (a veces imposible), y posteriormente perseguirlo judicialmente, en lugar de tratar de otorgar responsabilidad por la autoría de un hecho, como puede ser cualquier ciberataque, hoy, la tendencia por parte de la mayoría de países es cubrirse las espaldas con un buen sistema de defensa a través de políticas y normativas de ciberseguridad. De este modo tienen mayores posibilidades para enfrentarse a las constantes amenazas contra la seguridad en la red que diariamente sufren la mayoría de Estados en la era digital.

V. ACTUACIONES DE ORGANISMOS INTERNACIONALES SOBRE EL CIBERESPACIO

A) OTAN

La OTAN siempre ha tratado de proteger sus sistemas de información y comunicaciones, es por eso que ha ido poco a poco incluyendo el tema de la ciberseguridad en su agenda política. Tras los ataques a Estonia en 2007, la OTAN decidió reunirse con urgencia para determinar cómo tratar ataques de ese tipo, ya que hasta entonces nunca había sucedido que un país pidiese ayuda a la organización ante ciberataques[87].

En octubre de 2008, la OTAN se reunió en la Cumbre de Bucarest donde se decidió mejorar la capacidad de defensa de la organización de sus propios sistemas de información y comunicaciones. En ella se estableció desarrollar políticas de ciberdefensa, compartir prácticas y conocimiento técnico y lo más importante, proveer capacidad de asistencia a un país del tratado en cado de contra defensa frente a ataques

[86] SINGER, PETER and FRIEDMAN ALAN, *Cybersecurity and Cyberwar: What everyone needs to know,* Oxford University Press (2014), pag. 35 y siguientes

[87] CARO BEJARANO, MARIA JOSE, Documento informativo del IEEE 09/2011, "Nuevo concepto de Ciberdefensa de la OTAN", Ministerio de Defensa (España 2011). Pag 2.

de este tipo[88]. Además, los ministros de defensa de los países aliados acordaron reconocer que, en suma, el espacio terrestre, aéreo y marítimo, el ciberespacio también se constituía como un nuevo campo de operaciones al igual que los anteriores y que quedaba sometido de la misma manera al derecho internacional ya que la mayoría de conflictos hoy en día, tenían una implicación cibernética[89]. Ya en 2010, la OTAN concluyó que las amenazas más probables contra países aliados consistirían, entre otras, en ataques en el ciberespacio de diferente grado y severidad[90]

El planteamiento clave de la OTAN ante las amenazas de seguridad en la red es la defensa de sus estructuras a través de colaboración internacional y mejora de conocimientos técnicos. Tras reunirse en la Cumbre de Wales de 2014, la organización se propuso mejorar el equipamiento técnico, la preparación de protocolos de respuesta, en áreas de ciberdefensa, a través de acuerdos para la prevención, detección y defensa y recuperación frente a ciberataques, usando capacidades de coordinación centralizada desde los propios países nacionales bajo unas pautas comunes[91].

Las principales actividades de ciberdefensa que se propone la OTAN consisten en dar prioridad alta a las cuestiones relativas a ciberseguridad. Entre sus preocupaciones se encuentra la asistencia a países aliados que no dispongan de medios para desarrollar políticas nacionales de ciberdefensa bajo las pautas de la organización; políticas que incluyan training y programas de educación, así como crear una cadena de administración para la cooperación entre los países miembros, ONGs y el sector privado[92].

---

[88] 03 Apr. 2008 | Press Release (2008) 049Issued on 03 Apr. 2008 Acceso a la web 29/01/2018 [9:55] https://www.nato.int/cps/ua/natohq/official_texts_8443.htm

[89] Cumbre de Varsovia 14 de junio de 2016 sobre Ciberdefensa

[90] NATO, "Analysis and recomendations of the group of experts on a new strategis concept for NATO", (2010) pag. 105, Acceso a la web: 29/01/2018 [12:25] https://www.nato.int/cps/en/natohq/topics_85961.htm

[91] NATO, "Wales Summit Guide", Edited by NATO (Newport 2014), pag. 33 Acceso a la web 29/01/2018 [12:00] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20141008_140108-SummitGuideWales2014-eng.pdf

[92] NATO, "Wales Summit Guide", Edited by NATO (Newport 2014), pag. 104 Acceso a la web 29/01/2018 [12:00] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20141008_140108-SummitGuideWales2014-eng.pdf

Entre los institutos externos con los que fomenta esa cooperación se encuentra el Cooperative Cyber Defence Centre of Excellence (CCD CoE) en Tallinn, Estonia. Este Centro está acreditado por la OTAN y tiene gran reconocimiento y prestigio; entre sus publicaciones se haya el Manual de Tallín para el derecho internacional en las ciberoperaciones. Además, la OTAN cuenta con varios órganos dedicados a la ciberdefensa como el Computer Incident Response Capability Center (CIRCC), que protege la red propia y las infraestructuras de la organización, y provee de análisis diarios de amenazas a la OTAN y a países aliados o la Agencia de Comunicació e Informacion[93].

B) Naciones Unidas

En 2013 la Asamblea General de Naciones Unidas acordó que se solicitara al Secretario General, la formación un grupo de expertos gubernamentales que "continúe examinando, con miras a promover un entendimiento común, las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza, las cuestiones relativas al uso de las tecnologías de la información y las comunicaciones en los conflictos y la manera en que se aplica el derecho internacional al uso de esas tecnologías por los Estados"[94].

El grupo presentó un informe sobre normas, reglas y principios regidores en la esfera del ciberespacio, así como medidas que fomentaban la cooperación internacional y la creación de capacidad para que los estados defendieran su ciberespacio de manera regional bajo unos mismos principios fomentando que los países no permitan que sus territorios sean usados para llevar a cabo actos maliciosos en ese dominio[95].

---

[93] Fact-Sheet on Cyberdefense by NATO Public Diplomacy Division, (December 2017), Acceso a la web: 29/01/2018 [13:22] https://www.nato.int/cps/en/natohq/topics_78170.htm

[94] Res. de 27 de diciembre de 2013 [sobre la base del informe de la Primera Comisión (A/68/406)] 68/243. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

[95] Res. A/70/174 de 22 de julio 2015, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security pag 1.

Entre las recomendaciones que el grupo de expertos gubernamentales propuso se encontraba la de exhortar a los estados sobre que no deber conducir o permitir con conocimiento actividades en el ciberespacio que de manera intencional dañen o impidan el uso de infraestructuras críticas; además, recomendó a los países que los vínculos de confianza y el intercambio de información ayudan a la transparencia y evitan conflictos entre países[96].

En estrecha relación con el derecho humanitario, el grupo de expertos gubernamentales hizo ver también lo siguiente:

> "While recognizing the need for further study, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group also noted the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction."

Entre sus recomendaciones, el grupo de expertos reconocía como de vital importancia el compromiso de los estados por respetar: la soberanía igualitaria, el arreglo de disputas y controversias por medios pacíficos, que se abstengan de la amenaza o uso de la fuerza en sus relaciones internacionales contra la integridad o independencia política de los demás estados así como con el respeto de los derechos humanos, las libertades fundamentales y la no intervención en asuntos internos de otros países[97].

Desde 2009/2010 el grupo de expertos gubernamentales sobre tecnologías de la información ha continuado reuniéndose a lo largo de varias sesiones, la última de las cuales tuvo lugar en 2017, y confirmó la existencia de graves diferencias entre los estados sobre cómo aplicar derecho internacional sobre las tecnologías de la información.

Esta última sesión mostraba las diferencias existentes entre los grandes grupos de ciberpoder (Rusia, EEUU y China principalmente), cada nación defiende visiones opuestas en este entorno. Muchos de estos bloques apoyaron el estudio de las

---

[96] Res. A/70/174 de 22 de julio 2015, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security pag 4

[97] Res. A/70/174 de 22 de julio 2015, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security párrafo 26.

tecnologías de la información y su desarrollo, pero mostraron su negación a desarrollar algún tipo de cuerpo legal que cubriese las lagunas que el derecho internacional no lograba clarificar sobre estas tecnologías, entendiendo que la ley vigente es suficiente para su regulación[98].

Entre los principales puntos de inflexión que han acompañado al grupo de expertos gubernamentales de Naciones Unidas sobre el desarrollo de las tecnologías de la comunicación y la información, y que han imposibilitado llegar a un consenso internacional a lo largo de todas las sesiones que se han ido llevando a cabo, se encuentran los siguientes:

Primero, la existencia de diferencias en la interpretación que se debe hacer del artículo 2.4 de la Carta de Naciones Unidas sobre la prohibición del uso de la fuerza, y la referencia a la posibilidad del activar el artículo 51 (legítima defensa) y la aplicación del derecho humanitario. Algunos países como China entienden que aceptar esta prohibición sugeriría a la comunidad internacional que se está legitimando la ciberguerra; otros, como Rusia, en cambio entienden que el artículo 2.4 debería ser de aplicación absoluta[99].

Segundo, las distintas perspectivas sobre la soberanía nacional de los estados. China ha apoyado en frecuentes ocasiones el derecho de cada estado para regular su ciberespacio de acuerdo a su legislación doméstica[100]. Por otro lado, países en desarrollo como Cuba, mostraron su preocupación en cuanto a que las economías poderosas como son Estados Unidos, son las que poseen una posición privilegiada que les permite imponer estándares tecnológicos que facilitan el uso de la información y las telecomunicaciones como una agresión[101]. Añadiendo que, en contraste, los países desarrollados no tendrían otra alternativa que aceptar esas premisas para poder

---

[98] TIKK ENEKEN and KERTUNENN MIKA, "The alleged demise of the UN GGE: autopsy and eulogy", Cyber Policy Institute (New York , The Hague, Tartu , Jyva skyla 2017) pag. 15 Acceso a la web: 30/01/2018 [10:09] http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

[99] TIKK ENEKEN and KERTUNENN MIKA, "The alleged demise of the UN GGE: autopsy and eulogy", Cyber Policy Institute (New York , The Hague, Tartu , Jyva skyla 2017) pag. 16 Acceso a la web: 30/01/2018 [11:05] http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

[100] Res. Asamblea General UN, Developments in the field of information and telecommunications in the context of international security, A/61/161 27 de diciembre de 2013 pág.4 China report.

[101] Res. Asamblea General UN, Developments in the field of information and telecommunications in the context of international security, A/54/213 pag. 3, párrafo 5.

sobrevivir en las nuevas condiciones de la era moderna, que debido a su desconocimiento en la materia podrían amenazar la seguridad nacional[102].

Tercero, respecto a la libre circulación de información en internet. Aquí se contrapusieron perspectivas occidentales y orientales. Por un lado, el bloque del Este veía el flujo libre de información descentralizado como una posible amenaza a su seguridad nacional. China defendía la postura de que esa descentralización podría debilitar sus estructuras políticas, económicas, militares y sociales[103]. Estados Unidos, en oposición, entendía que la seguridad de la información y la comunicación no podía impedir la libertad de dar y recibir información o ideas[104] como recoge el artículo 19 de la Declaración Universal de Derechos Humanos. La postura de Estados Unidos respecto a la ciberseguridad se centra en la persecución y condena de conductas criminales, estableciendo que respecto a conductas criminales, las leyes de derechos internacional y los principios de derecho humanitario bastan, y un cuerpo legal nuevo al respecto no es necesario[105].

Por último, otra de las diferencias más obvias entre los distintos bloques fue si se debía crear una regulación propia y especial relativa a las tecnologías de la información y la comunicación o no. En este punto dos grandes potencias divergen; por un lado, Rusia ha llevado a cabo varias propuestas de regulación[106] que muestran su intención de alcanzar un consenso para crear un proceso de regulación. En oposición, Estados Unidos posición que no sería sabio por parte de la Asamblea General, formular estrategias o actividades directas que interfieran con el trabajo que la comunidad internacional está desarrollando respecto a las tecnologías de la información y la comunicación[107] y más tarde ha continuado reafirmando su posición sobre la no necesidad de un tratado especial respecto a esta tecnología.

---

[102] Misma A 54/213 pag. 3 párrafo 6.
[103] Res. UN, Developments in the field of information and telecommunications in the context of international security, A/61/161 27 de diciembre de 2013 pág.4

[104] Res. UN, Developments in the field of information and telecommunications in the context of international security 59/116 Add.1 diciembre de 2004 pag.3 párrafo 3.
[105] Misma A/59/116 Add.1 diciembre de 2004 pag.3 y siguientes, párrafo 4. Y 5.
[106] Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (June 2009), Concept Convention on International Information Security (Russian Minister of Foreignt Affairs, September 2011), International Code of conduct for information security (A/66/359 de 14 septiembre 2011 y A/69/723 de 13 de enero de 2015).
[107] Misma A/59/116 Add.1 diciembre de 2004 pag.3 y siguientes.

El hecho de que el grupo de expertos gubernamentales no llegó a un consenso común evidencia la necesidad de seguir dialogando al respecto y desarrollando nuevas perspectivas y negociaciones entre los diferentes estados.

C) Unión Europea

La mayoría de gobiernos y países en toda la Unión Europea confían en las redes e infraestructuras digitales en su día a día. Muchos gobiernos utilizan softwares conectados a internet o redes internas inalámbricas fácilmente hackeables, lo que supone una mayor vulnerabilidad a los ciberataques. A pesar de ser una creciente amenaza, la consciencia sobre su dimensión es aún preocupante: 51% de los ciudadanos europeos afirman desconocer cuales son las amenazas cibernéticas y el 69% de las compañías carecen de unos conocimientos básicos o políticas internas de actuación[108].

Ya en 2012, el Parlamento Europeo, tras analizar varias de la actuaciones de los órganos de la Unión y demás organismos internacionales respecto a la ciberseguridad reconocía la necesidad de un tratamiento respecto a las tecnologías emergentes que se habían desarrollado y promovía las estrechas colaboraciones entre EU, OTAN, países europeos no miembros, así como con grandes potencias tecnológicas como Estados Unidos[109].

En 2016, se aprobó la Directiva para la seguridad de las redes y sistemas de información de la Unión Europea. Con ella se pretendía establecer un marco común de seguridad estableciendo obligaciones para los Estados miembros para crear estrategias nacionales de seguridad, crear un grupo de cooperación para apoyar y facilitar la cooperación estratégica, además de establecer obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de

---

[108] Reform of cybersecurity, artículo de información; acceso a la web: 31/01/2018 [12:08] http://www.consilium.europa.eu/en/policies/cyber-security/

[109] Resolución del Parlamento Europeo, de 22 de noviembre de 2012, sobre ciberseguridad y ciberdefensa (2012/2096(INI)) pag. 1

información[110]. Esta Directiva insta a los Estados a que adopten una estrategia nacional de seguridad de las redes y sistemas de información que establezca los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información[111]; también recoge, en su artículo 8, que los Estados deberán designar un órgano encargado a tal efecto como punto de contacto único y Equipos de Respuesta a Incidencias de Emergencia (CIRST, en inglés).

Las amenazas en el ciberespacio no solo amenazan la economía de la Unión Europea, también socaban el funcionamiento de las democracias, las libertades y los valores que en ella conviven, poniendo en riesgo tanto infraestructuras civiles como militares[112]. Los ataques pueden venir tanto de actores estatales, como no estatales y que éstos últimos pueden estar motivados por estrategias geopolíticas más que por la búsqueda de beneficio[113]. La Comisión dijo en comunicación al Parlamento Europeo y al Consejo Europeo que los actores estatales están incrementando su persecución de metas geopolíticas no solo a través de la fuerza militar sino también usando discretas ciber herramientas interfiriendo en procesos democráticos internos[114]. Saber si esta interferencia en procesos democráticos amenaza o ataca la integridad política de un país, como prohíbe el artículo 2.4 de la Carta de Naciones Unidas sería una interesante cuestión a resolver por la comunidad internacional.

El uso del ciberespacio como un campo de batalla es globalmente reconocido. Campañas de desinformación y noticias falsas como los casos de Estonia, Georgia y más recientemente EEUU; o ataques a infraestructuras críticas como el caso de las centrales nucleares de Irán y los ataques DDoS sufridos con el virus Wannacry en todo el mundo necesitan una respuesta; es por esto que la Comisión Europea ha manifestado

---

[110] DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[111] Artículo 7 de la DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

[112] Nota del General Secretariat of the Council a las delegaciones, en relación a las conclusiones del European Council meeting (22 and 23 June 2017), European Union Docs. (Bruselas 23 de junio 2017) pag. 3 párrafo 6.

[113] European Commission, comunicación conjunta al European Council y al European Parliament, Brussels, 13.9.2017 JOIN(2017) 450 final. Pág. 2 y siguientes

[114] Misma comunicación conjunta de 13 de septiembre de 2017 pag.3

la importancia de la cooperación en ciberdefensa entre los distintos países miembros ya que "the risk of politically-motivated attacks on civilian targets, and of shortcomings in military cyber defence, deepens the risk [of not to trust on emerging technologies] still further"[115].

La Unión Europea se compromete a desarrollar políticas de ciberseguridad y mejoras en las capacidades nacionales y de cooperación entre los países miembros y, en su comunicación de 23 de septiembre de 2017 al Parlamento y al Consejo estableció los pasos a seguir para conseguir esa meta. Primero, se busca construir resistencia en la Unión Europea a los ciberataques a través de[116]:

- Fortalecimiento de la Agencia de la Unión Europea para la seguridad en las redes de la información (EUNIS, en inglés)
- La creación de un cibermercado común seguro
- Implementando la Directiva sobre Seguridad en las Redes de Información (NIS, en inglés)
- Respondiendo a los ciberataques a través de una respuesta de emergencia rápida para lo que se crearán sistema de alertas rápidos en cooperación
- Mejora de las redes de cooperación con el European Cybersecurity Research and Competence Centre (ECRC)
- Construyendo una base de sólida de habilidades y conocimientos sobre las cibertecnologías en toda la Unión.

A su vez, la Unión Europea busca crear una política efectiva de disuasión para impedir que sea considerada como un blanco para el ciberataque por parte de actores estatales y no estatales; para ello llevará a cabo lo siguiente[117]:

- Identificando malware, ramsonware y cualquier otro software malicioso, así como a sus creadores, y perpetradores
- Mejorando la respuesta de persecución e investigación de los hechos; para ellos incrementará la formación sobre encriptación de códigos, darknet, pagos en

[115] European Commission, comunicación conjunta al European Council y al European Parliament, Brussels, 13.9.2017 JOIN (2017) 450 final. Pág. 2 y siguientes

[116] Misma pag.3 y siguientes
[117] Misma pag. 12 y siguientes

bitcoin. Todo ello aumentando la financiación a agencias como Europol y su Centro d Cybercrimen

- Además de mejorar la cooperación entre el sector público y privado, ya que el sector privado es el que posee la mayoría de infraestructuras que soportan el funcionamiento de las redes de comunicación e internet.
- Implementando la respuesta política y diplomática frente a los ciberataques
- Construyendo disuasión al ataque a través de las mejoras de las redes de seguridad nacionales de los Estados Miembros a los que se les pide que implementen sus capacidades a través de mayor inversión en i+D para este cometido, entre otros.

Por último, se comunica a los países miembros que es necesario un fortalecimiento de la cooperación internacional en materia de ciberseguridad por medio de[118]:

- Relaciones internacionales donde se ponga de manifiesto el tema de la ciberseguridad, la debida diligencia y la responsabilidad de cada país del control de las infraestructuras para el ciberespacio que se encuentren en su jurisdicción, para conocer así desde donde se han producido los ciberataques. La Unión Europea reconoce la aplicabilidad de la ley internacional en el ciberespacio y promueve su respeto bajo los principios de la Carta de Naciones Unidas.
- Mejora de las capacidades de ciberdefensa de los países miembros para que así, se pueda reaccionar mejor a los incidentes y su persecución. Sugiere a los países que desarrollen legislación y políticas de ciberseguridad y que establezcan oficinas nacionales del Computer Emergency Response Team colaborando plenamente con el resto de centros.
- También fomenta en las relaciones internacionales la colaboración de la UE con la OTAN para la ciberseguridad y la defensa ante amenazas hibridas (militar físicamente y con ciberataques) con ejercicios de coordinación y estándares de operación en ambas organizaciones.

En enero de 2018, tras todas estas actuaciones, se impulsó la firma de un acuerdo interinstitucional [119], para establecer las normas para la organización y el

[118] European Commission, comunicación conjunta al European Council y al European Parliament, Brussels, 13.9.2017 JOIN (2017) 450 final. Pág. 18 y siguientes

funcionamiento del Equipo interinstitucional de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la Unión («CERT-UE»)[120]; con funciones como las de contribuir a la seguridad de las infraestructuras de las TIC de todas las instituciones, órganos y organismos de la Unión, ayudando a prevenir, detectar, mitigar y dar respuesta a los ataques cibernéticos, actuando como una plataforma de coordinación de la respuesta a incidentes de ciberseguridad y del intercambio de información[121].

Los CERT-UE prometen una coordinación de respuesta por parte de la Unión Europea en su conjunto frente a los ciberataques dirigidos contra sus instituciones, colaborando estrechamente con los equipos de seguridad informática de las instituciones de la UE y los Estados miembros y la OTAN. Con los ciberataques a Estonia y Georgia se comprobó la necesidad de cooperación internacional para sobreponerse a estas ciberamenazas; varias compañías americanas cedieron servidores y banda para ampliar la capacidad de flujo de información de los servidores estonios que habían sido saturados, y países de Europa facilitaron el uso de sus propias páginas web gubernamentales para publicar información oficial a la que pudiesen acceder sus ciudadanos. Por otra parte, algunos países de Europa cuentan con una menor capacidad para enfrentarse a estos ataques, así fue en el caso de Georgia, país menos dependiente de las redes de la información e internet, que contó con la ayuda de expertos estonios cuando sufrió un ciberataque en 2008 durante el conflicto con Rusia. Las iniciativas de la Unión Europea se encaminan a proteger las infraestructuras críticas de comunicaciones, pero también de abastecimiento de energía para evitar situaciones como la del virus Stuxnet; así como implementar el conocimiento tecnológico necesario para enfrentarse a estas amenazas.

---

[119] Acuerdo entre el Parlamento Europeo, el Consejo Europeo, el Consejo de la Unión Europea, la Comisión Europea, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo, el Tribunal de Cuentas Europeo, el Servicio Europeo de Acción Exterior, el Comité Económico y Social Europeo, el Comité Europeo de las Regiones y el Banco Europeo de Inversiones sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE.

[120] Artículo 1.1 del Acuerdo sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE de 2018.

[121] Artículo 1.2. Acuerdo sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE de 2018

VI. CONCLUSIONES FINALES

El derecho internacional tiene un carácter evolutivo mucho más diferenciado que los derechos internos. Una sociedad global no tan fuertemente estructurada hace que tenga que adaptarse continuamente a la realidad de la Sociedad Internacional en general. El derecho debe, por lo tanto, evolucionar a la vez que se desarrolla la sociedad que regula y a la que aplica sus normas. El derecho humanitario, como rama del derecho internacional público debe hacer lo mismo dentro de su ámbito actuación. Los conflictos armados, como escenario principal en la aplicación del derecho humanitario, ha cambiado a lo largo de la historia de la Humanidad; las guerras romanas y las guerras actuales son completamente distintas desde su punto de vista legal, y tecnológicamente se han transformado por completo. Dos, son los grandes cambios acontecidos:

Por un lado, a día de hoy todavía existen grandes y cruentos conflictos armados, tanto nacionales como internacionales, pero sus participantes han variado. Hoy en día las guerras son asimétricas y sus participantes son tanto soldados pertenecientes a las fuerzas armadas de un país, como empresas de seguridad privada o grupos terroristas.

Por otro lado, el campo de batalla como lo conocíamos en el mundo cinético está desapareciendo. Cada vez es más común encontrarnos con ataques llevados a cabo de manera remota desde instalaciones muy alejadas de lo que se podría llamar la zona de conflicto, distanciando al combatiente del entorno bélico. El hecho de que un soldado pueda acudir al cuartel, "jugar a la guerra" a través de una pantalla de ordenador durante unas horas y volver a su casa tras pasar por el supermercado, cambia por completo el sentido y efecto de la guerra en sus actores.

Todo esto es debido al incremento del uso de las tecnologías de las redes, la información y las telecomunicaciones; alcanzando su máximo exponente con la

aparición de internet y el ciberespacio. El ciberespacio como tal, ofrece grandes ventajas para una globalización desde todas las perspectivas, pero a la vez, esa interconexión conlleva la aparición de amenazas que el derecho también debe regular. Es más, cuando una sociedad depende tanto de una tecnología en concreto, esta puede convertirse fácilmente en un objetivo militar para sus enemigos. El hecho de que la mayoría de infraestructuras críticas, así como sectores de la Administración Pública, estén conectados a esta red global hace que las amenazas a las que se exponen aumenten.

Estas amenazas en internet se transforman en ciberataques. La importancia de este sector se ve reflejada en el hecho de que desde hace más o menos una década la ciberseguridad se ha convertido en una de las mayores preocupaciones tanto de gobiernos como de empresas. La universalidad del ciberespacio provoca que un ciberataque pueda afectar tanto a militares como a civiles, y objetos de ambas naturalezas. El hecho de que la mayoría de Estados y sus ciudadanos hagan depender la seguridad de sus servicios, infraestructuras o datos de él y la posibilidad de que internet sea usado tanto para fines militares y civiles, hacen que la protección y regulación del ciberespacio sea necesaria.

Se concluye pues que, la evolución del derecho internacional debe ir de la mano de la evolución tecnológica; de la misma manera que no toleraríamos las reglas que se imponían en tiempos de guerra durante la época Clásica en el caso de un conflicto armado, se debe adaptar, o al menos revisar, la aplicabilidad del derecho actual para el caso de los ciberataques.

Con el ciberespacio existe la posibilidad de encontrarnos ante un nuevo *domain* para la guerra y la seguridad internacional depende en gran medida de él, por ello debemos analizar la posibilidad de un ciberataque encuadrándolo en los principios generales del derecho humanitario.

Comenzando por el principio de distinción, este principio es difícilmente aplicable en el caso del ciberespacio ya que una de sus principales características es la ubiquidad y el anonimato. Es complicado desde ambos puntos de vista; cuando se realiza un ciberataque saber si éste afectará a civiles, o saber si quien lo está realizando es un civil o no. Este principio se ha ido recogiendo en tratados, convenios y en las costumbres internacionales, pero no existe ninguna mención a los ciberataques específicamente en el derecho internacional humanitario actual. El principio de

distinción se aplica tal como se interpreta de los convenios mediante una aplicación analógica a los casos actuales. Un objeto civil será un ordenador que le pertenezca a un civil, un objeto militar será aquel ordenador desde donde se lanza el ciberataque que pertenezca o se encuentre bajo el control de un mando militar. Se deberá, por lo tanto, en cada caso analizar a quién pertenecía el objeto desde el que se llevó a cabo el ciberataque, con qué intenciones, si el dueño era civil, o si en caso de serlo, era conocedor de que se estaba perpetrando un ciberataque desde él. Un ataque DDoS si podría violar este principio de distinción si altera la vida y sociedad de la población civil como sucedió con el virus Wannacry.

En el caso del principio de precaución y la limitación de los efectos, se debe tener en cuenta que en el ciberespacio es difícil controlar la expansión de un ciberataque en la mayoría de los casos. Cuando se envían virus informáticos ha instalaciones militares enemigas, no es fácil controlar si ese virus saldrá de las redes o sistemas de esa instalación e infectará computadoras o sistemas civiles. Aunque se debe realizar un examen y análisis de su cobertura a fin de evitar daños innecesarios, excesivos o bajas de civiles, esto es muy difícil en el caso del ciberespacio ya que existen muchas variables y no una gran *expertise* en la materia.

También se debe resaltar la conclusión sobre su efecto: cuando se realiza un ciberataque los daños al sistema económico, político y, en definitiva, al sustrato social, no son tan graves comparado con un ataque armado en el que se dan bajas y heridos. En ese sentido se puede decir que, aunque es complicado aplicar el principio de precaución, los daños a tener en cuenta suelen ser menos gravosos que la pérdida de vidas humanas, por lo tanto, el trauma sufrido durante el conflicto podría será mucho menor. Este puede ser un motivo que incentive a los actores estatales, como no estatales, a llevar a cabo una guerra en el ciberespacio donde el coste tanto de recursos como de número de vidas es muy inferior.

Respecto al principio de proporcionalidad en el caso de los ciberataques, la ventaja militar generalmente es alta porque, como se decía en el párrafo anterior, su bajo coste humano y económico hace que los perpetradores de ciberataques lo prefieran a un ataque armado en tierra. Este principio en aplicación respecto a ciberataques implica que los mandos militares y agentes estatales deben llevar a cabo un monitoreo del ataque desde el momento de su ejecución. Para ello deben ponerse en marcha una serie

de medidas legislativas, administrativas o de protocolos de actuación internos por parte de los estados que ayuden a gestionar la respuesta a estos ataques; es necesario una modernización interna tanto mediante capacitación del personal militar como de formación e información de la población civil para que también protejan sus ordenadores privados; así como por parte de las empresas tecnológicas al diseñar sus productos ya que los productos IoT cada día forma más parte de nuestra vida.

Con relación a la soberanía, las cuestiones principales que se han tratado de resolver en este estudio son principalmente si un ciberataque podría violar el artículo 2.4. de la Carta de Naciones Unidas cuando amenace la independencia política y territorial de un Estado. Las recientes noticias sobre interferencias rusas en las elecciones americanas de 2016 y en las elecciones francesas de 2017, así como varios conflictos como el caso de Estonia y Georgia, ponen de manifiesto que cabe una posibilidad notable de hacer peligrar la independencia política de un país. Por otra parte, los casos en que Rusia se aprovechó de ciberataques a Georgia para colaborar con los movimientos independentistas de Abjasia y Osetia también alterar, o al menos afectan la integridad territorial del país. ¿Debemos entender esa alteración como amenaza a la territorialidad? ¿deberían los países tener derecho a activar la cláusula de legítima defensa del artículo 51 de la Carta de Naciones Unidas? Entre las varias interpretaciones existentes en el panorama nacional, se puede concluir que la mayoría de posiciones no entienden este tipo de ciberataques con la misma gravedad que un ataque armado cinético en el mundo real, por lo que hasta ahora no se está permitiendo esta activación del artículo 51. La única alternativa que le queda a los países víctimas de ciberataques es implementar sus capacidades de defensa y aplicar medidas económicas o diplomáticas. Esto plantea mayores debates ya que la legitima defensa debe tener un carácter de inmediatez, de lo contrario serían medidas de represalia, la legitima defensa debe respetar también los principios generales del derecho humanitario respecto a un ataque en el ciberespacio.

En cuanto a la jurisdicción, su delimitación en el ciberespacio es complicada. No existe barreras físicas que la delimiten, ni espacios que puedan usarse de referencia. Por lo que se concluye que quizás se debiera implementar la colaboración internacional para que cada país mantenga una debida diligencia sobre sus infraestructuras para evitar que sean vulnerables a ataques, pero sobre todo para evitar que desde ellas se ataque a

terceros. En este trabajo se ha comprobado que existe un vacío legal y que hay que rellenar esas lagunas del derecho manteniendo un equilibrio entre libertad y seguridad.

Esta necesidad de regulación y continuo debate se ve clara tras desarrollar un estudio sobre los casos concretos de Estonia, Georgia o Irán. Con estos ejemplos reales se ha podido desarrollar una pequeña aproximación a las implicaciones de un ciberataque, comprobando como en la mayoría de casos no se ha podido vincular un acto directamente a un Estado o a subordinados de este, debido a la facilidad de anonimato en el ciberespacio, lo que ha supuesto impunidad en muchos casos. Con los DDoS de Estonia, la administración del país quedó bloqueada por completo. Con Georgia el mando militar no pudo comunicarse con sus subordinados, situación que aventajó a las fuerzas armadas pro-rusas que defendía los movimientos independentistas de Abjasia y Osetia. Respecto a las centrales nucleares de Irán, el autor del trabajo considera que el virus Stuxnet es la más clara representación de un arma cibernética moderna, que pudo haber provocado daños potencialmente mayores en las centrales nucleares. Con el Virus Wannacry se bloqueó completamente el sistema de varios hospitales británicos lo que supuso graves efectos en los pacientes, además hizo que empresas como Telefónica en el caso de España tuvieran grandes pérdidas en tan solo un par de semanas. No es descartable, la situación donde se de un bloqueo de cajeros automáticos de entidades financieras puede hacer que muchos clientes no puedan realizar sus gestiones diarias de manera normal ya que tanto los cajeros como los sistemas informáticos de los bancos podrían fallar.

Tras el estudio de los diferentes ciberataques más notorios de la última década se puede concluir que el peligro existe y que tanto el estrato económico como político de un país pueden verse afectados por un ciberataque con apenas consecuencias legales, por lo tanto, los ciberataques se pueden considerar como una amenaza más para la seguridad nacional e internacional de los estados. Es por ello que en la mayoría de foros internacionales se han comenzado debates sobre este entorno, su posible regulación y sus efectos a través de políticas y protocolos de ciberseguridad.

En el último apartado del trabajo se ha realizado un resumen de las políticas, normativas y resoluciones más importantes de organismos internacionales respecto a esta materia, pudiéndose concluir que la existencia todavía de dos grandes posturas principales al respecto. Las diferencias entre estos dos puntos de vista se basan en la

concepción que ellos mismos tienen políticamente: por un lado, el bloque occidente (EEUU, Europa) entienden que ciertas libertades como la libertad de expresión y el derecho al respeto de la privacidad no deben olvidarse a la hora de redactar normativas de ciberseguridad. Al contrario, el bloque ruso-chino defiende que la seguridad nacional debe implementarse respecto al uso del ciberespacio, aun con deterioro de ciertas libertades individuales.

La conclusión, tras el caso de analizar las normativas de la Unión Europea es que esta, trata de armonizar unas mismas conductas en el ciberespacio a través de mejorar la ciberseguridad. Ello pretende conseguirlo a través de formación a personal oficial pero también creando conciencia ciudadana sobre los peligros del mal uso de internet.

El ciberespacio es un lugar de uso universal y a la hora de su regulación, así como de la redefinición de ciertos conceptos básicos legales, necesita de un gran consenso global. Es ahí donde el autor del trabajo encuentra el mayor obstáculo. Un ciberespacio seguro libre de amenazas no descansa solo en puntos técnicos y mejora de capacidades, descansa también en el comportamiento de sus ciudadanos y empresas. Si el Estado se protege y los ciudadanos y las empresas hacen lo mismo, será más difícil ser vulnerables respecto a ataques de este tipo. Es mejor una estrategia defensiva frente a los agentes externos que ejecutan ciberataques que una de carácter ofensivo.

VII. BIBLIOGRAFIA Y DOCUMENTOS

Instrumentos de órganos internacionales:

- Convención de Viena sobre Relaciones diplomáticas de 18 de abril de 1961
- Acuerdo sobre la organización y el funcionamiento del Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la UE de enero de 2018
- Protocolo Adicional I a los Convenios de Ginebra
- DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea
- Convención de Ottawa de 1997
- Cumbre de Varsovia 14 de junio de 2016 sobre Ciberdefensa
- Directiva de la UE 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
- Protocolo II de la Convención sobre ciertas armas convencionales (1980), Protocolo II enmendado de la Convención sobre ciertas armas convencionales

(1996), Protocolo III de la Convención sobre ciertas armas convencionales (1980)

Resoluciones y documentos de organismos internacionales:

- A/59/116 Add.1 Resolución Asamblea General de Naciones Unidas de diciembre de 2004
- European Commission, comunicación conjunta al European Council y al European Parliament, Brussels, 13.9.2017 JOIN (2017) 450 final
- Nota del General Secretariat of the Council a las delegaciones, en relación a las conclusiones del European Council meeting (22 and 23 June 2017), European Union Docs. (Bruselas 23 de junio 2017)
- A/70/174 Resolución de 22 de julio 2015, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
- A/61/161 Resolución Asamblea General UN, Developments in the field of information and telecommunications in the context of international security, 27 de diciembre de 2013 China Report
- A/54/213 Resolución Asamblea General UN, Developments in the field of information and telecommunications in the context of international security,
- Resolución de 27 de diciembre de 2013 [sobre la base del informe de la Primera Comisión (A/68/406)] 68/243. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional
- A/61/161 27 Resolución UN, Developments in the field of information and telecommunications in the context of international security, de diciembre de 2013
- A/66/359 y A/69/723 Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (June 2009), Concept Convention on International Information Security (Russian Minister of Foreignt Affairs, September 2011), International Code of conduct for information security (de 14 septiembre 2011 y de 13 de Enero de 2015)
- 59/116 Add.1 Resolución UN, Developments in the field of information and telecommunications in the context of international security diciembre de 2004

- Resolución del Parlamento Europeo, de 22 de noviembre de 2012, sobre ciberseguridad y ciberdefensa (2012/2096(INI))
- Op. Consultiva de la Corte Internacional de Justicia del 8 de julio de 1996 sobre la licitud de la amenaza o del empleo de armas nucleares
- A/69/723 "International Code of Conduct for Information Security", de China, Kazajstán, Kyrgyzstán, Rusia, Tajikistán y Uzbekistán ante la Secretaría General de UN (enero 2013)

Jurisprudencia y casos:

- DARMON, N. Opinión en los casos *"CASES 89, 104, 114, 116, 117 AND 125 TO 129/85*" (25 Ma y 1988)
- ICTY, The Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, 43 ILM 794 Judgment (Trial Chamber 1), 5 December 2003
- Corte Internacional de Justicia (CIJ), Caso del Canal de Corfú (Reino Unido de Gran Bretaña e Irlanda del Norte c. Albania), fallo del 9 de abril de 1949
- ICTY, The Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, 43 ILM 794 Judgment (Trial Chamber 1), 5 December 2003

Artículos de prensa y noticias

- Citado recomendado: 03 Apr. 2008 | Press Release (2008) 049 Issued on 03 Apr. 2008
- Fact-Sheet on Cyberdefense by NATO Public Diplomacy Division, (December 2017)
- FRIEIRO BARRIOS, RUBEN; PEREZ SANJOSE, PABLO; PASCUAL VILLANUEVA, XABIER, "¿Qué impacto ha tenido el ciberincidente de Wannacry en nuestra economía? Editado por CyberRisk para Deloitte en Junio 2017
- GUIMÓN, PABLO, "Un ciberataque paraliza 16 hospitales de Reino Unidos y les exige dinero", El Pais online (Mayo 2017)
- HARRISON, FERGUS, "*Waging war in peacetime: Cyber attacks and international norms", The Interpreter* (2015), Madrid 10 de enero de 2017
- iWonder, BBC Mundo, 11 Octubre 2015 *"El virus que tomó el control de mil máquinas y les ordenó autodestruirse"*

- LANDLER, MARK, "*Digital fears emerge after data siege in Estonia*", Ed. New York Times, 29 Mayo 2007
- NATO, "Analysis and recomendations of the group of experts on a new strategis concept for NATO", (2010)
- NATO, "Wales Summit Guide", Edited by NATO (Newport 2014)
- MENN, JOSEPH, "Symantec says 'highly likely' North Korea Group behind ransomware attack", Ed. Reuters online techonology news (Mayo 2017)
- Programa de Naciones Unidas para el Desarrollo (PNUD), *Informe sobre Desarrollo Humano 1994,* Fondo de la Cultura Económica (México 19914)
- SAWAINE, JOHN, "Georgia: `Rusia conducting cyberwar`", The Telegraph, 11 Agosto 2008
- SHACHTMAN, NOAH, "GOOGLE HELP 'CYBERLOCKED' GEORGIA", The Wired
- STAUFFACHER, DANIEL and MEYER, PAUL, "Wannacry, the Geneva Digital Convention and the urgent need for cyber peace", artículo online de ICT4Peace

Libros y editoriales:

- WOLFF HEINTSCHEL von HEINEGG, "*Legal Implications of Territorial Sovereignty in Cyberspace*", Ed. NATO CCD COE Publications, Tallinn (2012)
- Bert Koenders, Ministerio de Asuntos Exteriores de Netherland, Prólogo de "Manual de Tallin sobre ley internacional aplicable a ciberoperaciones 2.0" (Ed. Cambridge) 2017
- GUTIERREZ PONSE, Hortensia DT., *"Elementos del Derecho Internacional Humanitario",* Edit. Eudeba, Buenos Aires 2015
- MELZER, NILS, "*Guía de interpretación de la noción de participación directa en las hostilidades según el derecho internacional humanitario*", Editorial del ICRC, Suiza 2010
- Toomas Hendrik Ilves, Presidente de la República de Estonia, Prólogo de "Manual de Tallin sobre ley internacional aplicable a ciberoperaciones 2.0" (Ed. Cambridge) 2017
- PEREZ LUÑO, A., "La tercera generación de derechos humanos", Ed. Thompson/Aranzadi (Navarra) 2006

- SWINARSKI, CHRISTOPHE, "Principales nociones del Derecho Internacional Humanitario como sistema internacional de protección de la persona" ed. Instituto Interamericano de DDHH, Cátedra Jean Pictet (San José, 1990)

Artículos académicos y revistas científicas:

- DROEGUE, CORDULA , "*Fuera de mi nube: guerra cibernética, derecho internacional humanitario y protección de la población civil*", International Review of the Red Cross, Junio de 2012, N.º 886 de la versión original
- ALSTON, PHILIP and SHAMSI, HINA, "*A killer above the law*?", The Guardian (febrero 2010) Vol. Opinion on Afghasnistan
- BACKSTROM, ALAN and HENDERSON, IAN, "*New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews*", International Review of the Red Cross (Summer 2012),
- BERMEJO GARCIA, ROMUALDO, "The nuclear program of the Islamic Republic of Iran and its development (Politics and Law)", Anuario Español de Derecho Internacional Vol. 31 (2015)
- BERNARD, VINCET, "Comentario Editorial", *International Review of the Red Cross* (Summer 2012), Volume 94 Number 886
- CARO BEJARANO, MARIA JOSE, Documento informativo del IEEE 09/2011, "Nuevo concepto de Ciberdefensa de la OTAN", Ministerio de Defensa (España 2011)
- DROEGE, C. "*Get off my cloud: ciberwarfare, humanitarian law and the protection of civilians*", International Review of the Red Cross, Ed. Volume 94 Number 886 Summer 2012, Geneva
- [1] EVRON, GADI «*Battling botnets and online mobs*», Revista «Science & Technology» Winter/spring 2008
- GERMAIN, ERIC, "*Out of sight, moral issue in the globalization of the battlefield*", International Review of the Red *Cross* (2015), 97 (900), The evolution of warfare
- HATHAWAY O., and CROOTOF R., "The law of Cyberattack" (2012), Faculty Scholarship Series

- HENCKAERTS JEAN-MARIE, DOSWALD-BECK LOUISE, "*El Derecho Internacional Humanitario Consuetudinario Vol. I: Normas",* Ed. del ICRC Argentina 2007
- QUÉGUINER, JEAN-FRANÇOIS, "*Precauciones previstas por el derecho relativo a las conducciones de hostilidades*", International Review of the Red Cross, diciembre de 2006, N.º 864
- ROJAS, FRANCISCO and SOTO, DANIEL, "Estándares internacionales y Seguridad Pública", Revista de Derecho Público Vol. 77 (Santiago de Chile 2012)
- SHULMAN, MARK, "*Discrimination in the laws of information warfare*", Columbia Journal of Transnational Law, vol. 37 (1999)
- [1] SINGER, PETER and FRIEDMAN ALAN, *Cybersecurity and Cyberwar: What everyone needs to know,* Oxford University Press (2014)
- YORAM DISTEIN, "*The Conduct of Hostilities under the Law of International Armed Conflict*", Cambridge University Press, Cambridge, 2004
- William J. Fenrick, "*Targeting and proportionality during NATO bombing campaign against Yugoslavia*", EJIL, vol. 12 (3) (2001)
- WRIGHT, JASON D., "*Excessive' ambiguity: analysing and refining the proportionality standard",* International Review of the Red Cross, Volume 94 Number 886 Summer 2012
- SINGER, PETER W., "*Interview with Peter W. Singer*" en respuesta a la pregunta "Can new technologies benefit the humanitarian community?", *International Review of the Red Cross* (Summer 2012), Volume 94 Number 886

Trabajos académicos (AcademicGoogle):

- GANUZA ARTILES, NESTOR "S*ituación internacional de la ciberseguridad en el ámbito de la OTAN: Caso Estonia*"
- BRAUMAN, Rony, *L'action humanitaire, Dominos Flammarion*, Paris, 1995
- DEL CAMPO, AGUSTINA, "Hacia un internet sin censura", *Centro de Estudios en Libertad de Expresión y Acceso a la información"* Facultad de Derecho de Palermo (Buenos Aires 2017)

- REYES MANZANO, ROSA, "*El ciberespacio como un nuevo reto del Derecho Internacional. La ciberguerra en el Derecho Internacional Humanitario*", Trabajo de Fin de Máster 2012-2013
- Sklerov Lieutenant, Matthew J. Sklerov "*Solving the dilema of State response to cyberattacks: justification for the use of active defenses against states who neglect their duty to prevent*", Thesis Presented to The Judge Advocate General's School, United States Army, in partial satisfaction ofthe requirements for the Degree of Master of Laws (LL.M.) in Military Law (abril 2009)
- TIKK ENEKEN and KERTUNENN MIKA, "The alleged demise of the UN GGE: autopsy and eulogy", Cyber Policy Institute (New York , The Hague, Tartu , Jyva skyla 2017)
- DOREY GABRIELLE, "*Cyberspace: the new battlefield?", Ed. online Centre International pour la paix et les droits de l'homme*" (May 2017)