UNIVERSIDAD DE Belgrano

BUENOS AIRES - ARGENTINA

Facultad de Derecho y Ciencias Sociales

TESINA

"La aplicación del Derecho internacional humanitario en el marco de los ataques informáticos."

Casos: Stuxnet, Estonia, Georgia

Alumno: Franco Repetto

Matrícula: 10228334

Carrera: Relaciones Internacionales (102)

Email: franco.repetto@comunidad.ub.edu.ar

Tutor: Profesor Ricardo Arredondo

Legajo: 141070

Índice

1) Introducción

Este trabajo de investigación se centrará en determinar cuándo y en que momento los ataques informáticos, dependiendo del grado de su magnitud, pueden generar la aplicación de los principios del Derecho internacional humanitario; rama del derecho que comprende al cuerpo de leyes que regula el uso de la fuerza en los conflictos armados. En esta misma línea, se hará foco específicamente en los desafíos que representa la transposición del principio de distinción a ataques informáticos y su aplicación en el contexto cibernético.

La investigación considerará escenarios tanto reales como potenciales a la luz de la Convención de Ginebra y sus Protocolos adicionales, la doctrina perteneciente al tema, y otras normas de *soft law* relacionadas como el *Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra*; normas que son de carácter no vinculante, impulsadas por la OTAN con el objetivo de regular el uso de ciberataques en tiempos de guerra.

Se abordarán tres ejemplos de casos reales de ciberataques (Estonia 2007, Georgia 2008, Stuxnet 2010) para respaldar con casos reales la magnitud y alcance de estos fenómenos cibernéticos y corroborar, la eventual y pertinente atribución de responsabilidad penal internacional desde un abordaje del Derecho internacional.

No obstante, y como base fundamental de lo que será analizado, se abordará un profundo marco teórico que dotará de significancia jurídica y tecnológica a las conclusiones a las que se arribará en relación a la hipótesis de investigación formulada.

La primera aclaración que corresponde realizar es que los ataques informáticos se dan en el marco del ciberespacio, donde la existencia de los límites geográficos son difusos y, por lo tanto, también el sistema tradicional de la jurisdicción territorial.

En este sentido, los ataques informáticos o ciberataques se caracterizan principalmente por su naturaleza transnacional, es decir, la capacidad de que una operación cibernética produzca efectos o un daño real tanto a infraestructuras críticas como a la población civil de un país a través de las fronteras de forma remota. Debe existir un acto que sea deliberado e intencionado y que ocasione un daño como resultado. De esta forma, los ataques informáticos pueden ser llevados a cabo por gobiernos o por actores no estatales; pudiendo afectar consecuentemente a individuos, entidades estatales, corporaciones, organizaciones no gubernamentales como así también a otros actores. El anonimato que provee el campo del ciberespacio presenta uno de los desafíos más importantes a la hora de atribuir la responsabilidad a los autores que obran detrás de los ciberataques, resultando imprescindible profundizar los mecanismos de cooperación internacional entre Estados.

Cuando los ciberataques ocurren de manera transnacional, es decir, desde un Estado hacia otro u otros países; entran en conflicto, en primera instancia, los principios tradicionales de territorialidad, soberanía nacional y jurisdicción específica. De la misma manera, el anonimato que ofrece el ciberespacio y su competencia transnacional pone en jaque a los principios del Derecho internacional humanitario; los de distinción, proporcionalidad y precaución, que serán explicados más adelante.

Los ciberataques no existían cuando la Convención de Ginebra y sus Protocolos adicionales fueron adoptados. Sin embargo, el artículo 36 del Protocolo I adicional (PA) común a los Convenios de Ginebra estipula que los Estados están obligados a aplicar las reglas del Derecho internacional humanitario en caso de que surja una nueva arma o bien medios de

guerra. Por ello, resulta imperativo determinar hasta qué punto los principios del Derecho internacional humanitario pueden aplicarse a los ciberataques, y particularmente, cuán efectiva es la transposición del principio de distinción al contexto de un ciberataque.

A su vez, los ataques informáticos no siempre califican como crímenes internacionales, pues no todos cumplen con los requisitos estipulados por las normas del DIH; como ser la existencia de un conflicto armado y la pertinente atribución de responsabilidad a una de las partes del conflicto.

El presente trabajo de investigación se limitará a tratar a aquellos ciberataques que por su naturaleza interrumpan, degraden o destruyan redes computarizadas (infraestructuras críticas) de un Estado y, en consecuencia, provoquen la muerte de civiles o bien pongan sus vidas en riesgo.

Para acotar el amplio espectro de categorías y focalizar el tema en cuestión, quedan descartados los ciberdelitos que correspondan al ámbito económico o patrimonial, es decir, aquellos que se realizan con el mero fin de obtener una ganancia directa, y también, aquellos ciberdelitos que tengan como objeto la obtención de una determinada calidad de información (ciberespionaje). Según la opinión mayoritaria, éstos fenómenos están fuera de la competencia de la Corte Penal Internacional. Si bien más adelante se aclararán sus diferencias, no serán el centro del análisis del presente trabajo.

2) Hipótesis

La aplicación del principio de distinción al contexto del ciberespacio posee una importancia práctica limitada al momento de proteger la integridad de civiles tras un ciberataque.

3) Objetivo principal

Explicar los desafíos que implica la aplicación del principio de distinción a un contexto cibernético seguido de un ciberataque. Establecer cuándo y en qué momento puede aplicarse el Derecho internacional humanitario a un ciberataque, esto es, verificar el cumplimiento de los requisitos generales y, en caso afirmativo, analizar que papel desempeñan los principios generales del Derecho internacional humanitario tras un ciberataque. Con un fin práctico, se relacionarán los casos mencionados anteriormente al objetivo principal (Casos: Estonia 2007, Georgia 2008 y Stuxnet 2010).

4) Objetivos específicos

Proporcionar al lector el contexto y el marco jurídico aplicable, relacionando conceptos tales como soberanía, anonimato, jurisdicción, transnacionalidad y ciberespacio -entre otros- para establecer una visión holística del tema en cuestión.

Asimismo, se buscará proporcionar un marco técnico y jurídico con la finalidad de determinar en qué casos resulta aplicable el Derecho internacional humanitario en éstos fenómenos.

5) Modalidad y metodología

La modalidad del trabajo responde a una forma descriptiva.

Se expone, a través de la investigación cualitativa, constituida de diversas fuentes bibliográficas académicas y formales, así como también los casos ya mencionados, el umbral que delimita hasta qué punto el Derecho internacional humanitario puede aplicarse a los ataques informáticos. A su vez se plantean, los desafíos que representa la trasposición del principio de distinción en el contexto del ciberespacio y cuán efectivo resulta ser para proteger a la población civil de ciberataques.

Dado que se realizará un registro narrativo y, por lo tanto descriptivo de los hechos, este trabajo responde a la lógica de una investigación cualitativa, diferenciándose de una investigación cuantitativa que se basa en la recopilación y análisis de datos.

Capítulo I: Marco teórico

a) El ciberespacio

En la actualidad, Internet desempeña un papel crucial en el desarrollo económico y social. La difusión y uso de la Red ha creado el "ciberespacio virtual"; al haberse configurado, paralelo al mundo físico, un espacio comunicativo e interactivo que, en las últimas décadas, ha modificado las relaciones personales, sociales, económicas y políticas.

Internet se ha integrado en todas las actividades públicas y privadas y el proceso de globalización que particulariza a la actual economía ha impulsado nuevas formas de producción, comercialización y de interacción de la comunidad a través de las redes sociales. La evolución de las Tecnologías de la Información y la Comunicación (TIC) va acompañada de beneficios y vulnerabilidades; lo que implica sus indiscutibles ventajas, pero también la presencia de nuevos riesgos.

En términos generales, los riesgos generados por Internet impactan en dos grupos: 1) los ocasionados con el empleo de nuevas tecnologías, y, 2) los riesgos que pesan sobre las propias infraestructuras electrónicas cuando son atacadas con el objetivo de alterar o impedir el normal funcionamiento de los sistemas de información[1]; como el acceso no autorizado, la difusión de programas informáticos (virus, bombas lógicas, caballos de Troya o gusanos), y los ataques intencionados de denegación de servicio (DDoS), los que pueden causar graves daños a personas, a entidades u organismos, como así también a infraestructuras críticas.

[1] Barrio Andrés. M, Ciberdelitos 2.0, Amenazas criminales del ciberespacio. 2da. Ed. Buenos Aires, Astrea, 2020, pp. 18

Los tribunales de EE.UU fueron los primeros en investigar los ciberataques y sus consecuencias a los inicios de años 90´. El acusado era un estudiante de ingeniería informática de la Universidad de Cornell, que creó un virus diseñado para infectar Internet y encriptar los datos de los sistemas informáticos con el propósito de demostrar las insuficiencias de las medidas de seguridad en las redes electrónicas; causando daños de gran envergadura a los sistemas informáticos de todo el país pertenecientes a instituciones académicas, militares y comerciales[2].

En ese sentido, es de advertir que el uso de programas maliciosos (*malware*) constituye actualmente uno de los fenómenos más complejos y discutidos en el plano internacional.

La actuación de grupos de especialistas informáticos atentando contra la integridad del sistema informático del gobierno de Estonia y de distintas empresas de ese país en el año 2007; el uso de un programa informático malicioso (*Stuxnet*) para menoscabar el plan de enriquecimiento de uranio iraní en 2010[3]; el ataque informático sufrido por la empresa *Sony* contra su producto *PlayStation* y la publicación de millones de cuentas de usuarios de ese sistema con un costo de más de cien millones de dólares en 2011; la introducción de virus de denegación de servicio en distintas compañías del mundo (*Spamhaus*); entre otros son sólo algunos de los casos más conocidos, pero sin dudas, existe una enorme cifra negra de daños informáticos que impiden precisar el alcance real de ésta modalidad delictiva trasnacional en las redes informáticas[4].

También, en la actualidad se destacan los cibercrímenes políticos o ideológicos, cometidos con la intención de desestabilizar a un Estado, aprovechando las posibilidades de

[2] United States v. Morris 928 f.2d 504, 505 (2d Cir. 1991)

[3] Worner, "Einseitiges Strafanwendungsrecht und entgrenztes Internet?", pp.459; cit. en Aboso, Gustavo. E; Derecho penal cibernético, Buenos Aires, Editorial B de f, 2017, pp.351 y ss.

[4] Aboso, Gustavo. E; Derecho penal cibernético, Buenos Aires, Editorial B de f, 2017, pp. 351 y ss.

comunicación masiva que ofrece el ciberespacio, tales como: la ciberguerra (*cyber warefare)*, el hacktivismo o el ciberterrorismo que convirtieron a las infraestructuras tecnológicas de los Estados en objetivos prioritarios de ataques de denegación de servicio, de infecciones de *malware* que puede llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país[5].

Es una real amenaza en nuestra sociedad moderna el eventual daño económico que puede provocar el uso de programas o virus informáticos cuya magnitud es siempre significativa.

La afectación de los sistemas informáticos puede canalizarse por dos vías:

a) Mediante la destrucción del soporte electrónico de los datos (*hardware*); por ejemplo destruyendo el disco rígido.
b) Mediante la manipulación de los datos almacenados en los sistemas informáticos alterando así su capacidad de rendimiento o su sistema operativo (*software*).

En efecto, las diversas manifestaciones vinculadas a las tecnologías cibernéticas, plantean importantes desafíos de carácter jurídico, comunitario e internacionales.

De acuerdo al Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas elaborado por la Organización de los Estados Americanos (OEA), la mayoría de las instituciones gubernamentales de América Latina han experimentado intentos de manipulación de sus equipos a través de una red o de un sistema[6].

b) Los ataques informáticos y su vinculación con el ciberespacio

[5] Barrio Andrés. M, Internet de las cosas, Madrid, Editorial Reus, 2018, pp.111
[6] Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas elaborado por la Organización de los Estados Americanos (OEA), pp.29. Disponible en www.sites.oas.org

Previo a adentrarnos en la significancia de los ataques cibernéticos, es conveniente fijar algunos conceptos básicos que van a ser utilizados a lo largo del presente trabajo.

La proliferación de los ataques informáticos se explican por dos razones:

1) Bajos costos para acceder a la tecnología y a la experiencia necesaria; pues muchas veces las instrucciones de uso se encuentran disponibles en la red.
2) Anonimato de sus autores, ya que la complejidad de las maniobras realizadas y las dificultadas propias de Internet, torna difícil la individualización de los responsables.

La trascendencia de estas conductas, tanto a nivel nacional como internacional, ha generado varias reacciones. En primer lugar, si bien las técnicas empleadas siempre suelen ser los virus, los gusanos y los troyanos, se distingue entre los ataques dirigidos contra Estados, que se dan dentro de las llamadas ciberguerras, y aquellas conductas que no se enmarcan en esos conflictos bélicos en el ciberespacio, pero que atentan contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos previstas en las legislaciones internas de cada país[7].

En el primero de los casos, se advierte una serie de reportes de distintos Estados en relación con ataques en sus sistemas[8]. De allí el abordaje de éstas conductas por el Derecho Internacional humanitario. Se retomará este punto más adelante en el capítulo II.

En el segundo de los casos, cada país hizo frente a éstos ataques digitales criminalizándolos en sus respectivas legislaciones; más allá de las iniciativas internacionales para afrontar éste

[7] Kiefer, Mariana. Cibercrimen, Aspectos de Derecho penal y procesal penal, Buenos Aires, Editorial B de f, 2016, pp. 314 y ss.

[8] En 2010, el *Malware* STUXNET, marcó un nuevo nivel cualitativo en las capacidades destructivas en lo que se denomina la ciberguerra. Este *malware* fabricado por Siemens infectó infraestructuras críticas, con la capacidad de manipular procesos técnicos esenciales para las centrales nucleares iraníes y el control de oleoductos.

fenómeno desde una política penal común, dado los problemas relacionados con los límites geográficos y las fronteras nacionales[9].

c) Concepto de ataques informáticos

Aunque aún se discute su significado exacto, un ataque informático puede ser considerado una operación cibernética, ya sea ofensiva o defensiva, que se espera que cause lesión o muerte a las personas o dañe o destruya objetos[10]; o también puede representar la forma más intensa de lo que puede ser considerada una guerra cibernética, a través del uso de medios técnicos[11].

Un ataque informático interrumpe, degrada o destruye una red computarizada y puede llevar a la interrupción de los equipos conectados con la red bajo ataque[12], pudiendo dañar gravemente la infraestructura crítica de un Estado como pueden serlo los servicios de emergencia.

Los ataques informáticos sobre datos, programas o sistemas informáticos, y los programas destinados a causar daños tienen vinculación con los llamados "virus informáticos". Los virus informáticos son programas que se reproducen a sí mismos el mayor número de veces posibles y aumentan su población en forma exponencial. En ese sentido, están diseñados para evitar su detección y el virus puede ser introducido ya sea mediante soportes externos

[9] Convenio sobre la Ciberdelincuencia, Consejo de Europa, Budapest, 2001, cfr. Informe explicativo, Convenio sobre la Ciberdelincuencia, STE#N185, https://:rm.coe.int.

[10] Schmitt Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017, página 61.

[11] Droege Cordula, Sobre las distintas interpretaciones de la "guerra cibernética" en la práctica estatal, *Get off my Cloud*: Cyber Warfare, International Humanitarian Law and the Protection of Civilians, IRRC (94), 2012, página 536-537.

[12] Lubell Noam, definición del Departamento de Defensa de EE.UU., Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?, 2013, pp. 258.

(pendrive) o a través de la red de internet (correos electrónicos u otros medios), con el fin de infectar un sistema[13].

d) Maniobras de ataques informáticos. Tipos y características de las amenazas lógicas.

Sin pretender realizar una clasificación rigurosa ni establecer un análisis técnico de cada programa, se expondrá algunos tipos de amenazas:

1) Virus archivos ejecutables: el virus puede adherirse a un archivo y desviar el flujo de ejecución de su código para luego retornar al huésped y realizar las acciones esperadas por el usuario. Una vez ejecutado el virus se aloja en la memoria y puede infectar otros archivos ejecutables que sean abiertos al dispositivo[14].
2) Virus boot: atacan los sectores de arranque y establecen sus propias rutinas de carga[15].
3) Virus macro: estos virus atacan documentos en los cuales pueden ser insertados otros comandos[16].

En cuanto a la forma de propagación, el método para replicar los virus informáticos son los gusanos o *worms*. Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso[17]. Estos gusanos se propagan utilizando archivos adjuntos a un correo electrónico. Si el usuario ejecuta el archivo, el gusano se envía a los contactos de su libreta de direcciones, aunque en la actualidad se utilizan otras técnicas para

[13] Kiefer, Mariana, ob.cit. pp. 321 y ss.
[14] Clasificación realizada por la empresa ESET, 15 de junio de 2016, http://soporte.eset-la.com
[15] Ibídem.
[16] Ibídem.
[17] www.segu-info.com.ar

lograr su reproducción (redes peer to peer -p2p-, Facebook, vulnerabilidades de puertos de comunicación de los sistemas, etc.).

Por otra parte, los gusanos resultan ser el vehículo para establecer una red de computadoras *zombie* con el objetivo de efectuar ataques distribuidos de denegación de servicio[18], cuyas características se explicarán más adelante.

Por su parte, los troyanos son programas maliciosos que se utilizan para eliminar archivos, borrar un disco o acceder remotamente a un sistema informático ajeno; aparentando ser un programa legítimo.

Otra de las modalidades de la acción de destruir en materia informática esta dada por el uso de las llamadas "bombas lógicas", que tienen como finalidad dañar el sistema o datos y su nombre responde a que la serie de instrucciones que provocan el daño se ejecutan de manera programada siguiendo un patrón seleccionado (fechas y horas determinadas, números, cantidad de veces que se presiona un tecla, etc.). Es decir, son programas maliciosos que se activan a voluntad de su programador y, al tener la función predeterminada de eliminar archivos del sistema informático afectado, hace más lento su funcionamiento, provocando denegaciones de servicio, entre otros efectos[19].

En cuanto a los diferentes tipos de ataques informáticos, se destacan:

1) Ataque de Denegación de Servicios (DoS): su característica principal consiste en bloquear un sistema informático, lo que conlleva a que los usuarios no puedan acceder a él durante un lapso de tiempo y hasta que el sistema pueda ser reestablecido. Se

[18] Kiefer, Mariana, ob.cit. pp. 325 y ss.

[19] Uno de los primeros casos registrados del uso de este tipo de programas informáticos maliciosos tuvo lugar en septiembre de 1985 en Texas (Fort Worth), cuando un empleado encargado de la seguridad informática instalo en la base de datos de su empleador un *software* malicioso que provocó el borrado de miles de datos, ocasionando un grave perjuicio a la empresa.

genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios.

2) Ataque Distribuido de Denegación de Servicios (DDoS): se lleva a cabo generando un gran flujo de información desde varios puntos de conexión; siendo la forma más común de realizarlo a través de una *botnet*[20]. Esta maniobra se utiliza para lograr el anonimato de los atacantes y para aumentar exponencialmente las peticiones de acceso para luego lograr bloquear servicios o páginas web. Es importante destacar que los dueños de los equipos infectados, en la mayoría de los casos, no conocen la conducta que se está desarrollando a través de sus computadoras.

El ataque mediante denegación de servicio ha sido utilizado frecuentemente para atacar los servicios online de multimedios como símbolos de protesta contra la política editorial de ese medio.

Así, en el año 1998, el diario *New York Times* sufrió un ataque de esas características que lo dejó sin servicio por muchas horas y que incluyó la difusión de imágenes pornográficas y epítetos raciales en respuesta a la publicación de una obra sobre el hacking (*The Happy Hacker*) en la que había participado una de las reporteras de ese diario[21].

En el año 2000, un grupo de compañías informáticas fueron afectadas por el uso de este tipo de virus malicioso que produjo la interrupción de sus sistemas informáticos, provocando un perjuicio patrimonial de alrededor de un billón de dólares. Pocos meses después, el virus *I love you* se diseminó a través de las redes informáticas llegando a afectar a más de 45

[20] *Botnet* es un conjunto de computadoras o dispositivos conectados a una red que están a disposición de un equipo central y son controlados por una persona cuyo objetivo es atacar redes de computadoras o servidores. A los equipos que se encuentran a disposición del autor, se los conoce como equipos *zombies.*

[21] Satapathy, "Law for Computer Misuse and Data Protection", *Economic and Political Weekly*, octubre de 1998, p. 2639. Ob.cit. Aboso, pp.359.

millones de computadoras, replicándose automáticamente en los correspondientes directorios, utilizando los correos electrónicos como vínculo de acceso indebido a los programas informáticos.

3) *Ramsonware*: es un código malicioso que bloquea el acceso a los sistemas hasta que la víctima pague el rescate consistente en una suma de dinero que, en la mayoría de los casos se traduce en criptomonedas. Estos casos consisten en la encriptación de los archivos contenidos en los sistemas informáticos atacados, cuyos usuarios observan en la pantalla de sus computadoras una comunicación en la que los delincuentes solicitan una suma de dinero o *bitcoins* o, en su defecto, procederán al borrado definitivo de los documentos y archivos afectados[22]. Si el presente hecho lo traspasamos al ataque de una infraestructura crítica, como la torre de control de un aeropuerto, por ejemplo, es muy fácil imaginar el efecto devastador que generará dicho ataque informático[23]

   Es decir, la peculiaridad de la extorsión online (*ramsonware*), consiste en el empleo de un programa malicioso (*malware*) que impide el acceso al titular o usuario de datos. De esta manera, el autor utiliza este programa informático para apoderarse de los datos ajenos y así exigir un rescate en dinero para liberar esa información[24].

Otro de los ejemplos más recientes en cuanto al alcance transnacional que producen estos ataques informáticos es el generado en el Registro Nacional de las Personas (Renaper).

[22] Aboso, Gustavo. E, Derecho penal cibernético, la cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación, Buenos Aires, B de f, 2017, pp. 371 y ss.
[23] Como el conocido caso del *malware* Wanna Cry
[24] En el código penal norteamericano la disposición 1030 (a) (7), abarca distintos supuestos desde la amenaza de dañar el sistema informático hasta la obtención de información sin autorización, o excediendo la otorgada, para exigir la entrega de dinero o efectos bajo la intimidación de revelar esos datos. En todos esos casos el autor debe exigir una contraprestación indebida en dinero. Sin embargo, en el código penal argentino aún no está expresamente tipificado, aunque, se podría subsumir en el art. 168 del código penal (extorsión).

El jueves 27 de agosto de 2020, un *ransomware* (un *software* malicioso) denominado *NetWalker* vulneró los datos de la Dirección Nacional de Migraciones. Un mensaje extorsivo señalaba que, si no se pagaba una cifra millonaria por recuperar la información secuestrada, harían públicos los datos, poniendo en juego 22 carpetas con información de embajadas, incluida la de Estados Unidos, informes de Interpol y de la AFI (Agencia Federal de Inteligencia), entre otros[25].

e) Identificación de IP

Si bien se ha abordado la magnitud y el impacto transnacional que implican los ataques cibernéticos, es importante hacer al menos una breve referencia a la identificación de la IP desde donde los autores habrían efectuado dicho sabotaje internacional. En ese sentido, la dirección de IP es un número que identifica de forma única, ya sea, servidor o cliente, un recurso dentro de la red. Es decir, esa IP deberá ser correctamente identificada para saber quien atacó y desde qué país. La única forma de identificar a un usuario de la red es a través de su dirección IP, con la salvedad de que dicho número, por sí mismo, no es suficiente; toda vez que la IP debe estar acompañada de la hora exacta en que ha sido utilizada para cometer el ataque, ya que de lo contrario se podría caer en el error de asignarle responsabilidad a una persona distinta de la que se esta investigando[26].

[25] https://www.infobae.com/tecno/2020/09/05/quienes-estan-detras-del-hackeo-a-migraciones-y-como-funciona-netwalker-el-software-malicioso-utilizado/ (ultima vez visto: el 29 de mayo de 2021)

[26] Poveda Criado, Miguel Ángel, Delitos en la red, Madrid, Editorial Fragua, 2015, pp. 138 y ss.

Es fundamental el tiempo universal coordinado (UTC), que es el tiempo de la zona horaria de referencia respecto a la cual se calculan las otras zonas del mundo.

Un problema común en este tipo de casos es la diversidad de países en los que se podrían encontrar los autores, como así también la cantidad de ciudades en los que se podrían encontrar las potenciales víctimas.

Una característica importante es que no es fácil identificar a los autores de los ataques. En muchos casos se trata de organizaciones con conocimientos técnicos e informáticos para actuar en la *Deep Web*, enmascarar sus direcciones IP y, de ésta manera, asegurarse el anonimato[27].

A diferencia de la web superficial[28], la web profunda (*Deep Web*) abarca todo el contenido que nunca se encontrará como resultado de una búsqueda en un motor de búsqueda de internet, dado que por diferentes motivos quienes lo publican en internet no quieren que se identifique por ésta vía[29].

En consecuencia, es de vital importancia que las fuerzas policiales internacionales, como por ejemplo: *FBI*, *Homeland Security*, *Interpol*, *Europol*, etc., se encuentren dotados de herramientas disruptivas y de última generación para contrarrestar los ataques informáticos que cada día son más sofisticados y complejos.

[27] Sallis, Ezequiel, Desafíos de la investigación de los delitos informáticos en la *Deep* y *Dark* Web, en Cibercrimen, Buenos Aires, Editorial B de f, 2016, pp. 601 y ss.

[28] Es el término con el que se denomina a todo el contenido que cualquier persona puede encontrar y acceder como resultado de una búsqueda en un buscador de internet, como por ejemplo Google o Bing. Es decir que, si se busca la palabra "internacional" en un motor de búsqueda, cualquiera de los contenidos que aparezcan como resultado, forman parte de lo que se conoce como la web superficial.

[29] Sallis, Ezequiel, Desafíos de la investigación de los delitos informáticos en la *Deep* y *Dark* Web, en Cibercrimen, Buenos Aires, Editorial B de f, 2016, pp. 608.

f) Problemas y desafíos en el ambito de cooperación entre Estados

No cabe duda que el diseño e implementación de una política de persecución internacional de los ciberataques no es solamente un tema jurídico, sino también, político, de seguridad y de relaciones internacionales.

No es únicamente un tema de derecho penal sino de posicionamiento de política internacional en uno de los aspectos claves para las relaciones internacionales del futuro: la regulación de Internet, siendo un tema central para todos los Estados como así también ámbitos de organizaciones internacionales universales como Naciones Unidas, Consejo de Europa, Unión Europea, etc. o regionales y subregionales, como OEA, MERCOSUR, entre otras.

Debido a la transnacionalidad, como característica indiscutible de éste fenomeno, un tema fundamental, es cómo se van a posicionar los Estados en cuestiones tan trascendentales como la soberanía y el principio de territorialidad, la cooperación eficiente e igualitaria entre Estados, la protección de garantías individuales en entornos digitales, la relación con las empresas multinacionales del sector de la informática y las telecomunicaciones, entre otros.

En efecto, el desarrollo de la informática y de las telecomunicaciones ha planteado un desafío aún no resuelto a la cooperación internacional. La constante necesidad de obtener evidencia digital de los crímenes organizados, requiere de mecanismos que no han sido regulados de manera unniforme, poniendo en crisis pilares básicos como la noción de soberanía como límite al poder de un Estado para realizar medidas de prueba en otro Estado.

Tanto los tratados multilaterales como los bilaterales de asistencia en materia penal no resuelven los problemas que plantea la evidencia digital, generando inconvenientes prácticos en las investigaciones que luchan contra el crimen organizado.

Lo expuesto tiene relación con que, por ejemplo, las empresas de tecnología alojan la información en la nube. También lo hacen todos los ciudadanos cuando utilizan una cuenta

de correo electrónico internacional como *gmail* o *hotmail*, alojando también información en la nube.

¿Qué quiere decir que la información este alojada en la nube? Significa que la información puede estar en el servidor de un país pero también, y por razones económicas y estratégicas, puede estar alojada y fragmentada en servidores ubicados en cinco países diferentes.

Si aplicamos los métodos tradicionales relacionados con los principios de soberanía y territorialidad, no se podrá, en el marco de una investigación, acceder a esos datos representativos de la evidencia digital que se necesita para identificar un crimen organizado. En este sentido, uno de los temas más importantes que se está discutiendo en el mundo es el acceso transfronterizo de datos[30]; una de las cuestiones que mayor controversia que genera en los foros internacionales[31] y que repercutirá en las investigaciones de crímenes organizados, tanto en términos de eficiencia como en lo que respecta a la protección de las garantías y a los datos personales[32].

En ésta discusión se encuentran involucrados tanto intereses de política y estrategia internacional como intereses económicos, que incluyen a las grandes empresas de Internet y al desarrollo económico en los que el manejo de la información es cada vez más importante.

[30] Seitz, Nicolai. Transborder Search. A New Perspective In Law Enforcement, Yale Journal of Law and Technology, vol 7, 2005.

[31] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Draft Protocol version 2, 12 de Abril 2021, www.coe.int/cybercrime

[32] Ley Orgánica 7/2021, de 26 de mayo, de Protección de Datos Personales Tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de acciones penales. Publicada en Boletín Oficial del Estado (España) de, 27 de mayo de 2021.

Capítulo II: Requisitos y principios del Derecho internacional humanitario

Ya habiendo proporcionado al lector el contexto de los aspectos técnicos de los ciberataques y los desafíos que representan para los agentes estatales, a continuación, se analizará cómo se aplican los principios generales del Derecho internacional humanitario a los ataques informáticos.

En este capítulo, se determinará cuándo y en qué momento es posible aplicar esta rama del derecho como marco jurídico en un contexto donde los conflictos entre Estados han evolucionado en cuanto a su forma y, por lo tanto, dificultado, en algunas ocasiones, la aplicabilidad de las Convenciones de Ginebra y su Protocolo adicional (I).

En una primera sección, el capítulo se referirá a los aspectos normativos de los principios de distinción, proporcionalidad y precaución, que servirán para un futuro análisis de los casos ya mencionados.

Como se señaló anteriormente, los ataques informáticos no existían cuando las Convenciones de Ginebra fueron adoptadas. Sin embargo, este hecho no imposibilita su aplicación. En esta línea, el artículo 36 del Protocolo Adicional I previó la posibilidad de nuevos medios de guerra[33]. El Comité Internacional de la Cruz Roja (CICR), impulsores del Manual de Tallin y la doctrina concuerdan en señalar que el Derecho de los conflictos armados debe ser aplicado al ciberespacio[34].

[33]Artículo 36. Protocolo Adicional (I) https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977

[34] Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, pp. 343.

Sin embargo, antes de explicar cómo los principios tradicionales del Derecho internacional humanitario se aplican a ciberataques, es menester considerar cuáles son los requisitos generales que deben ser alcanzados para que esto tenga lugar. En términos generales, esos requisitos son dos: la existencia de un conflicto armado y de un agente responsable[35].

Con relación a la existencia de un conflicto armado, el artículo 2, común a los Convenios de Ginebra, estipula que el Derecho internacional humanitario será aplicable en conflictos armados[36]. Al respecto, el Tribunal Penal Internacional para la ex Yugoslavia (TPIY) ha manifestado que: "Existe un conflicto armado cuando hay un recurso a la fuerza armada entre Estados, o a la violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados, o entre estos grupos dentro de un Estado"[37].

Como veremos en el capítulo 3, a través de los casos seleccionados, pueden presentarse dos situaciones en cuanto a ciberataques: a) una en la que el ciberataque ha tenido lugar durante el transcurso de un conflicto armado; y b) otra, en la que los ataques informáticos han tenido lugar independientemente de un conflicto armado. En este último escenario, la pregunta es qué se considera "fuerza armada" en el contexto digital y en ausencia de fuerza cinética o violencia o utilización de armas tradicionales[38].

En primer lugar, es preciso tener en cuenta que no existe una definición consensuada de fuerza armada para este tipo de ataques[39]. Según Kai Ambos, debe seguirse un enfoque en

---

[35] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 5.

[36] Convenio de Ginebra (1949). Artículo 2: "... el presente Convenio se aplicará en caso de guerra declarada o de cualquier otro conflicto armado que surja entre dos o varias de las Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra".
https://www.icrc.org/es/doc/assets/files/publications/convenios-gva-esp-2012.pdf

[37] *Prosecutor v. Tadic. ICTY-94-1-AR. October 2nd,1995.*

[38] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 542 y ss.

[39] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 6 y ss.

los efectos producidos por el ciberataque, esto es, analizar las consecuencias en lugar de los medios utilizados[40]. En sus palabras: "Si el ataque informático logra reemplazar al elemento físico de la red informática atacada, entonces satisface el requisito de la fuerza armada o del ataque armado del Derecho internacional humanitario"[41]. Esto implica, por otra parte, que si un ataque informático no causa ningún daño físico (permanente) o funcionalmente serio (por ejemplo, un apagón o el colapso temporal de un sistema computarizado) no satisface dicho requisito[42]. Por lo tanto, la pregunta es siempre si un ciberataque causa un daño comparable o análogo a un ataque armado tradicional[43]. En esta línea, si un ciberataque es análogo a los efectos producidos por medios cinéticos y resulta posible atribuir responsabilidad a un Estado, el desencadenamiento de un conflicto armado internacional es inminente[44].

Otro punto es la atribución del ciberataque a una parte, de acuerdo con las Convenciones de Ginebra y las normas internacionales sobre responsabilidad estatal. Esto puede resultar difícil en entornos cibernéticos. Como fue explicado en el marco teórico, uno de los principales atributos de los ataques informáticos es que la responsabilidad puede volverse difusa. Por ejemplo, los ataques distribuidos de denegación de servicio, donde diferentes computadoras, que pueden estar ubicadas en cualquier lugar del mundo, son coordinadas para lanzar un ataque, como en el caso de Estonia (ver capítulo III).

Ahora bien, las definiciones y los ejemplos de ataques informáticos establecidos anteriormente en el trabajo son importantes para analizar las implicancias del primer

[40] Ibídem.
[41] Ibídem.
[42] Ibídem.
[43] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 546 y ss.
[44] Ibídem.

principio del Derecho internacional humanitario, el de distinción. Sólo cuando el umbral que define a un ataque es alcanzado es que las prohibiciones del principio de distinción operan en casos de ataques a la red cibernética[45]. Cuando ataques a la red informática son utilizados en un conflicto armado, los blancos selectos deben ser objetivos militares y los principios de distinción, proporcionalidad y precaución deben ser respetados[46].

Sin embargo, la mayoría de las restricciones, aunque no todas, dependen del concepto de ataque y no todos los ataques a las redes informáticas alcanzan este nivel. La pregunta, entonces, es cuándo un ataque a una red informática implica un ataque, para aplicar los principios del Derecho internacional humanitario y qué restricciones se aplican en aquellos casos en los que no se ha alcanzado el umbral de ataque[47].

El término "Ataque" se encuentra definido en el artículo 49 (1) del Protocolo Adicional a los Convenios de Ginebra como actos de violencia contra el adversario, sean ofensivos o defensivos[48].

El Manual de Tallin define "ataque" como una "operación cibernética, sea ofensiva o defensiva, que se espera que cause lesión o muerte a las personas o dañe o destruya objetos"[49].

En cuanto a los "actos de violencia", ha sido acordado que el concepto no refiere solo a medios cinéticos: por ejemplo, el uso de armas químicas constituye un ataque, a pesar de que

[45] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo. 92.
[46] Dinniss Harrison, Heateher. "Cyber Warfare and the Laws of War." Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012. pp. 179.
[47] Dinniss, Ibídem.
[48] Artículo 49. Protocolo Adicional (I) https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#NORMA-FUNDAMENTAL
[49] Schmitt, Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017, página 61.

no haya uso de fuerza física[50]. Ciberataques que comprenden bombas lógicas, virus o gusanos, cuyas consecuencias implican daño físico a personas u objetos más allá de la mera computadora o sistema, pueden clasificarse como "actos de violencia" y, por lo tanto, constituyen un ataque según la Ley de la Guerra[51]. Como señalan varios autores, la violencia es analizada en términos de "efectos", en lugar de la "naturaleza" del acto[52]. Califica, por ejemplo, una operación cibernética que altera el funcionamiento de un sistema SCADA que controla una red eléctrica y da como resultado un incendio. Dado que las consecuencias son destructivas, la operación es un ataque[53].

Existe, no obstante, cierto desacuerdo en cuanto a lo que significa "daño" al analizar las consecuencias de un ciberataque. Schmitt indica que hubo una intensa discusión dentro del Grupo Internacional de Expertos a invitación del Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (en adelante, "Grupo de Expertos"), sobre si la interferencia por medios cibernéticos con la funcionalidad de sistemas constituye daño en el contexto del artículo 92 del Manual de Tallin. Indicó que la mayoría consideró que afectar la funcionalidad calificaría como daño solo si la restauración de la funcionalidad requería el reemplazo de componentes físicos[54].

---

[50] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Articulo 92.

[51] Dormann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." 2004, pp.4 Published in https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf ,visto: 06/10/2021.

[52] Ibídem, Droege Cordula, pp. 546; Ibídem, Dormann Knut, pp. 4**;** Ambos, Kai, "International Criminal Responsability in Cyberspace" in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, pp. 124.

[53] Schmitt Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017, página 61.

[54] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 92.

Al mismo tiempo, dado que en otra parte de la misma sección del Protocolo Adicional (I), en la definición de objetivo militar, se hace referencia a la neutralización de un objeto como posible resultado de un ataque, puede deducirse, según Dormann, que la mera inhabilitación de un objeto, como el apagado de la red eléctrica, sin destruirla también debe calificarse como un ataque[55]. En la misma línea, Ambos argumenta que el tratamiento igualitario de "destrucción" y "neutralización" en el artículo 52 (2) del Protocolo Adicional (I)[56] parece sugerir una interpretación más flexible en lugar de solo "daño análogo a la fuerza armada tradicional". La neutralización de un objetivo militar puede producir la misma ventaja militar y, por lo tanto, tener las mismas consecuencias que destruir el objeto[57].

Como Christakis resalta, un problema que surge de la prueba de "efectos" es que a veces la extensión del daño solo se puede ver a largo plazo. Esto lleva a la pregunta de cuándo evaluar el "ataque": días, meses o años después?[58].

¿Se consideraría un "ataque" la interrupción de la comunicación por correo electrónico en un país? El Grupo de Expertos concluyó que el Derecho de los Conflictos Armados no cubre este escenario[59]. Además, los ciberataques que cusan meros inconvenientes o irritación no constituyen "ataques". Sin embargo, cabe destacar lo que señala Droege en cuanto al término "inconveniencia":

---

[55] Dormann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." 2004, pp.4 Published in https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf ,visto: 06/10/2021.

[56] Artículo 52 (2). Protocolo Adicional (I) https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#NORMA-FUNDAMENTAL

[57] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 7 y ss.

[58] Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, p. 349/350

[59] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 92.

"Si bien el criterio de inconveniencia no está exento de méritos, puede haber desacuerdo sobre qué representa inconveniente en términos de interferencias con la ciber tecnología y la comunicación. Por ejemplo, si bien es posible estar de acuerdo en que la interrupción de un sistema de reservas en línea causa meros inconvenientes, el consenso puede ser más difícil de lograr en torno a cuestiones como la interferencia con los servicios bancarios. Queda por ver cómo se considerarán estas interferencias en el futuro, en particular en la práctica estatal"[60].

a) El principio de distinción y ciberataques

El principio de distinción requiere que se haga una distinción entre civiles y combatientes, y entre objetivos militares y bienes de carácter civil.

El artículo 48 del Protocolo Adicional (I) dice: "A fin de garantizar el respeto y la protección de la población civil y los bienes de carácter civil, las partes en conflicto distinguirán en todo momento entre la población civil y los combatientes y entre los bienes de carácter civil y los objetivos militares y, en consecuencia, sus operaciones solo contra objetivos militares"[61].

La distinción es fundamental para definir si se cometió un crimen de guerra o si tuvo lugar un acto lícito en un conflicto armado. Esto también aplica a ciberataques[62].

[60] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 560 y ss.
[61] Artículo 48. Protocolo Adicional (I). https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#NORMA-FUNDAMENTAL
[62] Schmitt Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017, pp 63 y ss.

El Grupo de Expertos indica que el principio de distinción se aplicará a las operaciones cibernéticas contra bienes de carácter civil cuando alcancen el umbral de "ataque", como se explicó anteriormente[63].

La pregunta que surge es si el principio de distinción se aplica solo a las operaciones cibernéticas en general o solo a aquellas que caen dentro de la definición de ataque[64].

Algunos autores han argumentado que este tema es preocupante desde el punto de vista de la población civil, ya que habilita y amplía el abanico de objetivos legítimos, debido a que las operaciones cibernéticas pueden no causar daño físico y por lo tanto quedan fuera del alcance del principio de distinción. En este sentido, se ha argumentado: "La naturaleza potencialmente no letal de las armas cibernéticas puede enturbiar la evaluación de la legalidad de un ataque, lo que lleva violaciones más frecuentes del principio de distinción en esta nueva forma de guerra que en la guerra convencional"[65]. Christakis señala que los civiles y los bienes de carácter civil pueden ser objetivos legítimos si no hay daños físicos como resultado de la operación cibernética, o si no se puede probar[66].

En esta línea, es oportuno recordar que el vínculo entre el ciberataque y sus consecuencias puede ser difícil de determinar, y sus consecuencias pueden verse mucho tiempo después del ataque.

---

[63] Ibídem

[64] Lubell, Noam. "Lawful Targets in Cyber Operations: Does the principle of distinction apply?" International Law Studies, US Naval War College. Vol. 89. 2013. p. 260.

[65] Kelsey T. G. Jeffrey. "Hacking into International Humanitarian Law: The principle of Distinction and Neutrality in the Age of Cyber Warfare." Michigan Law Review. 2008. p. 1439.

[66] Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, pp. 354.

A su vez, otros autores sostienen que el principio de distinción debe aplicarse no solo a los ataques a redes informáticas, sino también a las operaciones militares en el ciberespacio en el contexto de las hostilidades[67]. En este sentido, Dinniss sostiene que los principios de distinción, proporcionalidad y precaución se aplican a los ciberataques que alcanzan el umbral antes mencionado, pero también a las operaciones militares. Esto podría entenderse a la luz del artículo 48 del Protocolo (I) y los capítulos de los artículos 51 y 57[68] que, de otra manera, serían superfluos[69]. Christakis sostiene además que debe adoptarse un enfoque dinámico, de modo que el principio de distinción pueda ser reinterpretado de acuerdo con las nuevas realidades a fin de respetar sus metas y propósitos: la protección de los civiles de los efectos de las guerras[70].

b) Los principios de proporcionalidad y precaución

El principio de proporcionalidad establece límites al uso de los medios y métodos de guerra y prohíbe aquellos que causen males superfluos o sufrimientos innecesarios[71]. Dicha regla encuentra su fundamento en los artículos 51 (4) y 57 (2) del Protocolo Adicional (I)[72] y define a los ataques indiscriminados como aquellos que generan pérdidas de vidas civiles y daños a

[67] Ibídem.
[68] Artículo 48. Protocolo Adicional (I). Artículo 51 (I): "La población civil y las personas civiles gozarán de protección general contra los peligros procedentes de operaciones militares...". Artículo 57 (I): "Las operaciones militares se realizarán con un cuidado constante de preservar a la población civil, a las personas civiles y a los bienes de carácter civil". https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#NORMA-FUNDAMENTAL
[69] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 556 y ss.
[70] Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, pp. 346.
[71] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 17.
[72] Ibídem.

los bienes civiles que son "excesivos en relación con la ventaja militar concreta y directa prevista"[73]. En general, se conoce al principio como Regla de proporcionalidad, pero como una cuestión técnica legal, el tema sería de excesividad[74].

Este principio también se aplica a los ataques cibernéticos que causan un daño colateral excesivo, ya sea durante la utilización transitoria de la infraestructura civil, o bien a través del ataque mismo[75]. Si se siguiera la postura estricta de que cualquier uso militar potencial de un bien civil lo transforma en un objetivo militar, el bien referido sería un objetivo lícito y solo el estándar de proporcionalidad excesiva brindaría posibles límites a los ataques cibernéticos[76]. Sobre este tema se profundizará más adelante.

Por último, en cuanto al principio de precaución, su objetivo general es minimizar los daños civiles en la mayor medida posible, sin perjuicio de cualquier consideración de proporcionalidad.

Este principio tiene dos componentes: a) las precauciones en el ataque y b) las precauciones contra los efectos de los ataques[77].

La omisión de adoptar estas precauciones puede convertir en un crimen de guerra lo que de otra manera sería un ataque permitido contra una persona o bien civil.

[73] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 17.
[74] Schmitt Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017, pp. 87.
[75] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Pp. 160, cit. Kai Ambos, pp. 18
[76] Ibídem, pp. 18.
[77] Cfr. artículos 57 (2) y 58 del Protocolo Adicional (I) de la Convención de Ginebra.

CAPITULO III: Casos de ataques informáticos internacionales. Estonia (2007); Georgia (2008); Stuxnet (2010).

En los últimos años, hubo reportes sobre ciberataques que contribuyen a clarificar la magnitud y el alcance de estos fenómenos.

Un caso muy conocido fue el de Stuxnet. En junio de 2010, una empresa de antivirus bielorrusa informó de un gusano informático encontrado en las redes de sus clientes iraníes. Las consecuencias de la infección duraron meses y se determinó que el gusano era en realidad un software malicioso sofisticado que se suponía que afectaba a las centrifugadoras nucleares de la instalación de enriquecimiento de combustible nuclear en Natanz en Irán. El *malware* afectó la velocidad de las centrifugadoras giratorias[78]. Stuxnet es un ejemplo de cuán diligente puede ser un ciberataque, logrando el objetivo militar exacto sin afectar a ningún civil. Solo afectó a los sistemas informáticos fabricados por Siemens, relacionados con la planta nuclear de Natanz. En ese contexto, los expertos concluyeron que "Stuxnet" cumplía con los criterios de distinción. Sin embargo, Stuxnet no se realizó en un contexto de conflicto armado, por lo que no fue evaluado bajo las normas del Derecho de los Conflictos Armados[79].

Otro caso fue el de los ciberataques a Estonia en 2007. La Unión Soviética colocó una estatua de bronce en Tallin, Estonia, durante la Segunda Guerra Mundial. Los estonios vieron la estatua como un símbolo de la ocupación soviética y la represión política. Por otro lado, los rusos étnicos en Estonia vieron la estatua como un tributo a los soldados soviéticos caídos.

[78] Miller, Kevin. "The Kampala Compromise and Cyberattacks: Can there be an International Crime of Cyber-Agression?" Southern California Interdisciplinary Law Jorunal. Vol. 23. 2014. pp. 222.
[79] Kilovaty, Ido. "Virtual violence, disruptive cyber-space operations as "attacks" under international humanitarian law." 23 Mich. Telecomm. Tech. L. Rev. 113. pp. 16.

Como resultado, en abril de 2007, el gobierno de Estonia decidió retirar la estatua. Tras esta decisión, hubo dos noches de protestas masivas y disturbios en Estonia, conocidas como la "Noche de Bronce". En las semanas siguientes, la infraestructura digital de Estonia experimentó un ciberataque masivo originado principalmente en Rusia[80]. La modalidad utilizada para el ataque fue un ataque masivo de denegación de servicio distribuido (DDoS). Los objetivos específicos influyeron noticias y sitios web gubernamentales. Resultó imposible determinar quién dirigió la operación, pero existían sospechas de participación rusa. Durante el ataque, se cortaron varias líneas telefónicas, así como servicios de emergencia, lo que podría haber puesto en peligro vidas humanas. Dichos ataques informáticos no fueron considerados (públicamente) ni por Estonia ni por la comunidad internacional como un ataque armado. El Grupo de Expertos estuvo de acuerdo en que no se alcanzó el umbral de escala y efectos[81].

En 2008, se produjo otro ciberataque en las redes de Georgia. En agosto de 2008, los conflictos entre Georgia y Rusia por las regiones separatistas de Abjasia y Osetia del Sur generaron un conflicto armado. Hubo ataques cinéticos y ciberataques operados desde Rusia. Específicamente, un ataque distribuido de denegación de servicio masivo tuvo como objetivo los sitios web del gobierno de Georgia, publicando imágenes de Adolf Hitler con el presidente georgiano. Los sitios web gubernamentales también fueron atacados cuando se realizaron ataques físicos, lo que dificultó especialmente la comunicación. Los servidores de

[80] Gervais, Michael. "Cyber Attacks and the Laws of War." 30 Berkeley J. Int'l L. 525. p. 12.
[81] Schmitt Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017, pp. 36.

CNN y BBC en Georgia también fueron atacados, bloqueando el acceso a noticias internacionales[82].

Por último, otro caso que vale la pena mencionar es el de Corea del Sur. En marzo de 2013, las empresas de radiodifusión y los bancos fueron objeto de un ataque mediante una "bomba lógica" en Corea del Sur. El *malware* infectó y afectó a los servidores, así como a las computadoras: más de 50,000. Corea del Norte fue acusada de estar detrás del ataque. "Mientras tanto, el colectivo de hackers Anonymus tomó represalias apuntando a una agencia de noticias estatal de Corea del Norte por incitar una supuesta guerra. Corea del Norte respondió a estas afirmaciones negando su participación y amenazando con una "guerra termonuclear" contra el Sur[83].

Como se puede ver, los ciberataques pueden adoptar diversas formas. Los virus se pueden utilizar para infectar sistemas y destruir o afectar el funcionamiento de la red. Además, los virus pueden ser portadores de *malware*, que permanece oculto y sin ser detectado en los sistemas, con el objetivo de recopilar información, alterarla o destruirla.

[82] Gervais, Michael. "Cyber Attacks and the Laws of War." 30 Berkeley J. Int'l L. 525. p. 12.
[83] Miller, Kevin. "The Kampala Compromise and Cyberattacks: Can there be an International Crime of Cyber-Agression?" Southern California Interdisciplinary Law Jorunal. Vol. 23. 2014. pp. 226.

Capítulo IV: Desafíos en la aplicación del principio de distinción en el ciberespacio

Es necesario diferenciar cuando los ataques son contra las personas o contra objetos.

a) Ataques contra personas

Hay cuatro grupos de personas que pueden ser objetivos legítimos[84]. Primero, miembros de las fuerzas armadas. En segundo lugar, miembros de grupos organizados. Estas categorías están estrictamente relacionadas con el estado de las personas. El tercer grupo es el de los civiles que participan directamente en las hostilidades y, finalmente, los participantes en un "levantamiento en masa" en un conflicto armado internacional. Las dos ultimas categorías dependen de la conducta en la que se involucren los civiles.

Las opiniones del Grupo de Expertos estuvieron divididas cuando se discutió el alcance de los "grupos organizados". Por un lado, se afirmó que cuando se demuestra que la persona es parte de un grupo organizado, se convierte en un objetivo legítimo. Por otro lado, algunos expertos enfatizaron que se debe tratar de un estatus continuo; de lo contrario, las personas se considerarán civiles y se convertirán en objetivos legítimos solo en el momento en que participen efectivamente en las hostilidades. Cabe señalar con respecto a esta última opinión, que el lanzamiento de un ciberataque puede durar unos minutos y ser prácticamente imposible identificar al perpetrador durante el período en el que esté participando activamente en las hostilidades[85]. Será diferente al caso en que un agricultor dedica toda su

[84] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 92.

[85] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 96, comentarios 4 y 5.

vida a la finca, pero una vez al día, durante quince minutos, dispara un cohete al enemigo en un conflicto en curso, y por lo tanto se convierte en un objetivo durante ese período de tiempo. Este es el enfoque de la Cruz Roja, pero puede ser muy difícil de aplicar en la realidad a los ciberataques, debido a sus características únicas, explicadas anteriormente.

Puede surgir otra pregunta con respecto a los grupos que no pertenecen a una de las partes en conflicto. ¿Serían estos grupos objetivos legítimos si lanzaran un ciberataque, pero por otras razones, como objetivos étnicos o religiosos? La opinión del Grupo de Expertos volvió a estar dividida: algunos de ellos argumentaron que debían ser tratados como civiles y solo podían ser atacados en el momento en que participaban en las hostilidades, mientras que otros expertos sostuvieron que no era necesario que estas personas pertenecieran a una de las partes, y que puedan ser objetivos debido a su conducta.

En relación con los civiles que participan en las hostilidades, el artículo 51 (3) del Protocolo Adicional (I) establece: "Los civiles gozarán de la protección que brinda esta Sección, a menos que toman parte directa en las hostilidades y mientras dure tal participación". No forman parte de grupos armados organizados, pero como en el caso del campesino que dispara un cohete todos los días durante quince minutos, participan en las hostilidades y pueden contribuir con un ataque, por lo que pueden convertirse en un objetivo legítimo.

Imaginar, por ejemplo, un ataque distribuido de denegación de servicio (DDoS). Como se mencionó en el marco teórico, si el perpetrador utiliza una "botnet" para lanzar el ataque coordinado, ¿las computadoras "zombis" se convertirían en un objetivo legítimo? Para hacer la evaluación y analizar la "participación directa en las hostilidades" en las operaciones cibernéticas, muchos autores se basan en la clasificación con tres criterios acumulativos

establecidos por la Guía Interpretativa del Comité Internacional de la Cruz Roja[86]: 1. Un umbral de daño: la operación debe afectar las operaciones militares o la capacidad del adversario, o infligir la muerte, daño físico o destrucción material a personas u objetos protegidos contra un ataque directo. 2. El vínculo causal: debe existir una conexión probada entre el acto y el daño infligido o pretendido. 3. El nexo beligerante: el acto debe estar relacionado con las hostilidades.

Es posible notar que el umbral es más bajo que los requisitos para un "ataque". Christakis indica que muchos civiles pueden estar involucrados en una amplia gama de operaciones cibernéticas y, por lo tanto, convertirse en objetivos legítimos "incluso si en realidad no presionan el botón que lanza un ciberataque"[87].

Volviendo al ejemplo del ataque distribuido de denegación de servicios (DDoS), las computadoras "zombis" que lanzaron el ataque no serían objetivos legítimos. Más allá de la evaluación de los tres criterios, es importante comprender las características del ciberataque. En este caso, los civiles no tenían idea de que sus computadoras fueron utilizadas para el ciberataque. Sin embargo, y como se verá, los propios ordenadores pueden ser contraatacados para detener el ataque. Si se identifica al autor real - lo cual puede resultar complicado en estos casos por la complejidad de la acción -, esa persona se convertiría en un blanco legítimo durante el ataque.

En este sentido, ¿una persona encargada de mantener los equipos en una instalación militar es un objetivo legítimo? Según el Grupo de Expertos, esto no alcanzaría el umbral y, por lo

[86] Schmitt Michael N., El Manual de Tallin *2.0 (traducido al español),* Cambridge University Press, Reino Unido, 2017, pp. 67.

[87] Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, pp. 363/364

tanto, esa persona no sería un objetivo legítimo según el principio de distinción[88]. ¿Y una persona que está diseñando un *malware* específicamente destinado a deshabilitar, por ejemplo, la red militar de una de las partes a través de la cual se activan los ataques cinéticos? Esto encajaría con los criterios. Sin embargo, el Grupo de Expertos planteó algunas dudas con respecto al *malware* diseñado para lanzar un ataque, pero en el que el diseñador no sabe quién es el objetivo. Esto pone en duda el cumplimiento del vínculo causal entre el acto de proporcionar el *malware*[89].

Otro problema que debe abordarse - y se señaló anteriormente en relación con la expresión "por tal tiempo" en lo que respecta a los civiles que participan directamente en las hostilidades - es la cuestión de cuándo comienza y cuándo termina la participación del civil que los convierte en blanco legítimo. Hasta ahora, se sabe que los ciberataques pueden durar segundos, minutos, horas o incluso meses. Algunos comentaristas dan el ejemplo de una "bomba lógica". Como se ha explicado, este tipo de ataques se lanzan después de que se activa un disparador. Esto puede llevar tiempo, ya que el desencadenante puede ser una acción requerida por la víctima. ¿Es el civil que instaló el *malware* un objetivo legítimo durante el tiempo que se colocó la "bomba lógica" en el sistema, pero no se activó? El Grupo de Expertos ha enfatizado que el civil será un objetivo legítimo "desde el comienzo de su participación en la planificación de la misión hasta el momento en que termine su papel activo en la operación. [...] La duración de la participación directa iría desde el comienzo de la planificación de cómo colocar la bomba lógica hasta la activación por orden de ese

[88] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 97, comentario 6.
[89] Ibídem.

individuo"[90]. Se sostiene además que una interpretación más amplia, como entender que la persona sería un objetivo legítimo hasta que cesen los efectos de sus acciones, sería peligrosa[91]. La participación en el contexto de este tipo de ataques sería ilimitada.

Estas conclusiones preliminares, sin embargo, no resuelven todos los escenarios que pueden presentarse. ¿Qué pasa con los civiles que lanzan varios ataques durante un mes? ¿La intervención en la hostilidad comienza y termina cuando el civil presiona el botón, o se deben considerar los ataques como una actividad continua, para que la persona sea un objetivo todo el tiempo?

"Algunos de los expertos adoptaron la posición, adoptada en las Orientaciones Interpretativas del Comité Internacional de la Cruz Roja, de la que cada acto debe tratarse por separado en términos de análisis de participación directa. Otros expertos argumentaron que esta posición tiene poco sentido operativo. Crearía una "puerta giratoria" de participación directa y, por lo tanto, de capacidad de selección. Para estos Expertos, la participación directa comienza con la primera operación cibernética y continúa durante todo el período de actividad intermitente"[92].

b) <u>Ataques contra objetos</u>

[90] Ibídem. Comentario 9.

[91] Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, p. 363/364

[92] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Articulo 97, comentario 11.

Hay algunos problemas que surgen en relación con los bienes civiles y los objetivos militares. Los bienes de carácter civil se definen en el artículo 52 (1) del Protocolo Adicional (I) en sentido negativo[93]. El artículo 100 del Manual de Tallin establece: "Los bienes de carácter civil son todos los bienes que no son objetivos militares. Los objetivos militares son aquellos objetos que, por su naturaleza, ubicación, finalidad o uso, contribuyen eficazmente a la acción militar y cuya destrucción, captura o neutralización total o parcial, en las circunstancias que imperen en el momento, ofrece una clara ventaja militar. La infraestructura cibernética puede calificar como un objetivo militar"[94].

Una pregunta que se debe realizar después de leer el artículo es la siguiente: ¿Se incluye "datos" en el término "objeto"? ¿Pueden los datos ser un objetivo lícito? La posición mayoritaria es que el término "objetos" solo cubre los objetos tangibles y visibles. Por lo tanto, un ataque a datos que son intangibles no califica como un "ataque". Sin embargo, el Grupo de Expertos ha señalado que una "operación cibernética dirigida a datos a veces puede calificar como un ataque cuando la operación afecta la funcionalidad de la infraestructura cibernética o da como resultado otras consecuencias que calificarían la operación cibernética en cuestión como un ataque"[95]. Dinniss sostiene que "el mero hecho de la intangibilidad no debería impedir *per se* que un fragmento de código sea un objetivo militar si cumple con los

[93] Artículo 52 (1) P.A (I) dicta: "Los bienes de carácter civil no serán objeto de ataques ni represalias. Son bienes de carácter civil todos los bienes que no son objetivos militares en el sentido del párrafo 2.". Artículo 52 (2) P.A (I) dicta: Los ataques se limitarán estrictamente a los objetivos militares. En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida." https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#NORMA-FUNDAMENTAL

[94] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 100, comentario 7.

[95] Ibídem, Artículo 100, Comentario 7.

demás criterios establecidos en el artículo 52 (2) del Protocolo Adicional (I)... en el mundo actual de creciente virtualización y extensiva interdependencia entre la infraestructura militar y civil, que requiere resultados tangibles, es un resultado manifiestamente irrazonable. Tal resultado es incompatible con otros tratamientos de la intangibilidad en el Derecho internacional humanitario y contrario al propósito expreso de brindar protección efectiva a civiles y bienes de carácter civil. Por lo tanto, independientemente de su intangibilidad, el código puede calificar como un objetivo militar al proporcionar una contribución efectiva a la acción militar ya sea por su naturaleza, ubicación, propósito o uso"[96].

Una minoría en el Grupo de Expertos sostiene que, a efectos de focalización, determinados datos podrían considerarse un objeto. Según la opinión mayoritaria -no considerar los datos como un objeto-, varios datos esenciales para la población civil quedarían fuera de la protección, en contra de lo dispuesto en el artículo 48, Protocolo I. Se debe proteger la eliminación de datos civiles esenciales como la seguridad social y las cuentas bancarias[97].

Lubell también sostiene que no aceptar los datos como un objeto plantea la cuestión de si un ataque cinético que resulta en la destrucción de miles de bolsas de correo es más dañino que un ataque cibernético que borra millones de correos electrónicos. En su opinión, el análisis debería centrarse en el daño contra el contenido de los datos y no en el daño físico a un sistema informático[98]. Según Kilovaty "Los datos deben verse como un objeto, ya que cualquier otra propuesta comprometería los datos por completo. La consideración de si la

[96] Dinniss Harrison, Heateher. "Cyber Warfare and the Laws of War." Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012. pp. 179. También ver: Ambos, Kai, "International Criminal Responsability in Cyberspace" in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015, pp. 131.

[97] Lubell, Noam. "Lawful Targets in Cyber Operations: Does the principle of distinction apply?" International Law Studies, US Naval War College. Vol. 89. 2013. p. 267.

[98] Ibídem, Lubell, pp. 267.

operación cibernética dirigida a los datos es un "ataque" debería depender de tres factores: (1) una operación que comienza en el ciberespacio o en un sistema informático; (2) es de naturaleza interrumpida, el compromiso o la pérdida de datos está interrumpiendo la vida cotidiana de los civiles; y (3) es violento, es decir, los datos son críticos, el daño es irreversible y los efectos son prolongados"[99].

Como se indicó anteriormente, los objetos pueden calificar como objetivos militares de acuerdo con una prueba de cuatro criterios: naturaleza, ubicación, uso y propósito.

Los objetos que contribuyen por su naturaleza a las acciones militares incluyen armas, transporte, fortificaciones, edificios ocupados por las fuerzas armadas, etc. En lo que respecta a los ataques a redes informáticas, los objetivos pueden incluir sistemas de armas, conjuntos de sensores, redes militares[100].

Otra posibilidad es que puedan representar una ventaja militar debido a su ubicación. A veces puede resultar importante denegar un servicio de red al enemigo cuando su ubicación juega un papel en los ataques informáticos. Durante un conflicto armado, la interrupción de determinados medios de comunicación representaría una clara ventaja, siempre sujeta al principio de proporcionalidad[101].

En cuanto al uso, se establece que "cuando un objeto o instalación civil se utiliza con fines militares, se convierte en objetivo militar a través del criterio de "uso"[102]. En relación con el propósito, "se refiere al uso futuro previsto de un objeto, es decir, el objeto no se está

[99] Kilovaty, Ido. "Virtual violence, disruptive cyber-space operations as "attacks" under international humanitarian law." 23 Mich. Telecomm. Tech. L. Rev. 113. pp. 16 y ss.
[100] Dinniss Harrison, Heateher. "Cyber Warfare and the Laws of War." Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012. pp. 185.
[101] Ibídem, Dinniss, pp. 187.
[102] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Articulo 100. Comentario 10.

utilizando actualmente con fines militares, pero se espera que se utilice en el futuro. Adquiere la condición de objetivo militar tan pronto como se hace evidente"[103].

En cuanto a la contribución efectiva a la acción militar, la doctrina está dividida en su interpretación. Por ejemplo, Estados Unidos reemplazó el término "acción militar" por la idea de capacidad de "sostener la guerra" o "luchar en la guerra". Por lo tanto, de acuerdo con esta interpretación, "los objetivos económicos del enemigo que de manera indirecta pero efectiva apoyan y sostienen la capacidad de guerra del enemigo también pueden ser atacados"[104]. Por ejemplo, desde este punto de vista, sería lícito "lanzar ataques cibernéticos contra la industria de exportación de petróleo del Estado enemigo si el esfuerzo de guerra depende de los ingresos de las ventas de petróleo"[105].

Esta opinión es rechazada por la mayoría de la comunidad internacional. Droege indica que el Derecho internacional humanitario nunca permite dañar la capacidad económica de un Estado, independientemente de la ventaja militar que esa acción pueda brindar. De lo contrario, no habría límites y toda la economía de un país puede considerarse "sostenible de la guerra"[106]. Se ha dicho que la conexión entre las actividades de mantenimiento de la guerra y las acciones militares es demasiado remota[107].

En cuanto a la ventaja militar definitiva, conviene recordar el artículo 52 (Protocolo Adicional. I) cuando establece que la destrucción, captura o neutralización del objeto debe

[103] Ibídem, Artículo 200. Comentario 13.
[104] Ibídem.
[105] Ibídem. Artículo 100. Comentario 18.
[106] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 562.
[107] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 100, comentario 19.

proporcionar esta ventaja. La ventaja debe ser de naturaleza militar. Dinniss señala que la ventaja está relacionada con la ventaja del ataque en su conjunto y no con sus partes aisladas[108].

c) El problema del "uso dual" de objetos.

Esto trae el problema de los objetos de "uso dual". En este tema, el Manual de Tallin establece en el artículo 101 que "la infraestructura cibernética utilizada tanto para fines civiles como militares es un objetivo militar". En este sentido, el Grupo de Expertos sostiene que en casos poco claros, cuando no sabemos qué conexiones a Internet se utilizan con fines militares, toda la red califica como objetivo militar. Sin embargo, el ataque debe limitarse a segmentos discretos[109]. Como afirma Dinniss, esto puede ser relevante para países como Estados Unidos, donde la mayoría de las comunicaciones militares se transmiten a través de redes civiles y, por lo tanto, se convierten en un objetivo potencial para ataques a las redes informáticas[110]. En este sentido, este tipo de ataques deben analizarse a la luz del principio de proporcionalidad y precaución. El Grupo de Expertos destaca que estos objetivos duales podrían ser blancos siempre que contribuyan eficazmente a la acción militar, con sujeción a una ventaja militar definitiva[111].

Droege también sostiene lo siguiente: "[...] la mayor parte de la infraestructura cibernética en todo el mundo es de naturaleza de doble uso y podría considerarse un objetivo militar,

[108] Dinniss Harrison, Heateher. "Cyber Warfare and the Laws of War." Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012. pp. 191.
[109] Ibídem. Artículo 101. Tallinn Manual. Ver Artículo 52 (2) Protocolo I.
[110] Dinniss Harrison, Heateher. "Cyber Warfare and the Laws of War." Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012. p. 184.
[111] Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017. Artículo 101, comentario 1-4.

esto plantea la cuestión fundamental de los límites geográficos del conflicto armado. Realmente no hay fronteras en el ciberespacio, y los sistemas informáticos desde cualquier lugar pueden ser atacados, manipulados o transformados (de forma remota) en medios de guerra y objetivos militares. Debe tenerse en cuenta que la consecuencia no solo sería que dichos equipos podrían ser contraatacados por los sistemas informáticos blanco. En teoría, como objetivos militares podrían ser destruidos por medios cinéticos"[112]. La autora sostiene además que, en este sentido, el principio de distinción parece brindar poca protección a los civiles en el ciberespacio: la principal protección legal será el principio de proporcionalidad. Dinniss da el ejemplo de los sistemas de posicionamiento global (GPS) como un sistema dual: la interrupción de este sistema a través de un ciberataque causaría una interrupción masiva y potencialmente pondría en peligro la vida de civiles. Además, sostiene que estos objetivos de doble uso son atractivos debido a su potencial para obtener beneficios militares y políticos[113].

Kai Ambos argumenta que, en la infraestructura cibernética, debido a que los sistemas informáticos civiles y militares son difíciles de distinguir (ambos pueden tener fines civiles y militares al mismo tiempo), el principio de distinción tiene una importancia práctica limitada. En esta línea, Ambos brinda el ejemplo en que una parte en conflicto utiliza un sistema de información - per se civil - de un hospital para lanzar un ciberataque, estos sistemas de información se convierten en objetivos militares[114].

[112] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 565.
[113] Dinniss Harrison, Heateher. "Cyber Warfare and the Laws of War." Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012. pp. 195.
[114] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 15 y ss.

d) Prohibición contra ataques indiscriminados

Una consecuencia más del principio de distinción es la prohibición de ataques indiscriminados[115]. Según Droege, existe una carga doble para las partes. Primero, no deben emplear armas que sean indiscriminadas por naturaleza o incontroladas.

En segundo lugar, la parte debe verificar si el arma empleada en el ataque puede estar y está dirigida contra un objetivo militar específico[116]. Existe, sin embargo, cierto riesgo de que los ataques puedan ser indiscriminados debido a la interconexión del ciberespacio. En este sentido, sería difícil creer que sea posible cumplir con esta prohibición de la misma manera en que ocurre con los ataques tradicionales[117].

Ambos indica que un ataque indiscriminado se diferencia de un ataque directo contra bienes civiles en que el atacante no está realmente tratando de dañar a la población civil, el daño a los civiles es simplemente un asunto que no le preocupa al atacante[118].

Como se explicó en el Capítulo III, el caso Stuxnet es un ejemplo de lo diligente que puede ser un ciberataque, logrando el objetivo militar exacto sin ningún efecto a los civiles. Solo afectó a los sistemas informáticos fabricados por Siemens, relacionados con la planta nuclear de Natanz. No obstante, podría darse el caso de que un virus o gusano afecte no solo a un

[115] Artículo 51 (4) Protocolo Adicional (I): Se prohíben los ataques indiscriminados. Son ataques indiscriminados: (a) los que no están dirigidos contra un objetivo militar concreto; (b) los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o (c) los que emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el presente Protocolo; 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.

[116] Droege, Cordula "Get off my Cloud: Cyber Warfare, International Humanitarian Law and the protection of civilians." International Review of the Red Cross. Vol. 94 number 886. 2012. pp. 571

[117] Ibídem. Droege, pp. 570. Ver también: Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 16.

[118] Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015, pp. 16.

objetivo militar sino también a redes civiles, debido a la replicabilidad inherente a estos programas. En esos casos, se violaría la prohibición de ataque indiscriminado.

Conclusión.

La evolución de las Tecnologías de la Información y la Comunicación (TIC) va acompañada de beneficios y vulnerabilidades; lo que implica sus indiscutibles ventajas, pero también la presencia de nuevos riesgos.

En términos generales, los riesgos generados por Internet impactan en dos grupos: 1) los ocasionados con el empleo de nuevas tecnologías, y, 2) los riesgos que pesan sobre las propias infraestructuras electrónicas cuando son atacadas con el objetivo de alterar o impedir el normal funcionamiento de los sistemas de información; como el acceso no autorizado, la difusión de programas informáticos (virus, bombas lógicas, caballos de Troya o gusanos), y los ataques intencionados de denegación de servicio (DDoS), los que pueden causar graves daños a personas, a entidades u organismos, como así también a infraestructuras críticas.

De acuerdo al Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas elaborado por la Organización de los Estados Americanos (OEA), la mayoría de las instituciones gubernamentales de América Latina han experimentado intentos de manipulación de sus equipos a través de una red o de un sistema.

La trascendencia de estas conductas, tanto a nivel nacional como internacional, ha generado varias reacciones. En primer lugar, si bien las técnicas empleadas siempre suelen ser los virus, los gusanos y los troyanos, se distingue entre los ataques dirigidos contra Estados, que se dan dentro de las llamadas ciberguerras, y aquellas conductas que no se enmarcan en esos conflictos bélicos en el ciberespacio, pero que atentan contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos previstas en las legislaciones internas de cada país.

En el primero de los casos, se advierte una serie de reportes de distintos Estados en relación con ataques en sus sistemas. De allí el abordaje de éstas conductas por el Derecho Internacional humanitario. En el segundo de los casos, cada país hizo frente a éstos ataques digitales criminalizándolos en sus respectivas legislaciones; más allá de las iniciativas internacionales para afrontar éste fenómeno desde una política penal común, dado los problemas relacionados con los límites geográficos y las fronteras nacionales.

No cabe duda que el diseño e implementación de una política de persecución internacional de los ciberataques no es solamente un tema jurídico, sino también, político, de seguridad y de relaciones internacionales.

No es únicamente un tema de derecho penal sino de posicionamiento de política internacional en uno de los aspectos claves para las relaciones internacionales del futuro: la regulación de Internet, siendo un tema central para todos los Estados como así también ámbitos de organizaciones internacionales universales como Naciones Unidas, Consejo de Europa, Unión Europea, etc. o regionales y subregionales, como OEA, MERCOSUR, entre otras.

El principio de distinción requiere que se haga una distinción entre civiles y combatientes, y entre objetivos militares y bienes de carácter civil.

El artículo 48 del Protocolo Adicional (I) dice: "A fin de garantizar el respeto y la protección de la población civil y los bienes de carácter civil, las partes en conflicto distinguirán en todo momento entre la población civil y los combatientes y entre los bienes de carácter civil y los objetivos militares y, en consecuencia, sus operaciones solo contra objetivos militares".

La distinción es fundamental para definir si se cometió un crimen de guerra o si tuvo lugar un acto lícito en un conflicto armado. Esto también aplica a ciberataques.

El Grupo de Expertos indica que el principio de distinción se aplicará a las operaciones cibernéticas contra bienes de carácter civil cuando alcancen el umbral de "ataque".

La pregunta que surge es si el principio de distinción se aplica solo a las operaciones cibernéticas en general o solo a aquellas que caen dentro de la definición de ataque.

Algunos autores han argumentado que este tema es preocupante desde el punto de vista de la población civil, ya que habilita y amplía el abanico de objetivos legítimos, debido a que las operaciones cibernéticas pueden no causar daño físico y por lo tanto quedan fuera del alcance del principio de distinción.

Sin embargo, otros autores sostienen que el principio de distinción debe aplicarse no solo a los ataques a redes informáticas, sino también a las operaciones militares en el ciberespacio en el contexto de las hostilidades. En este sentido, Dinniss sostiene que los principios de distinción, proporcionalidad y precaución se aplican a los ciberataques que alcanzan el umbral antes mencionado, pero también a las operaciones militares. Esto podría entenderse a la luz del artículo 48 del Protocolo (I) y los capítulos de los artículos 51 y 57 que, de otra manera, serían superfluos. Christakis sostiene además que debe adoptarse un enfoque dinámico, de modo que el principio de distinción pueda ser reinterpretado de acuerdo con las nuevas realidades a fin de respetar sus metas y propósitos: la protección de los civiles de los efectos de las guerras.

Con relación a los ataques contra personas, hay cuatro grupos de personas que pueden ser objetivos legítimos: 1) miembros de las fuerzas armadas; 2) miembros de grupos organizados. Estas categorías están estrictamente relacionadas con el estado de las personas. 3) los civiles que participan directamente en las hostilidades y, 4) los participantes en un "levantamiento en masa" en un conflicto armado internacional. Las dos ultimas categorías dependen de la conducta en la que se involucren los civiles.

Las opiniones del Grupo de Expertos estuvieron divididas cuando se discutió el alcance de los "grupos organizados". Por un lado, se afirmó que cuando se demuestra que la persona es

parte de un grupo organizado, se convierte en un objetivo legítimo. Por otro lado, algunos expertos enfatizaron que se debe tratar de un estatus continuo; de lo contrario, las personas se considerarán civiles y se convertirán en objetivos legítimos solo en el momento en que participen efectivamente en las hostilidades.

Con relación a los objetos, hay algunos problemas que surgen en relación con los bienes civiles y los objetivos militares. Los bienes de carácter civil se definen en el artículo 52 (1) del Protocolo Adicional (I) en sentido negativo. El artículo 100 del Manual de Tallin establece: "Los bienes de carácter civil son todos los bienes que no son objetivos militares. Los objetivos militares son aquellos objetos que, por su naturaleza, ubicación, finalidad o uso, contribuyen eficazmente a la acción militar y cuya destrucción, captura o neutralización total o parcial, en las circunstancias que imperen en el momento, ofrece una clara ventaja militar. La infraestructura cibernética puede calificar como un objetivo militar".

Una pregunta que se debe realizar después de leer el artículo es la siguiente: ¿Se incluye "datos" en el término "objeto"? ¿Pueden los datos ser un objetivo lícito? La posición mayoritaria es que el término "objetos" solo cubre los objetos tangibles y visibles. Por lo tanto, un ataque a datos que son intangibles no califica como un "ataque". Sin embargo, el Grupo de Expertos ha señalado que una "operación cibernética dirigida a datos a veces puede calificar como un ataque cuando la operación afecta la funcionalidad de la infraestructura cibernética o da como resultado otras consecuencias que calificarían la operación cibernética en cuestión como un ataque".

Los objetos pueden calificar como objetivos militares de acuerdo con una prueba de cuatro criterios: naturaleza, ubicación, uso y propósito.

Los objetos que contribuyen por su naturaleza a las acciones militares incluyen armas, transporte, fortificaciones, edificios ocupados por las fuerzas armadas, etc. En lo que respecta

a los ataques a redes informáticas, los objetivos pueden incluir sistemas de armas, conjuntos de sensores, redes militares.

Esto trae el problema de los objetos de "uso dual". En este tema, el Manual de Tallin establece en el artículo 101 que "la infraestructura cibernética utilizada tanto para fines civiles como militares es un objetivo militar". En este sentido, el Grupo de Expertos sostiene que en casos poco claros, cuando no sabemos qué conexiones a Internet se utilizan con fines militares, toda la red califica como objetivo militar. Sin embargo, el ataque debe limitarse a segmentos discretos.

Kai Ambos argumenta que, en la infraestructura cibernética, debido a que los sistemas informáticos civiles y militares son difíciles de distinguir (ambos pueden tener fines civiles y militares al mismo tiempo), el principio de distinción tiene una importancia práctica limitada. En esta línea, Ambos brinda el ejemplo en que una parte en conflicto utiliza un sistema de información - per se civil - de un hospital para lanzar un ciberataque, estos sistemas de información se convierten en objetivos militares.

Como pudimos ver, el fenómeno de los ciberataques está sujeto a las normas y principios del derecho internacional humanitario o de los Conflictos Armados.

El principio de distinción, como lo señaló la Corte Internacional de Justicia, es uno de los principios cardinales del derecho de los conflictos armados[119]. Este es un avance positivo, ya que implica la protección de los civiles. Sin embargo, hemos analizado los problemas y desafíos que presenta una reinterpretación y transposición del principio en entornos cibernéticos, poniendo en peligro la protección efectiva de la población civil y dificultando establecer una diferenciación clara de bienes militares y civiles. El análisis debe realizarse

[119] https://www.icrc.org/en/doc/assets/files/other/irrc_850_chetail.pdf

en conjunto con los principios de proporcionalidad y precaución, a fin de limitar las consecuencias de los ataques cibernéticos a la población civil. Este es un campo nuevo, en el que hay poca práctica. Deberíamos seguir discutiendo las protecciones necesarias para proteger la infraestructura civil de daños.

Bibliografía

- Aboso, Gustavo. E; Derecho penal cibernético, Buenos Aires, Editorial B de f, 2017.
- Ambos Kai, Responsabilidad penal internacional en el ciberespacio, InDret (Revista para el análisis del derecho), Barcelona, abril de 2015.
- Ambos, Kai, "International Criminal Responsability in Cyberspace" in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing ed, 2015.
- Barrio Andrés. M, Ciberdelitos 2.0, Amenazas criminales del ciberespacio. 2da. Ed. Buenos Aires, Astrea, 2020.
- Bannelier-Christakis Karine, "Is the principle of distinction still relevant in Cyberwarfare?", in Nicholas Tsagourias and Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar, Publishing ed, 2015.
- Convenio sobre la Ciberdelincuencia, Consejo de Europa, Budapest, 2001, cfr. Informe explicativo, Convenio sobre la Ciberdelincuencia, STE#N185, https://:rm.coe.int.
- Droege Cordula, Sobre las distintas interpretaciones de la "guerra cibernética" en la práctica estatal, *Get off my Cloud*: Cyber Warfare, International Humanitarian Law and the Protection of Civilians, IRRC (94), 2012.
- Dormann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." 2004. Published in https://www.icrc.org/eng/resources/documents/misc/68lg92.htm, visto: 03/08/2021.

- Dinniss Harrison, Heateher. “Cyber Warfare and the Laws of War.” Cambridge Studies in International and Comparative Law. Cambridge University Press. 2012.

- Gervais, Michael. “Cyber Attacks and the Laws of War.” 30 Berkeley J. Int'l L. 525.
- Kiefer, Mariana. Cibercrimen, Aspectos de Derecho penal y procesal penal, Buenos Aires, Editorial B de f, 2016.
- Kelsey T. G. Jeffrey. “Hacking into International Humanitarian Law: The principle of Distinction and Neutrality in the Age of Cyber Warfare.” Michigan Law Review. 2008.
- Kilovaty, Ido. “Virtual violence, disruptive cyber-space operations as “attacks” under international humanitarian law.” 23 Mich. Telecomm. Tech. L. Rev. 113.
- Lubell Noam, definición del Departamento de Defensa de EE.UU., Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?, 2013.
- Miller, Kevin. “The Kampala Compromise and Cyberattacks: Can there be an International Crime of Cyber-Agression?” Southern California Interdisciplinary Law Jorunal. Vol. 23. 2014.
- Poveda Criado, Miguel Ángel, Delitos en la red, Madrid, Editorial Fragua, 2015.
- *Prosecutor v. Tadic. ICTY-94-1-AR. October 2nd,1995.*
- Convenio de Ginebra (1949) https://www.icrc.org/es/doc/assets/files/publications/convenios-gva-esp-2012.pdf
- Protocolo Adicional (I) a los Convenios de Ginebra https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#GUERRA

- Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas elaborado por la Organización de los Estados Americanos (OEA), pp.29. Disponible en www.sites.oas.org
- Satapathy, "Law for Computer Misuse and Data Protection", *Economic and Political Weekly*, octubre de 1998.
- Sallis, Ezequiel, Desafíos de la investigación de los delitos informáticos en la *Deep* y *Dark* Web, en Cibercrimen, Buenos Aires, Editorial B de f, 2016.
- Seitz, Nicolai. Transborder Search. A New Perspective In Law Enforcement, Yale Journal of Law and Technology, vol 7, 2005.
- Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Draft Protocol version 2, 12 de Abril 2021, www.coe.int/cybercrime
- Schmitt Michael N., El Manual de Tallin (traducido al español), Cambridge University Press, Reino Unido, 2017.
- Schmitt, Michael N. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University Press ed. 2017.
- United States v. Morris 928 f.2d 504, 505 (2d Cir. 1991)